

# Guia de instalação, configuração e upgrade do vCloud Director

19 DE SETEMBRO DE 2019  
VMware Cloud Director 10.0

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 © 2010-2020 VMware, Inc. Todos os direitos reservados. [Informações sobre direitos autorais e marca registrada.](#)

# Conteúdo

Guia de instalação, configuração e upgrade do vCloud Director 7

## **1** Visão geral da instalação, configuração e atualização do vCloud Director 8

Arquitetura do vCloud Director 8

Planejamento de configuração 10

## **2** Requisitos de hardware e software do vCloud Director 11

Requisitos de configuração de rede para o vCloud Director 12

Requisitos de segurança de rede 13

## **3** Antes de instalar o vCloud Director ou implantar o dispositivo do vCloud Director 16

Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux 16

Preparando o armazenamento do servidor de transferência 18

Instalar e configurar um agente RabbitMQ AMQP 21

Baixe e instale a chave pública da VMware 22

Instalar e configurar o NSX Data Center for vSphere para o vCloud Director 22

Instalar e configurar o NSX-T Data Center para o vCloud Director 24

## **4** Criação e gerenciamento de certificados SSL para o vCloud Director no Linux 26

Antes de criar certificados SSL para o vCloud Director no Linux 26

Criar certificados SSL autoassinados para o vCloud Director no Linux 27

Criar um armazenamento de chaves de certificados SSL assinado por CA para o vCloud Director no Linux 28

Criar um armazenamento de chaves de certificados SSL assinado por CA com chaves privadas importadas para o vCloud Director no Linux 32

## **5** Instalar o vCloud Director no Linux 35

Instalar o vCloud Director no primeiro membro de um grupo de servidores 36

Configurar as conexões de rede e banco de dados 38

Referência de configuração interativa 40

Referência de configuração autônoma 41

Proteger e reusar o arquivo de resposta 45

Instalar o vCloud Director em um membro adicional de um grupo de servidores 46

## **6** Implantação do vCloud DirectorAppliance 49

Implantações de dispositivo e configuração de alta disponibilidade do banco de dados 51

Pré-requisitos para a implantação do appliance do vCloud Director 54

Implantar o dispositivo do vCloud Director usando o vSphere Client	55
Diretrizes de dimensionamento de dispositivos do vCloud Director	56
Iniciar a implantação do dispositivo do vCloud Director	61
Personalizar o dispositivo do vCloud Director e concluir a implantação	63
Implantação do dispositivo vCloud Director usando o VMware OVF Tool	65
<b>7 Criação e gerenciamento de certificados SSL do dispositivo vCloud Director</b>	<b>74</b>
Implantar o dispositivo vCloud Director com certificados curinga assinados para comunicação HTTPS e via proxy de console	74
Criar e importar certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director	76
Importar chaves privadas e certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director	80
Substituir um certificado de interface de usuário de gerenciamento do dispositivo vCloud Director e PostgreSQL incorporado autoassinado	82
Renovar os certificados do dispositivo vCloud Director	83
<b>8 Configuração do dispositivo do vCloud Director</b>	<b>85</b>
Visualizar o status das células em um cluster de alta disponibilidade de banco de dados	86
Recuperar de uma falha de banco de dados primário em um cluster de alta disponibilidade	86
Recuperar de uma falha de célula em espera em um cluster de alta disponibilidade	87
Backup e restauração do banco de dados incorporado do dispositivo do vCloud Director	88
Fazer backup do banco de dados incorporado do dispositivo vCloud Director	88
Restaurando um ambiente de dispositivo vCloud Director com uma configuração de banco de dados de alta disponibilidade	89
Configurar o acesso externo ao banco de dados do vCloud Director	92
Ativar ou desativar o acesso do SSH ao dispositivo do vCloud Director	93
Editar as configurações de DNS do vCloud Director Appliance	93
Editar as rotas estáticas para as interfaces de rede do dispositivo do vCloud Director	94
Scripts de configuração no appliance vCloud Director	96
Aumentar a capacidade do banco de dados PostgreSQL incorporado em um dispositivo do vCloud Director	96
Modificar as configurações do PostgreSQL no dispositivo do vCloud Director	97
<b>9 Usando o conjunto de ferramentas do Replication Manager em uma configuração de cluster de alta disponibilidade</b>	<b>99</b>
Verificar o status de conectividade de um cluster de alta disponibilidade de banco de dados	100
Verificar o status de replicação de um nó em um cluster de alta disponibilidade de banco de dados	101
Verificar o status de um cluster de alta disponibilidade do banco de dados	102
Detectando um nó primário antigo que volta a ficar online em um cluster de alta disponibilidade	103

- Alternar as funções da célula primária e de uma célula em espera em um cluster de alta disponibilidade de banco de dados 105
- Cancelar o registro de um nó em espera com falha ou inacessível em um cluster de alta disponibilidade de banco de dados 106
- Cancelar o registro de uma célula primária com falha em um cluster de alta disponibilidade de banco de dados 107
- Cancelar o registro de uma célula em espera em execução em um cluster de alta disponibilidade de banco de dados 108

## **10 Referência da ferramenta de gerenciamento de células 109**

- Configurar uma instalação do vCloud Director 113
- Habilitar o vCloud Director Web Console 115
- Desativar o acesso do provedor de serviços ao endpoint da API herdada 117
- Como gerenciar uma célula 118
- Como gerenciar aplicativos de célula 119
- Como atualizar as propriedades de conexão do banco de dados 121
- Detectar e reparar dados corrompidos do agendador 124
- Como gerar certificados autoassinados para os endpoints de proxy de console e HTTP 125
- Substituindo certificados para os endpoints de proxy de console e HTTP 127
- Importação de certificados SSL de serviços externos 128
- Gerenciamento da lista de codificações SSL permitidas 130
- Gerenciar a lista de protocolos SSL permitidos 132
- Como configurar a coleção de métricas 134
- Configuração de um banco de dados de métricas do Cassandra 136
- Recuperação da senha do administrador do sistema 138
- Atualizar o status de falha de uma tarefa 139
- Configurar o tratamento de mensagens de auditoria 140
- Configurar modelos de e-mail 142
- Encontrar VMs órfãs 143
- Entrar ou sair do Programa de aperfeiçoamento da experiência do cliente da VMware 145
- Atualização das definições de configuração do aplicativo 146
- Como configurar a limitação da sincronização de catálogo 147
- Solucionar problemas de falha no acesso à interface do usuário do vCloud Director 149
- Depuração da detecção de VM do vCenter 150
- Como regenerar endereços MAC para redes estendidas multissite 151
- Atualizar os endereços IP do banco de dados em células do vCloud Director 154

## **11 Após você instalar o vCloud Director ou implantar o dispositivo do vCloud Director 156**

- Instalar arquivos do Microsoft Sysprep nos servidores 156
- Alterar o fuso horário do dispositivo do vCloud Director 157
- Personalizar endereços públicos 158

Instalar e configurar um banco de dados Cassandra para armazenar dados de métricas de históricos 160

Realizar configurações adicionais no banco de dados PostgreSQL externo 161

## **12 Atualizando o vCloud Director 163**

Fazer upgrade do dispositivo do vCloud Director 167

Reverter um dispositivo do vCloud Director quando um upgrade falhar 170

Fazer upgrade do dispositivo do vCloud Director usando o Repositório de Atualização da VMware 171

Realizar uma atualização orquestrada de uma instalação do vCloud Director 173

Atualizar manualmente uma instalação do vCloud Director 176

Atualizar uma célula do vCloud Director 177

Atualizar o banco de dados do vCloud Director 179

Referência do utilitário de atualização de banco de dados 180

## **13 Migrando para o dispositivo do vCloud Director 184**

Migrando o vCloud Director com um banco de dados externo PostgreSQL para um dispositivo do vCloud Director 184

## **14 Depois de atualizar ou migrar o vCloud Director 190**

Atualizar cada NSX Manager associado a um sistema vCenter Server anexado 190

Atualizar sistemas vCenter Server, hosts ESXi e NSX Edges 191

## **15 Exibindo os logs do vCloud Director 193**

## **16 Solucionando problemas com o appliance vCloud Director 195**

Examinar os arquivos de log no vCloud Director Appliance 195

A célula do vCloud Director não é iniciada após a implantação do appliance 196

A reconfiguração do serviço do vCloud Director falha ao migrar ou restaurar para o dispositivo vCloud Director 197

Usando os arquivos de log para solucionar problemas de atualizações e patches do vCloud Director 197

Falha na verificação de atualizações do vCloud Director 198

Falha na instalação da atualização mais recente do vCloud Director 198

## **17 Desinstalar o software vCloud Director 200**

# Guia de instalação, configuração e upgrade do vCloud Director

*O Guia de instalação, configuração e upgrade do vCloud Director* fornece informações sobre como instalar e atualizar o software VMware vCloud Director<sup>®</sup> for Service Providers e configurá-lo para funcionar com o VMware vSphere<sup>®</sup>, o VMware NSX<sup>®</sup> for vSphere<sup>®</sup> e o VMware NSX-T<sup>™</sup> Data Center.

## Público-alvo

*O Guia de instalação, configuração e upgrade do vCloud Director* foi concebido para qualquer pessoa que queira instalar ou atualizar o software vCloud Director. As informações neste livro foram escritas para administradores de sistema experientes que estão familiarizados com o Linux, o Windows, redes IP e o vSphere.

# Visão geral da instalação, configuração e atualização do vCloud Director

# 1

Criar um grupo de servidores do vCloud Director instalando o software vCloud Director em um ou mais servidores Linux ou implantando uma ou mais instâncias do dispositivo do vCloud Director. Durante o processo de instalação, você deve executar a configuração inicial do vCloud Director, que inclui o estabelecimento de conexões de rede e do banco de dados.

O software vCloud Director para Linux requer um banco de dados externo, enquanto o appliance vCloud Director usa um banco de dados PostgreSQL incorporado.

Depois de criar o grupo de servidores do vCloud Director, você integra a instalação do vCloud Director aos recursos do vSphere. Para os recursos de rede, o vCloud Director pode usar NSX Data Center for vSphere, NSX-T Data Center ou ambos.

Quando você atualiza uma instalação existente do vCloud Director, você atualiza o software vCloud Director e o esquema do banco de dados, deixando as relações existentes entre servidores, o banco de dados e o vSphere em vigor.

Ao migrar uma instalação existente do vCloud Director no Linux para o appliance vCloud Director, você atualiza o software vCloud Director e migra o banco de dados para o banco de dados incorporado no appliance.

Este capítulo inclui os seguintes tópicos:

- [Arquitetura do vCloud Director](#)
- [Planejamento de configuração](#)

## Arquitetura do vCloud Director

Um grupo de servidores vCloud Director consiste em um ou mais servidores vCloud Director instalados no Linux ou em implantações do appliance vCloud Director. Cada servidor no grupo executa um conjunto de serviços chamado de célula do vCloud Director. Todas as células compartilham um único banco de dados vCloud Director e um armazenamento de servidor de transferência e se conectam aos recursos do vSphere e da rede.

---

**Importante** As instalações mistas do vCloud Director no Linux e as implantações de appliance vCloud Director em um único grupo de servidores não têm suporte.

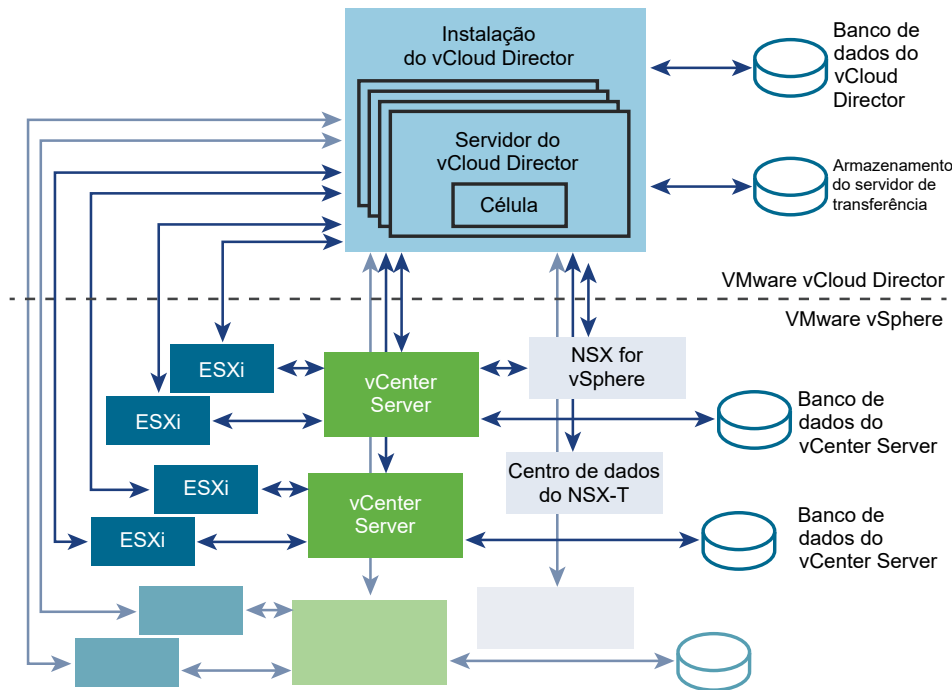
---



Para garantir a alta disponibilidade do vCloud Director, você deve instalar pelo menos duas células do vCloud Director em um grupo de servidores. Ao usar um balanceador de carga de terceiros, você pode garantir o failover automático sem tempo de inatividade.

Você pode conectar uma instalação do vCloud Director a vários sistemas do VMware vCenter Server® e aos hosts VMware ESXi™ que eles gerenciam. Para serviços de rede, o vCloud Director pode usar o NSX Data Center for vSphere associado ao vCenter Server ou você pode registrar o NSX-T Data Center no vCloud Director. NSX Data Center for vSphere e NSX-T Data Center mistos também são compatíveis.

Figura 1-1. Diagrama da arquitetura do vCloud Director



Um grupo de servidores vCloud Director instalado no Linux usa um banco de dados externo.

Um grupo de servidores vCloud Director que consiste em implantações de appliance usa o banco de dados incorporado no primeiro membro do grupo de servidores. Você pode configurar uma alta disponibilidade de banco de dados do vCloud Director implantando duas instâncias do appliance como células em espera no mesmo grupo de servidores. Consulte [Implantações de dispositivo e configuração de alta disponibilidade do banco de dados](#).

Figura 1-2. Appliances vCloud Director que compõem um cluster de alta disponibilidade de banco de dados incorporado

O processo de instalação e configuração do vCloud Director cria as células, conecta-as ao banco de dados compartilhado e ao armazenamento do servidor de transferência e cria a conta de **administrador do sistema**. Em seguida, o **administrador do sistema** estabelece conexões com o sistema do vCenter Server, os hosts do ESXi e as instâncias do NSX Manager ou do NSX-T Manager.

Para obter informações sobre como adicionar recursos do vSphere e de rede, consulte o *Guia do Portal de Administração do Provedor de Serviços do vCloud Director*.

## Planejamento de configuração

O vSphere fornece a capacidade de rede, processamento e armazenamento para o vCloud Director. Antes de iniciar a instalação, considere quanta capacidade do vSphere e do vCloud Director sua nuvem requer e planeje uma configuração que possa suportá-la.

Os requisitos de configuração dependem de muitos fatores, incluindo o número de organizações na nuvem, o número de usuários em cada organização e o nível de atividade desses usuários. As diretrizes a seguir podem servir como ponto de partida para a maioria das configurações:

- Aloque uma célula do vCloud Director para cada sistema do vCenter Server que você deseja tornar acessível em sua nuvem.
- Certifique-se de que todos os servidores Linux de destino do vCloud Director atendam a pelo menos os requisitos mínimos de memória e armazenamento detalhado em *Notas da Versão do vCloud Director*.
- Se você planeja instalar o vCloud Director no Linux, configure o banco de dados do vCloud Director conforme descrito em [Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux](#).

# Requisitos de hardware e software do vCloud Director

## 2

Cada servidor em um grupo de servidores do vCloud Director deve atender a determinados requisitos de hardware e software. Além disso, um banco de dados com suporte deve estar acessível a todos os membros do grupo. Cada grupo de servidores requer acesso a um sistema vCenter Server, uma instância do NSX Manager e um ou mais hosts do ESXi.

## Compatibilidade com outros produtos da VMware

Para obter as informações mais recentes sobre compatibilidade entre o vCloud Director e outros produtos VMware, consulte as *Matrizes de interoperabilidade de produtos VMware* em [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php).

## Requisitos de configuração do vSphere

Instâncias do vCenter Server e hosts do ESXi destinados ao uso com o vCloud Director devem atender a requisitos de configuração específicos.

- Redes do vCenter Server destinadas para uso como redes externas ou pools de rede do vCloud Director devem estar disponíveis para todos os hosts em qualquer cluster destinado ao uso pelo vCloud Director. Tornar essas redes disponíveis para todos os hosts em um datacenter simplifica a tarefa de adicionar novas instâncias vCenter Server a vCloud Director.
- Os switches distribuídos do vSphere são necessários para redes isoladas e pools de rede com o suporte do NSX Data Center for vSphere.
- Os clusters do vCenter Server usados com o vCloud Director devem especificar um nível de automação do vSphere DRS de **Totalmente automatizado**. O armazenamento DRS, se habilitado, pode ser configurado com qualquer nível de automação.
- As instâncias do vCenter Server devem confiar em seus hosts. Todos os hosts em todos os clusters gerenciados pelo vCloud Director devem ser configurados para exigir certificados de host verificados. Em particular, você deve determinar, comparar e selecionar impressões digitais correspondentes para todos os hosts. Consulte Definir configurações SSL na documentação do *vCenter Server and Host Management*.

## Requisitos de licenciamento do vSphere

O Pacote do provedor de serviços do vCloud Director inclui as licenças do vSphere necessárias.

## Plataformas, bancos de dados e navegadores com suporte

Consulte o *Notas da versão do vCloud Director 10.0* para obter informações sobre as plataformas de servidor, os navegadores, os servidores LDAP e os bancos de dados com suporte por esta versão do vCloud Director.

## Requisitos de espaço em disco, memória e CPU

Requisitos físicos, como espaço em disco, memória e CPU para células do vCloud Director, estão listados nas *Notas da versão do vCloud Director 10.0*.

## Armazenamento compartilhado

O NFS ou outro volume de armazenamento compartilhado para o serviço de transferência do vCloud Director. O volume de armazenamento deve ser expansível e acessível a todos os servidores no grupo de servidores.

Este capítulo inclui os seguintes tópicos:

- [Requisitos de configuração de rede para o vCloud Director](#)
- [Requisitos de segurança de rede](#)

## Requisitos de configuração de rede para o vCloud Director

A operação segura e confiável do vCloud Director depende de uma rede segura e confiável que ofereça suporte a pesquisa direta e inversa de nomes de host, um serviço de horário de rede e outros serviços. A rede deve atender a esses requisitos antes de você começar a instalar o vCloud Director.

A rede que conecta os servidores do vCloud Director, o servidor do banco de dados, os sistemas do vCenter Server e os componentes do NSX deve atender a vários requisitos:

### Endereços IP

Cada servidor do vCloud Director deve oferecer suporte a dois endpoints SSL diferentes. Um endpoint é para o serviço HTTP. Outro endpoint é para o serviço de proxy do console. Esses endpoints podem ser endereços IP separados, ou um único endereço IP com duas portas diferentes. Você pode usar aliases IP ou várias interfaces de rede para criar esses endereços. Não use o comando do Linux `ip addr add` para criar o segundo endereço.

O appliance vCloud Director usa seu endereço IP `eth0` com a porta personalizada 8443 para o serviço de proxy do console.

### Endereço proxy do console

O endereço IP configurado como o endpoint proxy do console não deve estar localizado atrás de um balanceador de carga com terminação SSL ou proxy reverso. Todas as solicitações de proxy de console devem ser enviadas diretamente ao endereço IP proxy do console.

Para uma instalação com um único endereço IP, você pode personalizar o endereço proxy do console do Service Provider Admin Portal. Por exemplo, para o appliance vCloud Director, você deve personalizar o endereço proxy do console como `vcloud.example.com:8443`.

### Serviço de horário de rede

Você deve usar um serviço de horário de rede, como o NTP, para sincronizar os relógios de todos os servidores do vCloud Director, incluindo o servidor de banco de dados. O desvio máximo permitido entre os relógios dos servidores sincronizados é de 2 segundos.

### Fusos horários do servidor

Todos os servidores do vCloud Director, incluindo o servidor de banco de dados, devem ser configurados para estarem no mesmo fuso horário.

### Resolução de nomes de host

Todos os nomes de host que você especificar durante a instalação e configuração devem ser resolvidos pelo DNS usando a pesquisa direta e inversa do nome de domínio totalmente qualificado ou o nome do host não qualificado. Por exemplo, para um host chamado `vcloud.example.com`, ambos os comandos a seguir devem ser bem-sucedidos em um host do vCloud Director:

```
nslookup vcloud
nslookup vcloud.example.com
```

Além disso, se o host `vcloud.example.com` tiver o endereço IP 192.168.1.1, o seguinte comando deverá retornar `vcloud.example.com`:

```
nslookup 192.168.1.1
```

A pesquisa de DNS inversa do endereço IP `eth0` é necessária para o dispositivo. O seguinte comando deve ser bem-sucedido no seu ambiente:

```
host -W 15 -R 1 -T <eth0-IP-address>
```

## Requisitos de segurança de rede

Uma operação segura do vCloud Director requer um ambiente de rede seguro. Configure e teste esse ambiente de rede antes de começar a instalação do vCloud Director

Conecte todos os servidores do vCloud Director a uma rede que é protegida e monitorada. As conexões de rede do vCloud Director têm vários requisitos adicionais:

- Não conecte o vCloud Director diretamente à Internet pública. Proteja sempre as conexões de rede do vCloud Director com um firewall. Somente a porta 443 (HTTPS) deve ser aberta para conexões de entrada. As portas 22 (SSH) e 80 (HTTP) também podem ser abertas para conexões de entrada, se necessário. Além disso, a `cell-management-tool` requer acesso ao endereço de loopback da célula. Todos os outros tráfegos de entrada de uma rede pública, inclusive as solicitações para JMX (porta 8999) devem ser rejeitados pelo firewall.

**Tabela 2-1. Portas que devem permitir pacotes de entrada de hosts do vCloud Director**

Porta	Protocolo	Comentários
111	TCP, UDP	Mapeador de porta NFS usado pelo serviço de transferência
920	TCP, UDP	rpc.statd NFS usado pelo serviço de transferência.
61611	TCP	AMQP
61616	TCP	AMQP

- Não conecte as portas usadas para conexões de saída à rede pública.

**Tabela 2-2. Portas que devem permitir pacotes de saída de hosts do vCloud Director**

Porta	Protocolo	Comentários
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	Mapeador de porta NFS usado pelo serviço de transferência
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	As conexões do vCenter, NSX Manager e ESXi que usam a porta padrão. Se você optou por uma porta diferente para esses serviços, desative a conexão para a porta 443 e ative-as para a porta que você escolheu.
514	UDP	Opcional. Permite o uso de syslog.
902	TCP	Conexões do ESXi e vCenter.
903	TCP	Conexões do ESXi e vCenter.
920	TCP, UDP	rpc.statd NFS usado pelo serviço de transferência.

**Tabela 2-2. Portas que devem permitir pacotes de saída de hosts do vCloud Director (continuação)**

Porta	Protocolo	Comentários
5432	TCP	Porta do banco de dados PostgreSQL padrão
5672	TCP, UDP	Opcional. Mensagens AMQP para extensões de tarefa.
61611	TCP	AMQP
61616	TCP	AMQP

- Rotear o tráfego entre os servidores do vCloud Director e os seguintes servidores em uma rede privada dedicada.
  - Servidor do banco de dados do vCloud Director
  - RabbitMQ
  - Cassandra
- Se possível, rotear o tráfego entre os servidores do vCloud Director, vSphere e NSX por uma rede privada dedicada.
- Os switches virtuais e os switches virtuais distribuídos que oferecem suporte a redes do provedor devem ser isolados entre si. Eles não podem compartilhar o mesmo segmento de rede física camada 2.
- Use NFSv4 para armazenamento de serviço de transferência. A versão mais comum de NFS, o NFS v3, não tem a criptografia de trânsito que, em algumas configurações, pode ativar a detecção ou adulteração dos dados transferidos em andamento. Ameaças inerentes ao NFSv3 são descritas no artigo técnico da SANS [SNFS Security in Both Trusted and Untrusted Environments](#). Informações adicionais sobre a configuração e proteção do serviço de transferência do vCloud Director estão disponíveis no artigo da Base de Conhecimento VMware [2086127](#).

# Antes de instalar o vCloud Director ou implantar o dispositivo do vCloud Director

## 3

Antes de instalar o vCloud Director em um servidor Linux ou implantar o dispositivo do vCloud Director, você deve preparar o seu ambiente.

Este capítulo inclui os seguintes tópicos:

- [Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux](#)
- [Preparando o armazenamento do servidor de transferência](#)
- [Instalar e configurar um agente RabbitMQ AMQP](#)
- [Baixe e instale a chave pública da VMware](#)
- [Instalar e configurar o NSX Data Center for vSphere para o vCloud Director](#)
- [Instalar e configurar o NSX-T Data Center para o vCloud Director](#)

## Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux

As células do vCloud Director usam um banco de dados para armazenar informações compartilhadas. Antes de instalar o vCloud Director no Linux, você deve instalar e configurar uma instância do banco de dados PostgreSQL e criar a conta de usuário do banco de dados vCloud Director.

Os bancos de dados PostgreSQL possuem requisitos de configuração específicos quando você os usa com o vCloud Director.

Você deve criar um esquema de banco de dados dedicado separado para o vCloud Director usar. O vCloud Director não pode compartilhar um esquema do banco de dados com nenhum outro produto VMware.



O vCloud Director oferece suporte a conexões SSL com o banco de dados PostgreSQL. Você pode habilitar o SSL no banco de dados PostgreSQL durante uma configuração de conexões de rede e banco de dados autônoma ou depois de criar o grupo de servidores do vCloud Director. Consulte [Referência de configuração autônoma](#) e [Realizar configurações adicionais no banco de dados PostgreSQL externo](#).

---

**Observação** Somente o vCloud Director no Linux usa um banco de dados externo. O appliance vCloud Director usa o banco de dados PostgreSQL incorporado.

---

## Pré-requisitos

Para obter informações sobre os bancos de dados do vCloud Director com suporte, consulte as [Matrizes de interoperabilidade de produtos VMware](#).

Você deve estar familiarizado com comandos, scripts e operações do PostgreSQL.

## Procedimentos

### 1 Configure o servidor do banco de dados.

Um servidor do banco de dados com 16 GB de memória, 100 GB de armazenamento e 4 CPUs é adequado para grupos de servidores típicos do vCloud Director.

### 2 Instale uma distribuição compatível do PostgreSQL no servidor do banco de dados.

- O valor de `SERVER_ENCODING` do banco de dados deve ser UTF-8. Esse valor é estabelecido quando você instala o banco de dados e sempre corresponde à codificação usada pelo sistema operacional do servidor do banco de dados.
- Use o comando `initdb` do PostgreSQL para definir o valor de `LC_COLLATE` e `LC_CTYPE` como `en_US.UTF-8`. Por exemplo:

```
initdb --locale=en_US.UTF-8
```

### 3 Crie o usuário do banco de dados.

O comando a seguir cria o usuário `vcloud`.

```
create user vcloud;
```

### 4 Crie a instância do banco de dados e dê a ela um proprietário.

Use um comando como este para especificar um usuário do banco de dados chamado `vcloud` como proprietário do banco de dados.

```
create database vcloud owner vcloud;
```

### 5 Atribua uma senha de banco de dados para a conta do proprietário do banco de dados.

O comando a seguir atribui a senha `vcloudpass` ao proprietário do banco de dados `vcloud`.

```
alter user vcloud password 'vcloudpass';
```

- 6 Permita que o proprietário do banco de dados faça login no banco de dados.

O comando a seguir atribui a opção login ao proprietário do banco de dados vcloud.

```
alter role vcloud with login;
```

#### Próximo passo

Depois de criar o seu grupo de servidores do vCloud Director, você pode configurar o banco de dados PostgreSQL para exigir conexões SSL das células do vCloud Director e ajustar alguns parâmetros de banco de dados para obter um desempenho ideal. Consulte [Realizar configurações adicionais no banco de dados PostgreSQL externo](#).

## Preparando o armazenamento do servidor de transferência

Para fornecer armazenamento temporário para uploads, downloads e itens de catálogo publicados ou assinados externamente, você deve tornar um volume NFS ou outro volume de armazenamento compartilhado acessível a todos os servidores de um grupo de servidores do vCloud Director.

---

**Importante** O dispositivo do vCloud Director apenas oferece suporte ao tipo NFS de armazenamento compartilhado. O processo de implantação do dispositivo envolve a montagem do armazenamento do servidor de transferência compartilhado NFS.

---

Quando o NFS é usado para o armazenamento do servidor de transferência, você deve configurar cada célula do vCloud Director no grupo de servidores do vCloud Director para montar e usar o armazenamento do servidor de transferência baseado em NFS. Você precisa de permissões de usuário e grupo específicas para configurar cada célula para montar o local baseado em NFS e usá-lo como o armazenamento do servidor de transferência.

Cada membro do grupo de servidores monta esse volume no mesmo ponto de montagem, que normalmente é `/opt/vmware/vcloud-director/data/transfer`. O espaço neste volume é consumido de duas maneiras:

- Durante transferências, uploads e downloads ocupam esse armazenamento. Quando a transferência termina, os uploads e downloads são removidos do armazenamento. As transferências que não fizerem progresso por 60 minutos serão marcadas como expiradas e serão apagadas pelo sistema. Como imagens transferidas podem ser grandes, é uma boa prática alocar pelo menos centenas de gigabytes para esse uso.

- Os itens de catálogo em catálogos externamente publicados e para os quais o cache do conteúdo publicado está ativado ocupam esse armazenamento. Itens de catálogos que são publicados externamente, mas que não permitem cache não ocupam esse armazenamento. Se você permitir que as organizações na sua nuvem criem catálogos que são publicados externamente, poderá assumir que centenas ou até mesmo milhares de itens de catálogo exigem espaço nesse volume. O tamanho de cada item de catálogo é cerca do tamanho de uma máquina virtual em um formulário OVF compactado.

---

**Observação** O volume do armazenamento do servidor de transferência deve ter capacidade para expansão futura.

---

## Como o vCloud Director usa as permissões do sistema de arquivos no local de armazenamento do servidor de transferência

Para todas as células do vCloud Director no grupo de servidores vCloud Director:

- Em operações de nuvem padrão, como carregar itens no catálogo, o daemon da célula do vCloud Director grava e lê arquivos no/do armazenamento do servidor de transferência com o usuário **vcloud** no grupo **vcloud**. O usuário **vcloud** grava os arquivos com umask 0077. Quando o instalador do vCloud Director é executado e instala o software vCloud Director em um membro do grupo de servidores, ele também cria o usuário **vcloud** e o grupo **vcloud**.
- O script do coletor de dados de log do vCloud Director `vmware-vcd-support` pode coletar os logs de todas as suas células do vCloud Director em uma única operação e reunir esses logs em um único arquivo `tar.gz`. Quando você executa o script, ele grava o arquivo `tar.gz` resultante em um diretório no local de armazenamento do servidor de transferência usando o ID do usuário que invoca esse script. Por padrão, o único usuário que tem permissões para executar o script é o usuário **root**.
- O usuário **root** na célula executa o script que grava o arquivo `tar.gz` no diretório `vmware-vcd-support` no local de armazenamento do servidor de transferência. Se você quiser usar as opções de várias células para coletar os logs de todas as células de uma só vez, o usuário **root** deverá ter permissão de leitura para recuperar o pacote de log de diagnóstico `tar.gz`.

## Requisitos para a configuração do servidor NFS

Há requisitos específicos para a configuração do servidor NFS, para que o vCloud Director possa gravar arquivos em um local de armazenamento do servidor de transferência baseado em NFS e ler arquivos a partir dele. Devido a eles, o usuário **vcloud** pode realizar as operações de nuvem padrão enquanto o usuário **root** pode realizar a coleta de logs de várias células.

- A lista de exportação para o servidor NFS deve permitir que cada membro do servidor no seu grupo de servidores vCloud Director tenha acesso de leitura/gravação à localização compartilhada que está identificada na lista de exportação. Esse recurso permite que o usuário **vcloud** grave e leia arquivos no/do local compartilhado.

- O servidor NFS deve permitir acesso de leitura/gravação ao local compartilhado pela conta de sistema **root** em cada servidor no seu grupo de servidores vCloud Director. Esse recurso permite coletar os logs de todas as células ao mesmo tempo em um único pacote usando o script `vmware-vcd-support` com suas opções de várias células. Você pode atender a esse requisito usando `no_root_squash` na configuração de exportação do NFS para este local compartilhado.

Por exemplo, se o servidor NFS tiver o endereço IP 192.168.120.7 e um diretório chamado `vCDspace` como o espaço de transferência para o grupo de servidores vCloud Director com o local `/nfs/vCDspace`, para exportar esse diretório, você deverá garantir que sua propriedade e permissões sejam **root:root** e **750**. O método para permitir acesso de leitura/gravação ao local compartilhado para duas células, `vcd-cell1-IP` e `vcd-cell2-IP`, é o método `no_root_squash`. Você deve adicionar uma linha ao arquivo `/etc/exports`.

```
192.168.120.7/nfs/vCDspace Endereço_vCD_Cell1_IP(rw,sync,no_subtree_check,no_root_squash)
Endereço_vCD_Cell2_IP(rw,sync,no_subtree_check)
```

Não deve haver espaço entre cada endereço IP da célula e o parêntese esquerdo imediato seguinte na linha de exportação. Se o servidor NFS for reinicializado enquanto as células estiverem gravando dados no local compartilhado, o uso da opção `sync` na configuração de exportação impedirá a corrupção de dados nesse local compartilhado. O uso da opção `no_subtree_check` na configuração de exportação melhora a confiabilidade quando um subdiretório de um sistema de arquivos é exportado.

Cada servidor no grupo de servidores do vCloud Director deve ter permissão para montar o compartilhamento do NFS, inspecionando a lista de exportação da exportação do NFS. Exporte a montagem executando `exportfs -a` para exportar novamente todos os compartilhamentos do NFS. Os daemons de NFS `rpcinfo -p localhost` ou `service nfs status` devem estar em execução no servidor.

## Considerações ao planejar o upgrade da sua instalação do vCloud Director para uma versão posterior

Durante um upgrade de um grupo de servidores do vCloud Director, você executa o arquivo de instalação para a versão atualizada para fazer upgrade de todos os membros desse grupo de servidores vCloud Director. Por conveniência, algumas organizações escolhem baixar o arquivo de instalação do upgrade para o local de armazenamento do servidor de transferência e executá-lo a partir daí, pois todas as células têm acesso a esse local. Como o usuário **root** deve ser usado para executar o arquivo de instalação de upgrade, se você quiser usar o local de armazenamento do servidor de transferência para executar um upgrade, deverá garantir que esse usuário **root** possa executar o arquivo de instalação de upgrade durante o processo de upgrade. Se você não puder executar o upgrade como usuário **root**, o arquivo deverá ser copiado para outro local onde possa ser executado como o usuário **root**, por exemplo, outro diretório fora da montagem do NFS.

## Instalar e configurar um agente RabbitMQ AMQP

AMQP, o Advanced Message Queuing Protocol, é um padrão aberto para enfileiramento de mensagens que fornece suporte a mensagens flexíveis para sistemas corporativos. O vCloud Director usa o agente RabbitMQ AMQP para fornecer o barramento de mensagem usado por serviços de extensão, extensões de objeto e notificações.


### Procedimentos

- 1 Baixe o Servidor do RabbitMQ do <https://www.rabbitmq.com/download.html>.  
Consulte *Notas da Versão do vCloud Director* para obter a lista de versões compatíveis do RabbitMQ.
- 2 Siga as instruções de instalação do RabbitMQ e instale-o em um host compatível.  
O host do servidor RabbitMQ deve estar acessível na rede por cada célula do vCloud Director.
- 3 Durante a instalação do RabbitMQ, anote os valores necessários para configurar o vCloud Director para funcionar com esta instalação do RabbitMQ.
  - O nome de domínio completo do host do servidor RabbitMQ, por exemplo *amqp.example.com*.
  - Um nome de usuário e senha válidos para autenticação no RabbitMQ.
  - A porta na qual o agente atende mensagens. O padrão é 5672.
  - O host virtual do RabbitMQ. O padrão é "/"

### Próximo passo

Por padrão, o serviço AMQP do vCloud Director envia mensagens não criptografadas. Você pode configurar o serviço AMQP para criptografar essas mensagens usando o SSL. Você também pode configurar o serviço para verificar o certificado do agente usando o armazenamento confiável JCEKS padrão do Java Runtime Environment na célula do vCloud Director, normalmente em `$VCLLOUD_HOME/jre/lib/security/cacerts`.

Para ativar o SSL com o serviço AMQP do vCloud Director:

- 1 No menu principal () do vCloud Director Service Provider Admin Portal, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, clique em **Extensibilidade**.
- 3 Clique em **Extensibilidade** e em **Editar** para a seção **AMQP Broker**.
- 4 Ative o botão de alternância **Usar SSL**.
- 5 Ative o botão de alternância **Aceitar todos os certificados** ou forneça um dos seguintes:
  - Um nome de caminho do certificado SSL
  - Um nome de caminho e senha do truststore JCEKS

## Baixe e instale a chave pública da VMware

O arquivo de instalação está assinado digitalmente. Para verificar a assinatura, você deve baixar e instalar a chave pública da VMware.

Você pode usar a ferramenta do Linux `rpm` e a chave pública da VMware para verificar a assinatura digital do arquivo de instalação do vCloud Director ou qualquer outro arquivo assinado baixado de `vmware.com`. Se você instalar a chave pública no computador no qual pretende instalar o vCloud Director, a verificação acontecerá como parte da instalação ou atualização. Você também pode verificar manualmente a assinatura antes de iniciar o procedimento de instalação ou atualização e, em seguida, usar o arquivo verificado para todas as instalações ou atualizações.

---

**Observação** O site de download também publica um valor de soma de verificação para o download. A soma de verificação é publicada em dois formulários comuns. Verificar a soma de verificação confere se o conteúdo do arquivo baixado é o mesmo conteúdo postado. Isso não verifica a assinatura digital.

---

### Procedimentos

- 1 Crie um diretório para armazenar as chaves públicas de pacotes VMware.
- 2 Use um navegador da Web para baixar todas as chaves públicas de pacotes públicos da VMware do diretório [de](#) .
- 3 Salve os arquivos de chave no diretório que você criou.
- 4 Para cada chave que você baixar, execute o seguinte comando para importar a chave.

```
# rpm --import /key_path/key_name
```

*key\_path* é o diretório no qual você salvou as chaves.

*key\_name* é o nome de arquivo de uma chave.

## Instalar e configurar o NSX Data Center for vSphere para o vCloud Director

Se você planeja a instalação do vCloud Director para usar os recursos de rede do NSX Data Center for vSphere, deve instalar e configurar o NSX Data Center for vSphere e associar uma instância do NSX Manager exclusiva a cada instância do vCenter Server que planeja incluir na instalação do vCloud Director.

O NSX Manager está incluído no download do NSX Data Center for vSphere. Para obter as informações mais recentes sobre a compatibilidade entre o vCloud Director e outros produtos VMware, consulte as *Matrizes de interoperabilidade de produtos VMware* em [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php). Para obter informações sobre os requisitos de rede, consulte [Requisitos de configuração de rede para o vCloud Director](#).

---

**Importante** Esse procedimento é utilizado somente quando você está realizando uma nova instalação do vCloud Director. Se você estiver atualizando uma instalação existente do vCloud Director, consulte [Capítulo 12 Atualizando o vCloud Director](#).

---

### Pré-requisitos

Verifique se cada um dos seus sistemas do vCenter Server atende os pré-requisitos de instalação do NSX Manager.

### Procedimentos

- 1 Realize a tarefa de instalação para o dispositivo virtual do NSX Manager.

Consulte o *Guia de Instalação do NSX*.

- 2 Faça login no dispositivo virtual do NSX Manager que você instalou e confirme as configurações que você especificou durante a instalação.
- 3 Associe o dispositivo virtual do NSX Manager que você instalou com o sistema do vCenter Server o qual planeja adicionar ao vCloud Director na instalação do vCloud Director planejada.
- 4 Configure o suporte VXLAN nas instâncias do NSX Manager associadas.

O vCloud Director cria pools de rede VXLAN para fornecer recursos de rede para VDCs de provedor. Se o suporte VXLAN não está configurado no NSX Manager associado, os VDCs de provedor mostram um erro de pool de rede, e você deve criar um tipo diferente de pool de rede e associá-lo ao VDC do provedor. Para obter detalhes sobre como configurar o suporte VXLAN, consulte o *Guia de Administração do NSX*.

- 5 (Opcional) Se você quiser Gateways de Borda no sistema para fornecer roteamento distribuído, configure um cluster do NSX Controller.

Consulte o *Guia de Administração do NSX*.

# Instalar e configurar o NSX-T Data Center para o vCloud Director

Se você planeja que a instalação do vCloud Director use os recursos de rede do NSX-T Data Center, deve instalar e configurar o NSX-T Data Center.

---

**Importante** Para configurar os objetos e as ferramentas do NSX-T Data Center, use a UI de política simplificada e as APIs de política que correspondem à UI simplificada. Para obter mais informações, consulte a visão geral do NSX-T Manager no *Guia de administração do NSX-T Data Center*.

---

Para obter as informações mais recentes sobre a compatibilidade entre o vCloud Director e outros produtos VMware, consulte as [Matrizes de interoperabilidade de produtos VMware](#).

Para obter informações sobre os requisitos de rede, consulte [Requisitos de configuração de rede para o vCloud Director](#).

Esse procedimento é utilizado somente quando você está realizando uma nova instalação do vCloud Director. Se você estiver atualizando uma instalação existente do vCloud Director, consulte [Capítulo 12 Atualizando o vCloud Director](#).

## Pré-requisitos

Familiarize-se com o NSX-T Data Center.

## Procedimentos

- 1 Implante e configure os dispositivos virtuais do NSX-T Manager.

Para obter mais informações sobre a implantação do NSX-T Manager, consulte o *Guia de instalação do NSX-T Data Center*.

- 2 Crie zonas de transporte com base nos seus requisitos de rede.

Para obter mais informações sobre a criação de zonas de transporte, consulte o *Guia de instalação do NSX-T Data Center*.

---

## Observação

---

- 3 Implante e configure nós do Edge e um Edge Cluster.

Para obter mais informações sobre a criação do NSX Edge, consulte o *Guia de instalação do NSX-T Data Center*.

- 4 Configure os nós de transporte do host ESXi.

Para obter mais informações sobre como configurar um nó de transporte de host gerenciado, consulte o *Guia de instalação do NSX-T Data Center*.

- 5 Crie um gateway de camada 0.

Para obter mais informações sobre a criação da camada 0, consulte o *Guia de administração do NSX-T Data Center*.



## Próximo passo

Depois de instalar o vCloud Director, você poderá:

- 1 Registrar a instância do NSX-T Manager na sua nuvem.

Para obter informações sobre como registrar uma instância do NSX-T Manager, consulte o *Guia do Portal de Administração do Provedor de Serviços do vCloud Director*.

- 2 Crie um pool de redes com suporte de zona de transporte do NSX-T Data Center.

Para obter mais informações sobre como criar um pool de rede com o suporte de uma zona de transporte do NSX-T Data Center, consulte *Guia do Portal de Administração do Provedor de Serviços do vCloud Director*.

- 3 Importe o gateway de camada 0 como uma rede externa.

Para obter mais informações sobre como adicionar uma rede externa com o suporte de um roteador lógico de camada 0 do NSX-T Data Center, consulte *Guia do Portal de Administração do Provedor de Serviços do vCloud Director*.

# Criação e gerenciamento de certificados SSL para o vCloud Director no Linux

## 4

O vCloud Director usa SSL para proteger comunicações entre clientes e servidores. Cada servidor do vCloud Director deve oferecer suporte a dois endpoints SSL diferentes, um para HTTPS e um para comunicações de proxy do console.

Os endpoints podem ser endereços IP separados ou um único endereço IP com duas portas diferentes. Cada endpoint requer seu próprio certificado SSL. Você pode usar o mesmo certificado para ambos os endpoints, por exemplo, usando um certificado curinga.

Este capítulo inclui os seguintes tópicos:

- [Antes de criar certificados SSL para o vCloud Director no Linux](#)
- [Criar certificados SSL autoassinados para o vCloud Director no Linux](#)
- [Criar um armazenamento de chaves de certificados SSL assinado por CA para o vCloud Director no Linux](#)
- [Criar um armazenamento de chaves de certificados SSL assinado por CA com chaves privadas importadas para o vCloud Director no Linux](#)

## Antes de criar certificados SSL para o vCloud Director no Linux

Ao instalar o vCloud Director para Linux, você deve criar dois certificados para cada membro do grupo de servidores e importar os certificados para os armazenamentos de chaves do host.

---

**Observação** Você deve criar os certificados para os membros do grupo de servidores somente após a instalação do vCloud Director no Linux. O dispositivo do vCloud Director cria certificados SSL autoassinados durante a primeira inicialização.

---

### Procedimentos

- 1 Faça login no servidor vCloud Director como **root**.
- 2 Liste os endereços IP para o servidor.

Use um comando, como `ifconfig`, para detectar endereços IP do servidor.

- 3 Para cada endereço IP, execute o seguinte comando para recuperar o nome de domínio completo (FQDN) ao qual o endereço IP está ligado.

```
nslookup ip-address
```

- 4 Anote cada endereço IP e o FQDN associado a ele. Se não estiver usando um único endereço IP para ambos os serviços, decida qual endereço IP será para o serviço HTTPS e qual será para o serviço de proxy do console.

Você deve fornecer os FQDNs ao criar os certificados e os endereços IP ao configurar as conexões de rede e banco de dados. Anote quaisquer outros FQDNs que possam alcançar o endereço IP, porque você deve fornecê-los se desejar que o certificado inclua um Nome Alternativo da Entidade (SAN).

#### Próximo passo

Crie os certificados para os dois endpoints. Você pode usar certificados assinados por uma autoridade de certificação confiável (CA) ou certificados autoassinados.

---

**Observação** Certificados assinados por CA fornecem o mais alto nível de confiança.

---

- Para obter informações sobre como criar e importar certificados SSL assinados por CA, consulte [Criar um armazenamento de chaves de certificados SSL assinado por CA para o vCloud Director no Linux](#).
- Para obter informações sobre como criar certificados SSL autoassinados, consulte [Criar certificados SSL autoassinados para o vCloud Director no Linux](#).
- Para obter informações sobre como importar sua própria chave privada e seus arquivos de certificado assinados por CA, consulte [Criar um armazenamento de chaves de certificados SSL assinado por CA com chaves privadas importadas para o vCloud Director no Linux](#).

## Criar certificados SSL autoassinados para o vCloud Director no Linux

Os certificados autoassinados podem oferecer uma maneira prática de configurar o SSL para vCloud Director em ambientes onde as preocupações de confiança são mínimas.

Cada servidor do vCloud Director requer dois certificados SSL em um arquivo de armazenamento de chaves JCEKS, um para o serviço HTTPS e um para o serviço de proxy do console.

Use o `cell-management-tool` para criar os certificados SSL autoassinados. O utilitário do `cell-management-tool` é instalado na célula antes que o agente de configuração seja executado e depois que você executar o arquivo de instalação. Consulte [Instalar o vCloud Director no primeiro membro de um grupo de servidores](#).

---

**Importante** Esses exemplos especificam um tamanho de chave de 2048 bits, mas você deve avaliar os requisitos de segurança da instalação antes de escolher um tamanho de chave apropriado. Tamanhos de chaves menores que 1024 bits não são mais suportados pelo NIST Special Publication 800-131A.

---

#### Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH para o sistema operacional do servidor do vCloud Director como **raiz**.
- 2 Execute o comando para criar um par de chaves pública/privada para o serviço HTTPS e para o serviço de proxy do console.

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o certificates.ks -w passwd
```

O comando cria ou atualiza um armazenamento de chaves em `certificates.ks` que tenha a senha `passwd`. O `cell-management-tool` cria os certificados usando os valores padrão do comando. Dependendo da configuração de DNS do seu ambiente, o CN do emissor é definido como o endereço IP ou o FQDN de cada serviço. O certificado usa o comprimento de chave de 2048 bits padrão e expira um ano após a criação.

---

**Importante** O arquivo de armazenamento de chaves e o diretório no qual ele é armazenado devem ser legíveis pelo usuário **vcloud.vcloud**. O instalador do vCloud Director cria esse usuário e grupo.

---

#### Próximo passo

Anote o nome do caminho do armazenamento de chaves. Você precisará do nome do caminho do armazenamento de chaves quando executar o script de configuração para criar as conexões de rede e banco de dados para a célula do vCloud Director. Consulte [Configurar as conexões de rede e banco de dados](#).

## Criar um armazenamento de chaves de certificados SSL assinado por CA para o vCloud Director no Linux

Criar e importar certificados assinados pela autoridade de certificação fornece o mais alto nível de confiança para comunicações SSL e ajuda a proteger as conexões na infraestrutura da sua nuvem.

Cada servidor do vCloud Director requer dois certificados SSL para proteger as comunicações entre clientes e servidores. Cada servidor do vCloud Director deve oferecer suporte a dois endpoints SSL diferentes: para HTTPS e um para comunicações de proxy do console.

Os dois endpoints podem ser endereços IP separados ou um único endereço IP com duas portas diferentes. Cada endpoint requer seu próprio certificado SSL. Você pode usar o mesmo certificado para ambos os endpoints, por exemplo, usando um certificado curinga.

Os certificados para ambos os endpoints devem incluir um nome distinto X.500 e uma extensão de Nome Alternativo de Requerente X.509

Você pode usar certificados assinados por uma autoridade de certificação confiável (CA) ou certificados autoassinados.

Use o `cell-management-tool` para criar os certificados SSL autoassinados. O utilitário do `cell-management-tool` é instalado na célula antes que o agente de configuração seja executado e depois que você executar o arquivo de instalação. Consulte [Instalar o vCloud Director no primeiro membro de um grupo de servidores](#).

Se você já tiver sua própria chave privada e arquivos de certificado assinados pela autoridade de certificação, siga o procedimento descrito em [Criar um armazenamento de chaves de certificados SSL assinado por CA com chaves privadas importadas para o vCloud Director no Linux](#).

---

**Importante** Esses exemplos especificam um tamanho de chave de 2048 bits, mas você deve avaliar os requisitos de segurança da instalação antes de escolher um tamanho de chave apropriado. Tamanhos de chaves menores que 1024 bits não são mais suportados pelo NIST Special Publication 800-131A.

---

#### Pré-requisitos

- Verifique se você tem acesso a um computador com um ambiente de tempo de execução Java versão 8 ou posterior para poder usar o comando do `keytool` para importar os certificados. O instalador do vCloud Director coloca uma cópia do `keytool` no `/opt/vmware/vcloud-director/jre/bin/keytool`, mas você pode executar este procedimento em qualquer computador que tenha um ambiente de tempo de execução Java instalado. Os certificados criados com um `keytool` de qualquer outra fonte não são compatíveis para uso com o vCloud Director. Esses exemplos de linha de comando pressupõem que `keytool` está no caminho do usuário.
- Familiarize-se com o comando do `keytool`.
- Para obter mais detalhes sobre as opções disponíveis para o comando `generate-certs`, consulte [Como gerar certificados autoassinados para os endpoints de proxy de console e HTTP](#).
- Para obter mais detalhes sobre as opções disponíveis para o comando `certificates`, consulte [Substituindo certificados para os endpoints de proxy de console e HTTP](#).

#### Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH no sistema operacional da célula de servidor do vCloud Director como **root**.

- 2 Execute o comando para criar um par de chaves pública/privada para o serviço HTTPS e para o serviço de proxy do console.

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o certificates.ks -w keystore_password
```

O comando cria ou atualiza um armazenamento de chaves em `certificates.ks` com a senha especificada. Os certificados são criados usando os valores padrão do comando. Dependendo da configuração de DNS do seu ambiente, o CN do emissor é definido como o endereço IP ou o FQDN de cada serviço. O certificado usa o comprimento de chave de 2048 bits padrão e expira um ano após a criação.

---

**Importante** O arquivo de armazenamento de chaves e o diretório no qual ele é armazenado devem ser legíveis pelo usuário **vcloud.vcloud**. O instalador do vCloud Director cria esse usuário e grupo.

---

- 3 Crie uma solicitação de assinatura de certificado para o serviço HTTPS e para o serviço de proxy do console.

---

**Importante** Se estiver usando endereços IP separados para o serviço HTTPS e para o serviço de proxy do console, ajuste os nomes de host e os endereços IP nos comandos a seguir.

---

- a Crie uma solicitação de assinatura de certificado no arquivo `http.csr`.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass keystore_password -certreq -alias http -file http.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

- b Crie uma solicitação de assinatura de certificado no arquivo `consoleproxy.csr`.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass keystore_password -certreq -alias consoleproxy -file consoleproxy.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

- 4 Envie as solicitações de assinatura de certificado para sua Autoridade de Certificação.

Se a sua autoridade de certificação exigir que você especifique um tipo de servidor da Web, use o Tomcat da Jakarta.

Você obtém os certificados assinados pela CA.

## 5 Importe os certificados assinados para o armazenamento de chaves JCEKS.

- a Importe o certificado raiz da Autoridade de certificação do arquivo `root.cer` para o arquivo de armazenamento de chaves `certificates.ks`.

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks
-alias root -file root_certificate_file
```

- b Se tiver recebido certificados intermediários, importe-os do arquivo `intermediate.cer` para o arquivo de armazenamento de chaves `certificates.ks`.

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks
-alias intermediate -file intermediate_certificate_file
```

- c Importe o certificado do serviço HTTPS.

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks
-alias http -file http_certificate_file
```

- d Importe o certificado do serviço de proxy do console.

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks
-alias consoleproxy -file console_proxy_certificate_file
```

Os comandos substituem o arquivo `certificates.ks` pelas versões recém-criadas assinadas pela autoridade de certificação dos certificados.

- 6 Para verificar se os certificados foram importados para o armazenamento de chaves JCEKS, execute o comando para listar o conteúdo do arquivo de armazenamento de chaves.

```
keytool -storetype JCEKS -storepass keystore_password -keystore certificates.ks -list
```

- 7 Repita esse procedimento em todos os servidores do vCloud Director no grupo de servidores.

### Próximo passo

- Se você ainda não tiver configurado sua instância do vCloud Director, execute o script configure para importar o repositório de chaves de certificados para o vCloud Director. Consulte [Configurar as conexões de rede e banco de dados](#).

---

**Observação** Se você criou o arquivo de armazenamento de chaves `certificates.ks` em um computador diferente do servidor no qual você gerou a lista de nomes de domínio completos e seus endereços IP associados, copie o arquivo de armazenamento de chave para esse servidor agora. Você precisa do nome do caminho do armazenamento de chaves ao executar o script de configuração.

---

- Se você já tiver instalado e configurado sua instância do vCloud Director, use o comando `certificates` da ferramenta de gerenciamento de células para importar o armazenamento de chaves de certificados. Consulte [Substituindo certificados para os endpoints de proxy de console e HTTP](#).

## Criar um armazenamento de chaves de certificados SSL assinado por CA com chaves privadas importadas para o vCloud Director no Linux

Se você tiver sua própria chave privada e arquivos de certificado assinados pela CA, antes de importar os armazenamentos de chave para o seu ambiente do vCloud Director, deverá criar arquivos de armazenamento de chave nos quais importar os certificados e as chaves privadas para o serviço proxy HTTPS e o console.

### Pré-requisitos

- Consulte [Antes de criar certificados SSL para o vCloud Director no Linux](#).
- Verifique se você tem acesso a um computador com um ambiente de tempo de execução Java versão 8 ou posterior para poder usar o comando do `keytool` para importar os certificados. O instalador do vCloud Director coloca uma cópia do `keytool` no `/opt/vmware/vcloud-director/jre/bin/keytool`, mas você pode executar este procedimento em qualquer computador que tenha um ambiente de tempo de execução Java instalado. Os certificados criados com um `keytool` de qualquer outra fonte não são compatíveis para uso com o vCloud Director. Esses exemplos de linha de comando pressupõem que `keytool` está no caminho do usuário.
- Familiarize-se com o comando do `keytool`.
- Baixe e instale o OpenSSL.
- Para obter mais detalhes sobre as opções disponíveis para o comando `certificates`, consulte [Substituindo certificados para os endpoints de proxy de console e HTTP](#).

### Procedimentos

- 1 Se você tiver certificados intermediários, execute o comando para combinar o certificado assinado pela CA raiz com os certificados intermediários e criar uma cadeia de certificados.

```
cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
```



- 2 Use o OpenSSL para criar arquivos de armazenamento de chaves PKCS12 intermediários para os serviços de proxy HTTPS e console com a chave privada, a cadeia de certificados, o alias respectivo e especifique uma senha para cada arquivo de armazenamento de chaves.

- a Crie o arquivo de armazenamento de chaves para o serviço HTTPS.

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.pfx -chain
```

- b Crie o arquivo de armazenamento de chaves para o serviço de proxy do console.

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.pfx -chain
```

- 3 Use `keytool` para importar os armazenamentos de chaves PKCS12 para o armazenamento de chaves JCEKS.

- a Execute o comando para importar o armazenamento de chaves PKCS12 para o serviço HTTPS.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks -deststoretype JCEKS -srckeystore http.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

- b Execute o comando para importar o armazenamento de chaves PKCS12 para o serviço de proxy do console.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks -deststoretype JCEKS -srckeystore consoleproxy.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

- 4 Para verificar se os certificados foram importados para o armazenamento de chaves JCEKS, execute o comando para listar o conteúdo do arquivo de armazenamento de chaves.

```
keytool -storetype JCEKS -storepass keystore_password -keystore certificates.ks -list
```

- 5 Repita esse procedimento em todas as células do vCloud Director no seu ambiente.

#### Próximo passo

- Se você ainda não tiver configurado sua instância do vCloud Director, execute o script configure para importar o repositório de chaves de certificados para o vCloud Director. Consulte [Configurar as conexões de rede e banco de dados](#).

---

**Observação** Se você criou o arquivo de armazenamento de chaves `certificates.ks` em um computador diferente do servidor no qual você gerou a lista de nomes de domínio completos e seus endereços IP associados, copie o arquivo de armazenamento de chave para esse servidor. Você precisa do nome do caminho do armazenamento de chaves ao executar o script de configuração.

---

- Se você já tiver instalado e configurado sua instância do vCloud Director, use o comando `certificates` da ferramenta de gerenciamento de células para importar o armazenamento de chaves de certificados. Consulte [Substituindo certificados para os endpoints de proxy de console e HTTP](#).

# Instalar o vCloud Director no Linux

# 5

Você pode criar um grupo de servidores do vCloud Director instalando o software vCloud Director de um ou mais servidores Linux. A instalação e a configuração do primeiro membro do grupo cria um arquivo de resposta que você usa para configurar membros adicionais do grupo.

Este procedimento aplica-se apenas a novas instalações. Se você estiver atualizando uma instalação existente do vCloud Director, consulte [Capítulo 12 Atualizando o vCloud Director](#).

---

**Importante** As instalações mistas do vCloud Director no Linux e as implantações de appliance vCloud Director em um único grupo de servidores não têm suporte.

---

## Pré-requisitos

- Verifique se os servidores de destino para o seu grupo de servidores atendem a [Capítulo 2 Requisitos de hardware e software do vCloud Director](#).
- Verifique se você criou um certificado SSL para cada terminal dos servidores de destino para o seu grupo de servidores. Todos os diretórios no nome do caminho para os certificados SSL devem ser legíveis por qualquer usuário. Usar o mesmo caminho do armazenamento de chaves em todos os membros de um grupo de servidores simplifica o processo de instalação, por exemplo /tmp/certificates.ks. Consulte [Antes de criar certificados SSL para o vCloud Director no Linux](#).
- Verifique se você preparou um NFS ou outro volume de armazenamento compartilhado acessível a todos os servidores de destino para o seu grupo de servidores do vCloud Director. Consulte [Preparando o armazenamento do servidor de transferência](#).
- Verifique se você criou um banco de dados do vCloud Director que é acessível a todos os servidores no grupo. Consulte [Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux](#). Verifique se o serviço de banco de dados é iniciado quando você reinicializa o servidor de banco de dados.
- Verifique se todos os servidores do vCloud Director, o servidor do banco de dados, todos os sistemas do vCenter Server e as instâncias do NSX Manager associadas podem resolver cada nome de host no ambiente conforme descrito em [Requisitos de configuração de rede para o vCloud Director](#).
- Verifique se todos os servidores do vCloud Director e o servidor do banco de dados estão sincronizados a um servidor de horário de rede com as tolerâncias observadas em [Requisitos de configuração de rede para o vCloud Director](#).

- Se você planeja importar usuários ou grupos de um serviço de LDAP, verifique se o serviço está acessível para cada servidor do vCloud Director.
- Abra as portas de firewall conforme mostrado em [Requisitos de segurança de rede](#). A porta 443 deve estar aberta entre os sistemas do vCloud Director e do vCenter Server.

## Procedimentos

### 1 [Instalar o vCloud Director no primeiro membro de um grupo de servidores](#)

Após preparar seu ambiente e verificar os pré-requisitos, você pode começar a criar o grupo de servidores do vCloud Director, executando o instalador do vCloud Director no primeiro servidor Linux de destino.

### 2 [Configurar as conexões de rede e banco de dados](#)

Depois de instalar o vCloud Director no primeiro membro do grupo de servidores, você deve executar o script de configuração que cria as conexões de rede e banco de dados para essa célula. O script cria um arquivo de resposta que você deve usar ao configurar membros adicionais do grupo de servidores.

### 3 [Instalar o vCloud Director em um membro adicional de um grupo de servidores](#)

Você pode adicionar servidores a um grupo de servidores do vCloud Director a qualquer momento. Como todos os servidores em um grupo de servidores devem ser configurados com os mesmos detalhes de conexão do banco de dados, você deve usar o arquivo de resposta criado quando você criou o primeiro membro do grupo.

## Próximo passo

Use o comando `system-setup` da ferramenta de gerenciamento de célula para inicializar o banco de dados do grupo de servidores com uma conta de administrador do sistema e informações relacionadas. Consulte [Configurar uma instalação do vCloud Director](#).

## Instalar o vCloud Director no primeiro membro de um grupo de servidores

Após preparar seu ambiente e verificar os pré-requisitos, você pode começar a criar o grupo de servidores do vCloud Director, executando o instalador do vCloud Director no primeiro servidor Linux de destino.

O vCloud Director para Linux é distribuído como um arquivo executável assinado digitalmente com um nome do formulário `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, onde *v.v.v* representa a versão do produto e *nnnnnn* o número da compilação. Por exemplo: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. A execução desse executável instala ou atualiza o vCloud Director.

O instalador do vCloud Director verifica se o servidor de destino atende a todos os pré-requisitos de plataforma e instala o software vCloud Director no servidor.

## Pré-requisitos

- Verifique se você tem as credenciais de superusuário para o servidor de destino.
- Se você quiser que o instalador verifique a assinatura digital do arquivo de instalação, baixe e instale a chave pública da VMware para o servidor de destino. Se você já verificou a assinatura digital do arquivo de instalação, não é necessário verificá-la novamente durante a instalação. Consulte [Baixe e instale a chave pública da VMware](#).

## Procedimentos

- 1 Faça login no servidor de destino como **raiz**.

- 2 Baixe o arquivo de instalação para o servidor de destino.

Se você comprou o software na mídia, copie o arquivo de instalação para um local que seja acessível ao servidor de destino.

- 3 Verifique se a soma de verificação do download corresponde à soma de verificação lançada na página de download.

Os valores para as somas de verificação MD5 e SHA1 são lançados na página de download. Use a ferramenta adequada para verificar se a soma de verificação do arquivo de instalação baixado corresponde à soma de verificação mostrada na página de download. Um comando do Linux da seguinte forma exibe a soma de verificação para o *installation-file*.

```
[root@cell1 /tmp]# md5sum installation-file
```

O comando retorna a soma de verificação do arquivo de instalação que deve corresponder à soma de verificação MD5 da página de download.

- 4 Certifique-se de que o arquivo de instalação seja executável.

O arquivo de instalação requer a permissão de execução. Para ter certeza de que ele tem essa permissão, abra uma janela de console, shell ou terminal e execute o seguinte comando do Linux, onde o *arquivo de instalação* é o nome do caminho completo para o arquivo de instalação do vCloud Director.

```
[root@cell1 /tmp]# chmod u+x installation-file
```

- 5 Execute o arquivo de instalação.

Para executar o arquivo de instalação, insira o nome do caminho completo, por exemplo:

```
[root@cell1 /tmp]# ./installation-file
```

O arquivo inclui um script de instalação e um pacote RPM incorporado.

---

**Observação** Você não pode executar o arquivo de instalação de um diretório cujo nome do caminho inclui caracteres de espaço incorporado.

---

Se você não instalou a chave pública da VMware no servidor de destino, o instalador imprime um aviso da seguinte forma:

```
warning: installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

O instalador realiza as seguintes ações.

- a Verifica se o host atende a todos os requisitos.
- b Verifica a assinatura digital no arquivo de instalação.
- c Cria o usuário e grupo do vcloud.
- d Desempacota o pacote RPM do vCloud Director.
- e Instala o software.

Quando a instalação estiver concluída, o instalador solicitará que você execute o script de configuração, que configura as conexões de rede e do banco de dados.

- 6** Selecione se deseja executar o script de configuração.
  - a Para executar o script de configuração em um modo interativo, insira **y** e pressione Enter.
  - b Para executar o script de configuração mais tarde em um modo interativo ou autônomo, insira **n** e pressione Enter.

## Configurar as conexões de rede e banco de dados

Depois de instalar o vCloud Director no primeiro membro do grupo de servidores, você deve executar o script de configuração que cria as conexões de rede e banco de dados para essa célula. O script cria um arquivo de resposta que você deve usar ao configurar membros adicionais do grupo de servidores.

Todos os membros do grupo de servidores do vCloud Director compartilham a conexão de banco de dados e outros detalhes de configuração. Quando você executa o script de configuração no primeiro membro do grupo de servidores do vCloud Director, o script cria um arquivo de resposta que preserva informações de conexões de banco de dados para uso em instalações de servidor subsequentes.

Você pode executar o script de configuração em um modo interativo ou um modo autônomo. Para uma configuração interativa, você executa o comando sem opções e o script solicita as informações de configuração necessárias. Para uma configuração autônoma, você fornece as informações de configuração usando as opções de comando.

Se você quiser usar um único endereço IP com duas portas diferentes para o serviço HTTP e o serviço de proxy de console, deverá executar o script de configuração em um modo autônomo.

**Observação** A ferramenta de gerenciamento de células inclui subcomandos que você pode usar para alterar os detalhes de conexão da rede e do banco de dados configurados inicialmente. As alterações feitas usando esses subcomandos são gravadas no arquivo de configuração global e no arquivo de resposta. Para obter informações sobre como usar a ferramenta de gerenciamento de célula, consulte [Capítulo 10 Referência da ferramenta de gerenciamento de células](#).

#### Pré-requisitos

- Para uma configuração interativa, revise [Referência de configuração interativa](#).
- Para uma configuração autônoma, revise [Referência de configuração autônoma](#).
- Para uma configuração autônoma, verifique se o valor da variável de ambiente VCLLOUD\_HOME está definido para o nome do caminho completo do diretório no qual vCloud Director está instalado. Normalmente, esse valor é /opt/vmware/vcloud-director.

#### Procedimentos

1 Faça login no servidor vCloud Director como raiz.

2 Execute o comando configure:

- Para um modo interativo, execute o comando e, nos prompts, forneça as informações necessárias.

```
/opt/vmware/vcloud-director/bin/configure
```

- Para um modo autônomo, execute o comando com opções e argumentos apropriados.

```
/opt/vmware/vcloud-director/bin/configure options -unattended
```

O script valida as informações e, em seguida:

- a Inicializa o banco de dados e conecta o servidor a ele.
- b Exibe uma URL na qual você pode se conectar ao assistente de **Configuração do VMware vCloud Director** depois que o serviço do vCloud Director é iniciado.
- c Oferece para iniciar a célula do vCloud Director.

3 (Opcional) Anote a URL do assistente de **Configuração do VMware vCloud Director** e insira y para iniciar o serviço do vCloud Director.

Você pode decidir iniciar o serviço mais tarde executando o comando `service vmware-vcd start`.

## Resultados

As informações de conexão do banco de dados e outras informações reutilizáveis fornecidas durante a configuração são preservadas no arquivo de resposta em `/opt/vmware/vcloud-director/etc/responses.properties` neste servidor. Este arquivo contém informações confidenciais que você deve reutilizar ao adicionar servidores a um grupo de servidores.

## Próximo passo

Salve uma cópia do arquivo de resposta em um local seguro. Restringir o acesso a ele e garanta o backup em um local seguro. Quando você fizer backup do arquivo, evite enviar textos não criptografados em uma rede pública.

Se você planeja adicionar servidores ao grupo de servidores, monte o armazenamento de transferência compartilhada em `/opt/vmware/vcloud-director/data/transfer`.

## Referência de configuração interativa

Quando você executa o script `configure` em um modo interativo, o script solicita as informações a seguir.

Para aceitar um valor padrão, pressione Enter.

**Tabela 5-1. Informações necessárias durante uma configuração de rede e banco de dados interativa**

Informações necessárias	Descrição
Endereço IP do serviço HTTP	O padrão é o primeiro endereço IP disponível.
Endereço IP do serviço de proxy do console	O padrão é o primeiro endereço IP disponível.  <b>Observação</b> Se você quiser usar um único endereço IP com duas portas diferentes para o serviço HTTP e o serviço de proxy de console, deverá executar o script de configuração em um modo autônomo.
Caminho completo para o arquivo de repositório de chaves Java	Por exemplo, <code>/opt/keystore/certificates.ks</code> .
Senha para o repositório de chaves	Consulte <a href="#">Antes de criar certificados SSL para o vCloud Director no Linux</a> .
Senha da chave privada para o certificado SSL HTTP	Consulte <a href="#">Antes de criar certificados SSL para o vCloud Director no Linux</a> .
Senha da chave privada para o certificado SSL do proxy de console	Consulte <a href="#">Antes de criar certificados SSL para o vCloud Director no Linux</a> .



**Tabela 5-1. Informações necessárias durante uma configuração de rede e banco de dados interativa (continuação)**

Informações necessárias	Descrição
Habilitar o log de auditoria remoto para um host syslog	<p>Serviços em todas as mensagens de log de auditoria de célula do vCloud Director para o banco de dados vCloud Director, onde elas são preservadas por 90 dias. Para preservar as mensagens de auditoria por mais tempo, você pode configurar serviços do vCloud Director para enviar mensagens de auditoria para o utilitário do syslog além do banco de dados do vCloud Director.</p> <ul style="list-style-type: none"> <li>■ Para ignorar, pressione Enter.</li> <li>■ Para habilitar, insira o nome do host ou o endereço IP do syslog.</li> </ul>
Se você tiver habilitado o log de auditoria remoto, a porta UDP do host do syslog	Assume 514 como padrão.
Nome do host ou endereço IP do servidor de banco de dados	O servidor que executa o banco de dados.
Porta do banco de dados	O padrão é 5432.
Nome do banco de dados	O padrão é vcloud.
Nome de usuário do banco de dados	Consulte <a href="#">Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux</a> .
Senha do banco de dados	Consulte <a href="#">Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux</a> .
Participar ou não participar do Programa de aperfeiçoamento da experiência do cliente (CEIP) da VMware	<p>Este produto participa do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware. Detalhes referentes à coleta de dados através do CEIP e os fins para os quais ela é utilizada pela VMware estão estabelecidos no Trust &amp; Assurance Center em <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a>. Você pode usar a ferramenta de gerenciamento de células para participar ou sair do CEIP da VMware para este produto a qualquer momento. Consulte <a href="#">Capítulo 10 Referência da ferramenta de gerenciamento de células</a>.</p> <p>Para participar do programa, insira <b>y</b>.</p> <p>Se você preferir não participar do programa CEIP da VMware, insira <b>n</b>.</p>

## Referência de configuração autônoma

Ao executar o script do configure em modo autônomo, você pode fornecer as informações de configuração na linha de comando como opções e argumentos.

Tabela 5-2. Argumentos e opções do utilitário de configuração

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Exibe um resumo das opções e dos argumentos de configuração
<code>--config-file (-c)</code>	Caminho para o arquivo <code>global.properties</code>	As informações que você fornece ao executar o utilitário de configuração são salvas neste arquivo. Se você omitir esta opção, o local padrão é <code>/opt/vmware/vcloud-director/etc/global.properties</code> .
<code>--console-proxy-ip (-cons)</code>	Endereço IPv4, com o número da porta opcional	O sistema usa esse endereço para o serviço de proxy de console do vCloud Director. Por exemplo, <code>10.17.118.159</code> .
<code>--console-proxy-port-https</code>	Inteiro no intervalo de 0 a 65535	Número da porta a ser usada para o serviço de proxy de console do vCloud Director.
<code>--database-ssl</code>	true ou false	Você pode configurar o banco de dados PostgreSQL para exigir uma conexão SSL bem sinalizada do vCloud Director.  Se você deseja configurar o banco de dados PostgreSQL para usar um certificado autoassinado ou privado, consulte <a href="#">Realizar configurações adicionais no banco de dados PostgreSQL externo</a> .
<code>--database-host (-dbhost)</code>	Endereço IP ou nome de domínio completo do host do banco de dados do vCloud Director	Consulte <a href="#">Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux</a> .
<code>--database-name (-dbname)</code>	O nome do serviço de banco de dados	Consulte <a href="#">Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux</a> .
<code>--database-password (-dbpassword)</code>	Senha para o usuário do banco de dados. Ele pode ser nulo.	Consulte <a href="#">Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux</a> .
<code>--database-port (-dbport)</code>	Número da porta usada pelo serviço de banco de dados no host do banco de dados	Consulte <a href="#">Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux</a> .

Tabela 5-2. Argumentos e opções do utilitário de configuração (continuação)

Opção	Argumento	Descrição
<code>--database-type (-dbtype)</code>	O tipo de banco de dados. O tipo com suporte é postgres.	Opcional. O tipo de banco de dados padrão será postgres. Consulte <a href="#">Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux</a> .
<code>--database-user (-dbuser)</code>	Nome de usuário do usuário de banco de dados.	Consulte <a href="#">Configurar um banco de dados PostgreSQL externo para vCloud Director no Linux</a> .
<code>--enable-ceip</code>	true ou false	Este produto participa do Programa de Aperfeiçoamento da Experiência do Cliente (CEIP) da VMware. Detalhes referentes à coleta de dados através do CEIP e os fins para os quais ela é utilizada pela VMware estão estabelecidos no Trust & Assurance Center em <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> . Você pode usar a ferramenta de gerenciamento de células para participar ou sair do CEIP da VMware para este produto a qualquer momento. Consulte <a href="#">Capítulo 10 Referência da ferramenta de gerenciamento de células</a> .
<code>--uuid (-g)</code>	Nenhum	Gera um novo identificador exclusivo para a célula
<code>--primary-ip (-ip)</code>	Endereço IPv4, com o número da porta opcional	O sistema usa esse endereço para o serviço de interface da Web do vCloud Director. Por exemplo, <i>10.17.118.159</i> .
<code>--primary-port-http</code>	Inteiro no intervalo de 0 a 65535	Número da porta a ser usada para conexões HTTP (inseguras) para o serviço de interface da Web do vCloud Director
<code>--primary-port-https</code>	Inteiro no intervalo de 0 a 65535	Número da porta a ser usada para conexões HTTPS (seguras) para o serviço de interface da Web do vCloud Director
<code>--keystore (-k)</code>	Caminho para o armazenamento de chaves Java contendo seus certificados SSL e chaves privadas	Deve ser um nome de caminho completo. Por exemplo, <i>/opt/keystore/certificates.ks</i> .

Tabela 5-2. Argumentos e opções do utilitário de configuração (continuação)

Opção	Argumento	Descrição
<code>--syslog-host (-loghost)</code>	Endereço IP ou nome de domínio completo do host do servidor de syslog	Serviços em todas as mensagens de log de auditoria de célula do vCloud Director para o banco de dados vCloud Director, onde elas são preservadas por 90 dias. Para preservar as mensagens de auditoria por mais tempo, você pode configurar serviços do vCloud Director para enviar mensagens de auditoria para o utilitário do syslog além do banco de dados do vCloud Director.
<code>--syslog-port (-logport)</code>	Inteiro no intervalo de 0 a 65535	A porta na qual o processo do syslog monitora o servidor especificado. O padrão é 514 se não for especificado.
<code>--response-file (-r)</code>	Caminho para o arquivo de resposta	<p>Deve ser um nome de caminho completo. Se não for especificado, o padrão será <code>/opt/vmware/vcloud-director/etc/responses.properties</code>. Todas as informações que você fornece ao executar a configuração é preservada neste arquivo.</p> <p><b>Importante</b> Este arquivo contém informações confidenciais que você deve reutilizar ao adicionar servidores a um grupo de servidores. Preserve o arquivo em um local seguro e disponibilize-o somente quando necessário.</p>
<code>--unattended-installation (-unattended)</code>	Nenhum	Especifica a instalação autônoma.
<code>--keystore-password (-w)</code>	Senha do armazenamento de chaves do certificado SSL	Senha do armazenamento de chaves do certificado SSL.

## Exemplo: Configuração autônoma com dois endereços IP

O seguinte comando executa uma configuração autônoma de um servidor vCloud Director com dois endereços IP diferentes para o serviço HTTP e o serviço de proxy de console.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 -cons 10.17.118.158 \
-dbtype postgres -dbhost 10.150.10.78 -dbname postgresql-db-name -dbuser vcloud --enable-ceip true \
-dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret -loghost 10.150.10.10 -unattended
```

## Exemplo: Configuração autônoma com um endereço IP único

O seguinte comando executa uma configuração autônoma de um servidor vCloud Director com um endereço IP único com duas portas diferentes para o serviço HTTP e o serviço de proxy de console.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 --primary-port-https 9000
-cons 10.17.118.159 \
--console-proxy-port-https 9010 -dbtype postgres -dbhost 10.150.10.78 -dbname postgresql-db-name \
-dbuser vcloud -dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

## Proteger e reusar o arquivo de resposta

Detalhes de conexão de rede e banco de dados que você configura na primeira célula do vCloud Director são salvos em um arquivo de resposta. Este arquivo contém informações confidenciais que você deve reusar ao adicionar servidores ao grupo de servidores. Você deve preservar o arquivo em um local seguro.

O arquivo de resposta é criado em `/opt/vmware/vcloud-director/etc/responses.properties` no primeiro servidor para o qual você configura as conexões de rede e de banco de dados. Ao adicionar servidores ao grupo, você deverá usar uma cópia do arquivo de resposta para fornecer os parâmetros de configuração compartilhados por todos os servidores.

**Importante** A ferramenta de gerenciamento de células inclui subcomandos que você pode usar para alterar os detalhes de conexão da rede e do banco de dados especificados inicialmente. As alterações feitas usando essas ferramentas são gravadas no arquivo de configuração global e no arquivo de resposta. Assim sendo, o arquivo de resposta deve estar disponível (em `/opt/vmware/vcloud-director/etc/responses.properties`) e ser gravável antes que você use qualquer comando que possa modificá-lo.

### Procedimentos

#### 1 Proteja o arquivo de resposta.

Salve uma cópia do arquivo em um local seguro. Restrinja o acesso a ele e garanta o backup em um local seguro. Quando você fizer backup do arquivo, evite enviar texto não criptografado em uma rede pública.

## 2 Reutilize o arquivo de resposta.

- a Copie o arquivo para um local acessível ao servidor que você deseja configurar.

---

**Observação** Você deve instalar o software do vCloud Director em um servidor antes de reutilizar o arquivo de resposta para configurá-lo. Todos os diretórios no caminho do arquivo de resposta devem ser legíveis pelo usuário `vcld`, conforme mostrado neste exemplo.

```
[root@cell1 /tmp]# ls -l responses.properties
-rw----- 1 vcld vcld 418 Jun 8 13:42 responses.properties
```

O instalador cria este usuário e este grupo.

- b Execute o script de configuração, usando a opção `-r` e especificando o caminho do arquivo de resposta.

Faça login como raiz, abra uma janela de console, shell ou terminal e digite:

```
[root@cell1 /tmp]# /opt/vmware/vcloud-director/bin/configure -r /path-to-response-file
```

### Próximo passo

Depois de configurar os servidores adicionais, exclua a cópia do arquivo de resposta usado para configurá-los.

## Instalar o vCloud Director em um membro adicional de um grupo de servidores

Você pode adicionar servidores a um grupo de servidores do vCloud Director a qualquer momento. Como todos os servidores em um grupo de servidores devem ser configurados com os mesmos detalhes de conexão do banco de dados, você deve usar o arquivo de resposta criado quando você criou o primeiro membro do grupo.

---

**Importante** As instalações mistas do vCloud Director no Linux e as implantações de appliance vCloud Director em um único grupo de servidores não têm suporte.

### Pré-requisitos

- Verifique se você pode acessar o arquivo de resposta que foi criado quando você configurou o primeiro membro deste grupo de servidores. Consulte [Configurar as conexões de rede e banco de dados](#).
- Verifique se você montou o armazenamento de transferência compartilhado no primeiro membro do grupo de servidores do vCloud Director em `/opt/vmware/vcloud-director/data/transfer`.

### Procedimentos

- 1 Faça login no servidor de destino como **raiz**.

- 2 Baixe o arquivo de instalação para o servidor de destino.

Se você comprou o software na mídia, copie o arquivo de instalação para um local que seja acessível ao servidor de destino.

- 3 Certifique-se de que o arquivo de instalação seja executável.

O arquivo de instalação requer a permissão de execução. Para ter certeza de que ele tem essa permissão, abra uma janela de console, shell ou terminal e execute o seguinte comando do Linux, onde o *arquivo de instalação* é o nome do caminho completo para o arquivo de instalação do vCloud Director.

```
[root@cell1 /tmp]# chmod u+x installation-file
```

- 4 Execute o arquivo de instalação.

Para executar o arquivo de instalação, insira o nome do caminho completo, por exemplo:

```
[root@cell1 /tmp]# ./installation-file
```

O arquivo inclui um script de instalação e um pacote RPM incorporado.

---

**Observação** Você não pode executar o arquivo de instalação de um diretório cujo nome do caminho inclui caracteres de espaço incorporado.

---

Se você não instalou a chave pública da VMware no servidor de destino, o instalador imprime um aviso da seguinte forma:

```
warning: installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

O instalador realiza as seguintes ações.

- a Verifica se o host atende a todos os requisitos.
- b Verifica a assinatura digital no arquivo de instalação.
- c Cria o usuário e grupo do vcloud.
- d Desempacota o pacote RPM do vCloud Director.
- e Instala o software.

Quando a instalação estiver concluída, o instalador solicitará que você execute o script de configuração, que configura as conexões de rede e do banco de dados.

- 5 Insira **n** e pressione Enter para rejeitar a execução do script de configuração.

Você executa o script de configuração mais tarde, fornecendo o arquivo de resposta como entrada.

- 6 Monte o armazenamento de transferência compartilhado em `/opt/vmware/vcloud-director/data/transfer`.

Todos os servidores do vCloud Director no grupo de servidores devem montar este volume no mesmo ponto de montagem.

- 7 Copie o arquivo de resposta para um local acessível a este servidor.

Todos os diretórios no nome do caminho para o arquivo de resposta devem ser legíveis pela raiz.

- 8 Execute o script de configuração.

- a Execute o comando `configure`, fornecendo o nome do caminho do arquivo de resposta.

```
/opt/vmware/vcloud-director/bin/configure -r /responses.properties
```

O script copia o arquivo de resposta para um local legível pelo `vcloud.vcloud` e executa o script de configuração usando o arquivo de resposta como entrada.

- b Nos prompts, forneça os endereços IP para o HTTP e os serviços de proxy do console.
- c Se o script de configuração não encontrar certificados válidos no nome do caminho salvo no arquivo de resposta, quando solicitado, forneça o nome do caminho para os certificados e as senhas.

O script valida as informações, conecta o servidor ao banco de dados e propõe iniciar a célula do vCloud Director.

- 9 (Opcional) Insira **y** para iniciar o serviço do vCloud Director.

Você pode decidir iniciar o serviço mais tarde executando o comando `service vmware-vcd start`.

#### Próximo passo

Repita esse procedimento para adicionar mais servidores a este grupo de servidores.

Quando os serviços do vCloud Director estão em execução em todos os servidores, você deve inicializar o banco de dados do vCloud Director com uma chave de licença, conta de administrador do sistema e informações relacionadas. Você pode inicializar o banco de dados usando a ferramenta de gerenciamento de célula com o subcomando `system-setup`. Consulte [Configurar uma instalação do vCloud Director](#).



# Implantação do vCloud DirectorAppliance

## 6

Você pode criar um grupo de servidores do vCloud Director implantando uma ou mais instâncias do vCloud DirectorAppliance. Implante o dispositivo do vCloud Director usando o vSphere Client (HTML5) ou o VMware OVF Tool.

---

**Importante** As instalações mistas do vCloud Director no Linux e as implantações de appliance vCloud Director em um único grupo de servidores não têm suporte.

---

O vCloud DirectorAppliance é uma máquina virtual pré-configurada otimizada para executar os serviços do vCloud Director.

O dispositivo é distribuído com um nome do formulário VMware vCloud Director-*v.v.v.v-  
nnnnnn\_OVF10.ova*, onde *v.v.v.v* representa a versão do produto e *nnnnnn* o número da compilação. Por exemplo: VMware vCloud Director-9.7.0.0-9229800\_OVA10.ova.

O pacote do vCloud DirectorAppliance contém os seguintes softwares:

- VMware Photon™ OS
- O grupo de serviços do vCloud Director
- PostgreSQL 10

Os tamanhos de dispositivo do vCloud Director primário-pequeno e em espera-pequeno são adequados para sistemas de laboratório ou de teste. Os tamanhos primário-grande e em espera-grande atendem aos requisitos mínimos de dimensionamento para sistemas de produção. Dependendo da carga de trabalho, talvez seja necessário adicionar recursos adicionais.

---

**Importante** A instalação de qualquer componente de terceiros no dispositivo do vCloud Director não é suportada. Você pode instalar somente componentes com suporte da VMware, de acordo com [Matrizes de interoperabilidade de produto da VMware](#). Por exemplo, você pode instalar uma versão com suporte de um agente de monitoramento do VMware vRealize® Operations Manager™ ou VMware vRealize® Log Insight™.

---

## Configuração do banco de dados do Appliance

A partir da versão 9.7, o vCloud DirectorAppliance inclui um banco de dados PostgreSQL incorporado com a função de alta disponibilidade. Para criar uma implantação do Appliance com um cluster de alta disponibilidade de banco de dados, você deve implantar uma instância do vCloud DirectorAppliance como uma célula primária e duas instâncias como células em espera. Você pode implantar instâncias adicionais do vCloud DirectorAppliance no grupo de servidores como células do aplicativo vCD, que executam apenas o grupo de serviços do vCloud Director sem o banco de dados incorporado. As células do aplicativo vCD conectam-se ao banco de dados na célula primária. Consulte [Implantações de dispositivo e configuração de alta disponibilidade do banco de dados](#).

Por padrão, o dispositivo vCloud Director usa o TLS, no lugar do SSL obsoleto, para conexões de banco de dados, incluindo replicação. Esse recurso está ativo imediatamente após a implantação, usando um certificado PostgreSQL autoassinado. Para usar um certificado assinado de uma autoridade de certificação (CA), consulte [Substituir um certificado de interface de usuário de gerenciamento do dispositivo vCloud Director e PostgreSQL incorporado autoassinado](#).

---

**Observação** O vCloud DirectorAppliance não é compatível com bancos de dados externos.

---

## Configuração da rede do Appliance

A partir da versão 9.7, o vCloud DirectorAppliance é implantado com duas redes, eth0 e eth1, para que você possa isolar o tráfego de HTTP do tráfego do banco de dados. Serviços diferentes escutam em uma ou ambas as interfaces de rede correspondentes.

---

**Observação** As redes eth0 e eth1 devem ser colocadas em sub-redes separadas.

---

Serviço	Porta em eth0	Porta em eth1
SSH	22	22
HTTP	80	N/A
HTTPS	443	N/A
PostgreSQL	N/A	5432
IU de gerenciamento	5480	5480
Proxy do console	8443	N/A
JMX	8998, 8999	N/A
JMS/ActiveMQ	61616	N/A

Após a criação do dispositivo do vCloud Director, você pode usar os recursos de rede do vSphere para adicionar uma nova placa de interface de rede (NIC). Consulte as informações em [Adicionar um adaptador de rede a uma máquina virtual](#) no guia *Administração de máquinas virtuais do vSphere*.

O vCloud Director Appliance oferece suporte à personalização de regras de firewall por usuários usando o iptables. Para adicionar regras personalizadas do iptables, você pode adicionar seus próprios dados de configuração ao final do arquivo `/etc/systemd/scripts/iptables`.

Este capítulo inclui os seguintes tópicos:

- [Implantações de dispositivo e configuração de alta disponibilidade do banco de dados](#)
- [Pré-requisitos para a implantação do appliance do vCloud Director](#)
- [Implantar o dispositivo do vCloud Director usando o vSphere Client](#)
- [Implantação do dispositivo vCloud Director usando o VMware OVF Tool](#)

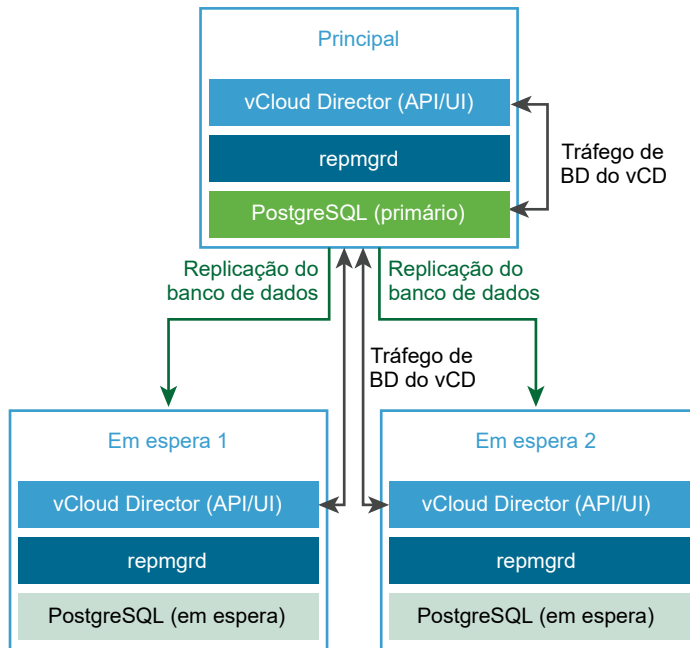
## Implantações de dispositivo e configuração de alta disponibilidade do banco de dados

O dispositivo do vCloud Director usa um banco de dados PostgreSQL incorporado. O banco de dados PostgreSQL incorporado inclui o pacote de ferramentas do Replication Manager (repmgr), que fornece uma função de alta disponibilidade (HA) para um cluster de servidores PostgreSQL. Você pode criar uma implantação de dispositivo com um cluster de alta disponibilidade do banco de dados que fornece recursos de failover para o seu banco de dados do vCloud Director.

Você pode implantar o dispositivo do vCloud Director como uma célula primária, célula em espera ou célula de aplicativo vCD. Consulte [Implantar o dispositivo do vCloud Director usando o vSphere Client](#), [Implantação do dispositivo vCloud Director usando o VMware OVF Tool](#) ou [Implantar o dispositivo vCloud Director com certificados curinga assinados para comunicação HTTPS e via proxy de console](#).

Para configurar o HA para o seu banco de dados do vCloud Director, ao criar o grupo de servidores, você pode configurar um cluster de HA do banco de dados implantando uma instância primária e duas instâncias de espera do dispositivo do vCloud Director.

Figura 6-1. Um cluster de HA do banco de dados do dispositivo do vCloud Director



## Criar uma implantação do dispositivo do vCloud Director com o banco de dados de HA

Para criar um grupo de servidores vCloud Director com uma configuração HA de banco de dados, siga este fluxo de trabalho:

- 1 Implante o dispositivo do vCloud Director como uma célula primária.  
A célula principal é o primeiro membro no grupo de servidores do vCloud Director. O banco de dados incorporado está configurado como o banco de dados do vCloud Director. O nome do banco de dados é `vcld` e o usuário do banco de dados é `vcld`.
- 2 Verifique se a célula primária está funcionando.
  - a Para verificar a integridade do serviço vCloud Director, faça login com as credenciais do **administrador do sistema** para o vCloud Director Service Provider Admin Portal em `https://primary_eth0_ip_address/provider`.
  - b Para verificar a integridade do banco de dados PostgreSQL, faça login como **root** na interface do usuário de gerenciamento de dispositivo em `https://primary_eth1_ip_address:5480`  
O nó primário deve estar em um status de execução.
- 3 Implante duas instâncias do dispositivo do vCloud Director como células em espera.

Os bancos de dados incorporados são configurados em modo de replicação com o banco de dados primário.

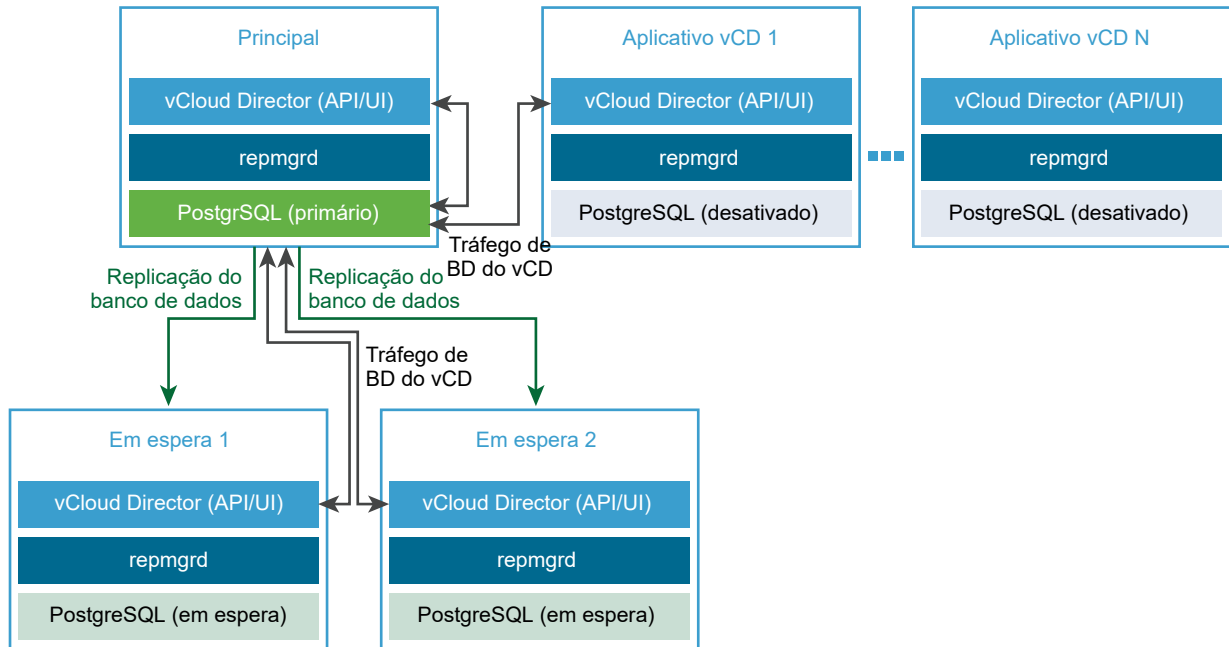
**Observação** Após a implantação do dispositivo em espera inicial, o Replication Manager começa a sincronizar seu banco de dados com o banco de dados do dispositivo primário. Durante esse tempo, o banco de dados do vCloud Director e, portanto, a interface de usuário do vCloud Director não estarão disponíveis.

- 4 Verifique se todas as células no cluster de HA estão em execução.

Consulte [Visualizar o status das células em um cluster de alta disponibilidade de banco de dados](#).

- 5 (Opcional) Implante uma ou mais instâncias do dispositivo do vCloud Director como células do aplicativo vCloud Director.

Os bancos de dados incorporados não são usados. A célula do aplicativo vCloud Director se conecta ao banco de dados primário.



## Criar uma implantação de dispositivo do vCloud Director sem o banco de dados de HA

**Observação** Você pode implantar um cluster vCloud Director com uma célula primária e nenhuma célula de espera ou célula de aplicativo. A VMware não oferece suporte para implantações de célula única em um ambiente de produção, pois elas são uma única fonte de falha de uma perspectiva do banco de dados. As implantações de célula única não recebem suporte para problemas relacionados ao desempenho ou estabilidade.

Para criar um servidor do vCloud Director sem uma configuração de HA do banco de dados, siga este fluxo de trabalho:

- 1 Implante o dispositivo do vCloud Director como uma célula primária.

A célula principal é o primeiro membro no grupo de servidores do vCloud Director. O banco de dados incorporado está configurado como o banco de dados do vCloud Director. O nome do banco de dados é `vc1oud` e o usuário do banco de dados é `vc1oud`.

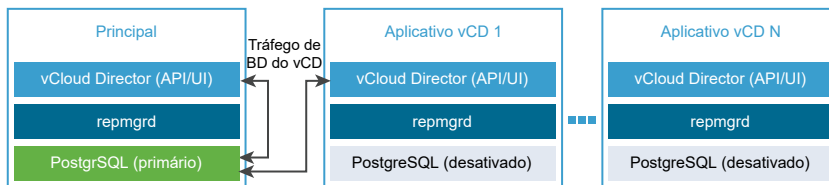
- 2 Verifique se a célula primária está funcionando.

- a Para verificar a integridade do serviço vCloud Director, faça login com as credenciais do **administrador do sistema** para o vCloud Director Service Provider Admin Portal em `https://primary_eth0_ip_address/provider`.
- b Para verificar a integridade do banco de dados PostgreSQL, faça login como **root** na interface do usuário de gerenciamento de dispositivo em `https://primary_eth1_ip_address:5480`

O nó primário deve estar em um status de execução.

- 3 (Opcional) Implante uma ou mais instâncias do dispositivo do vCloud Director como células de aplicativo vCD.

O banco de dados incorporado não é usado. A célula do aplicativo vCD se conecta ao banco de dados de dados primário.



## Pré-requisitos para a implantação do appliance do vCloud Director

Para garantir uma implantação bem-sucedida do appliance do vCloud Director, você deve executar algumas tarefas e pré-verificações antes de iniciar a implantação.

- Verifique se você tem acesso ao arquivo `.ova` do vCloud Director.
- Antes de implantar o appliance primário, prepare um armazenamento do serviço de transferência compartilhada NFS. Consulte [Preparando o armazenamento do servidor de transferência](#).

---

**Observação** O armazenamento do serviço de transferência compartilhada deve conter um arquivo `responses.properties` ou um diretório `appliance-nodes`.

---

- [Instalar e configurar um agente RabbitMQ AMQP](#).

## Métodos de implantação do dispositivo vCloud Director

- [Implantar o dispositivo do vCloud Director usando o vSphere Client](#)
- [Implantação do dispositivo vCloud Director usando o VMware OVF Tool](#)
- [Implantar o dispositivo vCloud Director com certificados curinga assinados para comunicação HTTPS e via proxy de console](#)

## Implantar o dispositivo do vCloud Director usando o vSphere Client

Você pode implantar o dispositivo do vCloud Director como um modelo OVF usando o vSphere Client (HTML5).

Você deve implantar o primeiro membro de um grupo de servidores do vCloud Director como uma célula principal. Pode implantar um membro subsequente de um grupo de servidores do vCloud Director como uma célula de aplicativo em espera ou vCD. Consulte [Implantações de dispositivo e configuração de alta disponibilidade do banco de dados](#).

---

**Importante** As instalações mistas do vCloud Director no Linux e as implantações de appliance vCloud Director em um único grupo de servidores não têm suporte.

Ao adicionar outros dispositivos ou dispositivos de substituição a um cluster de banco de dados, a vCPU e a RAM devem corresponder às das células primária e em espera existentes nesse cluster.

A versão OVA do modo de espera recém-implantado deve ser a mesma que a dos dispositivos existentes no cluster. Para visualizar a versão dos dispositivos em execução, consulte as informações em Sobre na UI de gerenciamento do dispositivo. O dispositivo é distribuído com um nome do formulário VMware Cloud Director-*v.v.v.v-nnnnnn\_OVF10.ovf*, onde *v.v.v.v* representa a versão do produto e *nnnnnn* o número da compilação. Por exemplo: VMware Cloud Director-10.0.0.0-9229800\_OVA10.ovf.

---

Para obter informações sobre como implantar modelos do OVF em vSphere, consulte *Administração da máquina virtual vSphere*.

Como alternativa, você pode implantar o dispositivo usando o VMware OVF Tool. Consulte [Implantação do dispositivo vCloud Director usando o VMware OVF Tool](#).

---

**Observação** Não há suporte para a implantação do vCloud DirectorAppliance em vCloud Director.

---

## Pré-requisitos

Consulte [Pré-requisitos para a implantação do appliance do vCloud Director](#).

## Procedimentos

### 1 Diretrizes de dimensionamento de dispositivos do vCloud Director

Dependendo das suas necessidades, você pode ter configurações diferentes do seu grupo de servidores com base no dispositivo do vCloud Director e tamanhos diferentes das instâncias do dispositivo virtual do vCloud Director.

### 2 Iniciar a implantação do dispositivo do vCloud Director

Para iniciar a implantação do dispositivo, abra o assistente de implantação no vSphere Web Client (Flex) ou no vSphere Client (HTML5).

### 3 Personalizar o dispositivo do vCloud Director e concluir a implantação

Para configurar os detalhes do vCloud Director, personalize o modelo do dispositivo.

## Próximo passo

- Configure o endereço de proxy do console público, pois o vCloud DirectorAppliance usa o NIC do seu eth0 com a porta personalizada 8443 para o serviço de proxy do console. Consulte [Personalizar endereços públicos](#).
- Para adicionar membros ao grupo de servidores do vCloud Director, repita o procedimento.
- Para inserir a chave de licença, faça login no vCloud Director Service Provider Admin Portal.
- Para substituir o certificado autoassinado criado durante a primeira inicialização do dispositivo, você pode [Criar um armazenamento de chaves de certificados SSL assinado por CA para o vCloud Director no Linux](#).

## Diretrizes de dimensionamento de dispositivos do vCloud Director

Dependendo das suas necessidades, você pode ter configurações diferentes do seu grupo de servidores com base no dispositivo do vCloud Director e tamanhos diferentes das instâncias do dispositivo virtual do vCloud Director.

## Visão geral

Para garantir que o cluster possa oferecer suporte a um failover automatizado se ocorrer uma falha na célula primária, a implantação mínima do vCloud Director deve consistir em uma célula primária e duas células em espera. O ambiente permanecerá disponível em qualquer cenário de falha no qual uma das células ficar offline por qualquer motivo. Se ocorrer uma falha em espera, até que você reimplante a célula com falha, o cluster operará em um estado totalmente funcional com uma certa degradação do desempenho. Consulte [Implantações de dispositivo e configuração de alta disponibilidade do banco de dados](#).



O dispositivo do vCloud Director tem quatro tamanhos que você pode selecionar durante a implantação: Pequeno, Médio, Grande e Extra Grande (VVD). O tamanho de dispositivo Pequeno é adequado para avaliação em laboratório, e este documento não fornece orientação sobre a configuração de dispositivos Pequenos. A tabela de opções de tamanho fornece as especificações para as opções restantes e os casos de uso mais adequados para um ambiente de produção. A configuração Extragrande corresponde ao perfil de escala do [VMware Validated Designs \(VVD\) for Cloud Providers](#).

Para criar tamanhos personalizados maiores, os **administradores de sistemas** podem ajustar o tamanho das células implantadas.

A menor configuração recomendada para implantações de produção é uma implantação de três nós de dispositivos virtuais de tamanho Médio.

**Observação** Você pode implantar um cluster vCloud Director com uma célula primária e nenhuma célula de espera ou célula de aplicativo. A VMware não oferece suporte para implantações de célula única em um ambiente de produção, pois elas são uma única fonte de falha de uma perspectiva do banco de dados. As implantações de célula única não recebem suporte para problemas relacionados ao desempenho ou estabilidade.

## Opções de tamanho de dispositivos do vCloud Director

Você pode usar a seguinte orientação de decisão para estimar o tamanho do equipamento para o seu ambiente.

	Médio	Grande	Extragrande (VVD)
Casos de uso recomendados	Ambientes de produção pequenos ou de laboratório	Ambiente de produção	Produção com integrações e monitoramento de API
Implantação do vRealize Operations Management Pack no ambiente do vCloud Director	Não	Não	Sim
Ativação de métricas de VM do Cassandra no vCloud Director	Não	Não	Sim
Número aproximado de usuários ou clientes simultâneos que acessam a API durante um período de pico de 30 minutos.	< 50	< 100	< 100
VMs gerenciadas	5.000	5.000	15.000

## Definições de configuração

**Observação** Os dispositivos `primary-large` e `standby-large` do vCloud Director 9.7 e posterior, por padrão, não têm as 16 vCPUs necessárias para uma configuração de cluster HA Grande. Se você quiser ter uma configuração de dispositivo do vCloud Director Grande, após a implantação, deverá alterar manualmente as vCPUs de célula primária e em espera para 16.

	Médio	Grande	Extragrande (VVD)
Configuração de cluster de HA	1 célula primária + 2 células em espera	1 célula primária + 2 células em espera + 1 célula de aplicativo	1 célula primária + 2 células em espera + 2 células de aplicativo
Célula primária ou em espera de vCPUs	8	16	24
Célula de aplicativo de vCPUs	N/A	8	8
Célula primária ou em espera de RAM	16 GB	24 GB	32 GB
Célula de aplicativo de RAM	N/A	8	8
Relação entre vCPU e núcleos físicos	1:1	1:1	1:1
Personalização do PostgreSQL em células primárias e em espera	shared_buffers = '3GB'; effective_cache_size = '9GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '8';	shared_buffers = '5GB'; effective_cache_size = '15GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '16';	shared_buffers = '7GB'; effective_cache_size = '21GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '24';

### Como detectar se o sistema está subdimensionado

Em uma célula do vCloud Director, o uso de CPU ou memória cresce e atinge um platô em um nível alto, ou seja, um nível próximo à capacidade máxima. A célula do vCloud Director também pode perder a conexão com o banco de dados.

### Como detectar se o número de células do sistema é insuficiente

Nos arquivos `vcloud-container-debug.log` e `cell-runtime.log` de qualquer uma das células do vCloud Director, você vê entradas semelhantes a `org.apache.tomcat.jdbc.pool.PoolExhaustedException: [pool-jetty-XXXXX] Timeout: Pool empty. Unable to fetch a connection in 20 seconds, none available.` A célula do vCloud Director também pode perder a conexão com o banco de dados.

**Observação** Com base na configuração da conexão com o banco de dados padrão, todas as configurações estão limitadas a um máximo de seis células do tipo primário, em espera e de aplicativo.

## Como personalizar o dimensionamento do dispositivo

Para personalizar o dimensionamento do dispositivo do vCloud Director para uma das configurações com suporte, depois de executar o implantador de dispositivo do vCloud Director, você deve seguir esse procedimento em todas as células.

- 1 Verifique se você tem o número necessário de células para a configuração selecionada.
- 2 Ajuste a memória e a vCPU de todas as células para corresponder a uma das configurações compatíveis desejadas.

**Importante** A quantidade de RAM e vCPU deve ser a mesma para todas as células primária e em espera.

- 3 Faça login diretamente ou usando um cliente SSH no sistema operacional do dispositivo primário como **root**.
- 4 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 5 Atualize o arquivo de configuração `postgresql.auto.conf` executando os seguintes comandos.

Tipo de configuração	Descrição
Médio	<pre>psql -c "ALTER SYSTEM set shared_buffers = '3GB';" psql -c "ALTER SYSTEM set effective_cache_size = '9GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '8';"</pre>
Grande	<pre>psql -c "ALTER SYSTEM set shared_buffers = '5GB';" psql -c "ALTER SYSTEM set effective_cache_size = '15GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '16';"</pre>
Extragrande	<pre>psql -c "ALTER SYSTEM set shared_buffers = '7GB';" psql -c "ALTER SYSTEM set effective_cache_size = '21GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '24';"</pre>

6 Retorne ao usuário **root** executando o comando `exit`.

7 Reinicie o processo `vpostgres`.

```
systemctl restart vpostgres
```

8 Altere o usuário para **postgres** novamente.

```
sudo -i -u postgres
```

9 Para cada nó em espera, copie o arquivo `postgresql.auto.conf` para o nó e reinicie o processo `vpostgres`.

a Copie `postgresql.auto.conf` do nó primário para o nó em espera.

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
```

b Reinicie o processo `vpostgres`.

```
systemctl restart vpostgres
```

Para adaptar o dimensionamento do dispositivo do vCloud Director para uma configuração personalizada, depois de executar o implantador de dispositivo do vCloud Director, você deve seguir esse procedimento em todas as células.

1 Faça login diretamente ou usando um cliente SSH no sistema operacional do dispositivo primário como **root**.

2 Para visualizar e anotar as informações da vCPU, execute o seguinte comando.

```
grep -c processor /proc/cpuinfo
```

3 Para exibir e anotar as informações da RAM, execute o seguinte comando.

A RAM relatada abaixo está em KB, e você deve converter esse número em GB dividindo por 1.024.000.

```
cat /proc/meminfo | grep MemTotal | cut -dk -f1 | awk '{print int($2/1024000)}'
```

4 Calcule o valor de `shared_buffers` para ser um quarto da RAM total menos 4 GB.

$shared\_buffers = 0,25 * (total\ de\ RAM - 4\ GB)$

5 Calcule o valor de `effective_cache_size` para ser três quartos da RAM total menos 4 GB.

$effective\_cache\_size = 0,75 * (total\ de\ RAM - 4\ GB)$

6 Calcule o valor de `max_worker_processes` para ser o número de vCPUs.

7 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 8 Atualize o arquivo de configuração `postgresql.auto.conf` executando os seguintes comandos e substituindo os valores calculados.

```
psql -c "ALTER SYSTEM set shared_buffers = 'shared_buffers value';"
psql -c "ALTER SYSTEM set effective_cache_size = 'effective_cache_size value';"
psql -c "ALTER SYSTEM set work_mem = '8MB';"
psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"
psql -c "ALTER SYSTEM set max_worker_processes= 'max_worker_processes value';"
```

- 9 Retorne ao usuário **root** executando o comando `exit`.
- 10 Reinicie o processo `vpostgres`.

```
systemctl restart vpostgres
```

- 11 Altere o usuário para **postgres** novamente.

```
sudo -i -u postgres
```

- 12 Para cada nó em espera, copie o arquivo `postgresql.auto.conf` para o nó e reinicie o processo `vpostgres`.

- a Copie `postgresql.auto.conf` do nó primário para o nó em espera.

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@standby-node-  
address:/var/vmware/vpostgres/current/pgdata/
```

- b Reinicie o processo `vpostgres`.

```
systemctl restart vpostgres
```

## Iniciar a implantação do dispositivo do vCloud Director

Para iniciar a implantação do dispositivo, abra o assistente de implantação no vSphere Web Client (Flex) ou no vSphere Client (HTML5).

### Procedimentos

- 1 No vSphere Web Client ou no vSphere Client, clique com o botão direito do mouse em um objeto de inventário e clique em **Implantar Modelo OVF**.
- 2 Insira o caminho para o arquivo `.ova` do vCloud Director e clique em **Avançar**.
- 3 Insira um nome para a máquina virtual e navegue no repositório do vCenter Server para selecionar um centro de dados ou uma pasta onde implementar o dispositivo e clique em **Avançar**.
- 4 Selecione um cluster ou host do ESXi no qual o dispositivo será implantado e clique em **Avançar**.
- 5 Revise os detalhes do modelo e clique em **Avançar**.
- 6 Leia e aceite os contratos de licença e clique em **Próximo**.

## 7 Selecione o tipo e o tamanho da implantação e clique em **Próximo**.

Os tamanhos de dispositivo do vCloud Director primário-pequeno e em espera-pequeno são adequados para sistemas de laboratório ou de teste. Os tamanhos primário-grande e em espera-grande atendem aos requisitos mínimos de dimensionamento para sistemas de produção. Dependendo da carga de trabalho, talvez seja necessário adicionar recursos adicionais.

Opção	Descrição
<b>Primária-pequena</b>	<p>Implanta o dispositivo com 12 GB de RAM e 2 vCPUs como o primeiro membro em um grupo de servidores do vCloud Director.</p> <p>O banco de dados incorporado na célula primária é configurado como o banco de dados do vCloud Director. O nome do banco de dados é vcloud e o usuário do banco de dados é vcloud.</p>
<b>Primária-grande</b>	<p>Implanta o dispositivo com 24 GB de RAM e 4 vCPUs como o primeiro membro em um grupo de servidores do vCloud Director.</p> <p>O banco de dados incorporado na célula primária é configurado como o banco de dados do vCloud Director. O nome do banco de dados é vcloud e o usuário do banco de dados é vcloud.</p>
<b>Em espera-pequena</b>	<p>Usado para ingressar em uma célula primária-pequena em um cluster de alta disponibilidade (HA) do banco de dados.</p> <p>Implanta o dispositivo com 12 GB de RAM e 2 vCPUs como o segundo ou terceiro membro de um grupo de servidores do vCloud Director com uma configuração de alta disponibilidade de banco de dados.</p> <p>O banco de dados incorporado em uma célula em espera é configurado em um modo de replicação com o banco de dados primário.</p>
<b>Em espera-grande</b>	<p>Usado para ingressar em uma célula primária-grande em um cluster de alta disponibilidade do banco de dados.</p> <p>Implanta o dispositivo com 24 GB de RAM e 4 vCPUs como o segundo ou terceiro membro de um grupo de servidores do vCloud Director com uma configuração de alta disponibilidade de banco de dados.</p> <p>O banco de dados incorporado em um dispositivo em espera é configurado em um modo de replicação com o banco de dados primário.</p>
<b>Aplicativo de célula do vCD</b>	<p>Implanta o dispositivo com 8 GB de RAM e 2 vCPUs como um membro subsequente em um grupo de servidores do vCloud Director.</p> <p>O banco de dados incorporado em uma célula de aplicativo vCD não é usado. A célula do aplicativo vCD se conecta ao banco de dados primário.</p>

**Importante** As células primária e em espera em um grupo de servidores do vCloud Director devem ter o mesmo tamanho. Um cluster de alta disponibilidade de banco de dados pode consistir em uma célula primária-pequena e duas em espera-pequenas, ou consistir em uma única célula primária grande e em duas em espera-grandes.

Após a implantação, você poderá reconfigurar o tamanho do dispositivo.

- 8 Selecione o formato do disco e o repositório de dados para os arquivos de configuração da máquina virtual e os discos virtuais, e clique em **Avançar**.

Os formatos espessos melhoram o desempenho e os formatos finos economizam espaço de armazenamento.

- 9 Nos menus suspensos nas células **Rede de Destino**, selecione as redes de destino para os NICs eth1 e eth0 do dispositivo.

---

**Importante** As duas redes de destino devem ser diferentes.

---

- 10 Nos menus suspensos **Configurações de Alocação de IP**, selecione alocação de IP **Estática-manual** e o protocolo **IPv4**.

- 11 Clique em **Avançar**.

Você é redirecionado para a página **Personalizar modelo** para configurar os detalhes do vCloud Director.

## Personalizar o dispositivo do vCloud Director e concluir a implantação

Para configurar os detalhes do vCloud Director, personalize o modelo do dispositivo.

Ao personalizar o dispositivo do vCloud Director, você define as configurações do dispositivo, o banco de dados e as propriedades de rede. Você define as configurações iniciais do sistema somente ao implantar um dispositivo primário, que é o primeiro membro de um grupo de servidores.

---

**Observação** Somente a [Etapa 3](#) desse procedimento é opcional. Você deve concluir todas as outras etapas para personalizar o dispositivo do vCloud Director.

---

### Procedimentos

- 1 Na seção **Configurações do dispositivo do VCD**, configure os detalhes do dispositivo.

Configuração	Descrição
<b>Servidor NTP</b>	O nome do host ou o endereço IP do servidor NTP a ser usado.
<b>Senha raiz inicial</b>	A senha raiz inicial do dispositivo. Deve conter pelo menos oito caracteres, um caractere maiúsculo, um caractere minúsculo, um dígito numérico e um caractere especial.  <b>Importante</b> A senha raiz inicial se torna a senha do armazenamento de chaves. A implantação do cluster requer que todas as células tenham a mesma senha raiz durante a implantação inicial. Após a conclusão do processo de inicialização, você poderá alterar a senha raiz em qualquer célula desejada.  <b>Observação</b> O assistente de implantação do OVF não valida a senha raiz inicial em relação aos critérios de senha.

Configuração	Descrição
<b>Expirar a senha raiz após o primeiro login</b>	Se você quiser continuar usando a senha inicial após o primeiro login, deverá verificar se a senha inicial atende aos critérios da senha raiz. Para continuar usando a senha raiz inicial após o primeiro login, desmarque essa opção.
<b>Ativar o SSH</b>	Desativado por padrão.
<b>Montagem do NFS para a localização do arquivo de transferência</b>	Consulte <a href="#">Preparando o armazenamento do servidor de transferência</a> .

**Observação** Para obter informações sobre como alterar a data, a hora ou o fuso horário do dispositivo, consulte <https://kb.vmware.com/kb/59674>.

- Se você estiver implantando o primeiro membro de um grupo de servidores, na seção **Configurar VCD - obrigatório apenas para dispositivos "primários"**, digite os detalhes do banco de dados, crie a conta do **administrador do sistema** e defina as configurações do sistema.

O nome do banco de dados é vcloud e o usuário do banco de dados é vcloud.

Configuração	Descrição
<b>A senha do banco de dados 'vcloud' para o usuário 'vcloud'</b>	A senha para o usuário do banco de dados <b>vcloud</b> .
<b>Nome do Usuário Administrador</b>	O nome de usuário para a conta do <b>administrador do sistema</b> . O padrão é administrator.
<b>Nome Completo do Administrador</b>	O nome completo do <b>administrador do sistema</b> . O padrão é vCD Admin.
<b>Senha do usuário administrador</b>	A senha para a conta do <b>administrador do sistema</b> .
<b>E-mail do administrador</b>	O endereço de e-mail do <b>administrador do sistema</b> .
<b>Nome do sistema</b>	O nome da pasta do vCenter Server a criar para esta instalação do vCloud Director. O padrão é vcd1.
<b>ID de Instalação</b>	A ID para esta instalação do vCloud Director a ser usada quando você cria os endereços MAC para NICs virtuais. O padrão é 1. Se você planeja criar redes estendidas entre instalações do vCloud Director em implantações em vários sites, considere definir um ID exclusivo de instalação para cada instalação do vCloud Director.

- (Opcional) Na seção **Propriedades de rede adicionais**, se necessário na sua topologia de rede, digite as rotas estáticas para as interfaces de rede eth0 e eth1 e clique em **Próximo**.

Se você quiser acessar hosts em uma rota de gateway não padrão, talvez seja necessário fornecer rotas estáticas. Por exemplo, a infraestrutura de gerenciamento é acessível apenas na interface eth1, enquanto o gateway padrão está em eth0. Na maioria dos casos, essa configuração pode permanecer vazia.



As rotas estáticas devem estar em uma lista separada por vírgula das especificações de rota. Uma especificação de rota deve consistir no endereço IP do gateway de destino e, opcionalmente, numa especificação de rede de Roteamento entre domínios sem classificação (CIDR). Por exemplo, **172.16.100.253 172.16.100.0/19, 172.16.200.253**.

- 4 Na seção **Propriedades de rede**, digite os detalhes da rede para os NICs eth0 e eth1 e clique em **Próximo**.

Configuração	Descrição
<b>Gateway Padrão</b>	O endereço IP do gateway padrão para o dispositivo.
<b>Nome de Domínio</b>	O domínio de pesquisa DNS, por exemplo, <i>mydomain.com</i> .
<b>Caminho de Pesquisa de Domínio</b>	Uma lista separada por vírgula ou por espaço de nomes de domínio para pesquisa de nomes de host de dispositivo, por exemplo, <i>subdomínio.exemplo.com</i> .  <b>Observação</b> O nome de domínio que você inseriu na caixa de texto Nome do Domínio é o primeiro elemento na lista de caminhos de pesquisa de domínio.
<b>Servidores de Nome de Domínio</b>	O endereço IP do servidor do nome de domínio para o dispositivo.
<b>Endereço IP de rede eth0</b>	O endereço IP para a interface eth0.
<b>Máscara de rede eth0</b>	A máscara de rede ou o prefixo da interface eth0.
<b>Endereço IP de rede eth1</b>	O endereço IP para a interface eth1.
<b>Máscara de rede eth1</b>	A máscara de rede ou o prefixo da interface eth1.

- 5 Na página **Pronto para Concluir**, revise as definições de configuração para o dispositivo do vCloud Director e clique em **Concluir** para iniciar a implantação.

#### Próximo passo

- Ligue a máquina virtual recém-criada.
- [Alterar o fuso horário do dispositivo do vCloud Director](#)

## Implantação do dispositivo vCloud Director usando o VMware OVF Tool

Você pode implantar o vCloud DirectorAppliance como um modelo OVF usando o VMware OVF Tool.

Você deve implantar o primeiro membro de um grupo de servidores do vCloud Director como uma célula principal. Pode implantar um membro subsequente de um grupo de servidores do vCloud Director como uma célula de aplicativo em espera ou vCD. Consulte [Implantações de dispositivo e configuração de alta disponibilidade do banco de dados](#).

Para obter informações sobre como instalar o OVF Tool, consulte o documento *Notas de versão do VMware OVF Tool*.

Para obter informações sobre como usar o OVF Tool, consulte *Guia do Usuário do OVF Tool*.

**Importante** As instalações mistas do vCloud Director no Linux e as implantações de appliance vCloud Director em um único grupo de servidores não têm suporte.

Ao adicionar outros dispositivos ou dispositivos de substituição a um cluster de banco de dados, a vCPU e a RAM devem corresponder às das células primária e em espera existentes nesse cluster.

A versão OVA do modo de espera recém-implantado deve ser a mesma que a dos dispositivos existentes no cluster. Para visualizar a versão dos dispositivos em execução, consulte as informações em Sobre na UI de gerenciamento do dispositivo. O dispositivo é distribuído com um nome do formulário VMware Cloud Director-*v.v.v.v-nnnnnn\_OVF10.ova*, onde *v.v.v.v* representa a versão do produto e *nnnnnn* o número da compilação. Por exemplo: VMware Cloud Director-10.2.0.0-9229800\_OVA10.ova.

Para obter informações sobre como implantar modelos do OVF em vSphere, consulte *Administração da máquina virtual vSphere*.

Como alternativa, você pode implantar o dispositivo usando o vSphere Client. Consulte [Implantar o dispositivo do vCloud Director usando o vSphere Client](#).

**Observação** Não há suporte para a implantação do vCloud DirectorAppliance em vCloud Director.

Antes de executar o comando de implantação, consulte [Pré-requisitos para a implantação do appliance do vCloud Director](#).

Depois de implantar o Appliance, visualize o arquivo de log da primeira inicialização para consultar as mensagens de erro de aviso. Consulte [Examinar os arquivos de log no vCloud Director Appliance](#).

## Opções de comando e propriedades do ovftool para implantar o vCloud DirectorAppliance

Opção	Valor	Descrição
--noSSLVerify	N/A	Ignora a verificação de SSL para conexões vSphere.
--acceptAllEulas	N/A	Aceita todos os contratos de licença de usuário final (EULAs).
--datastore	<i>target_vc_datastore</i>	O nome do datastore de destino no qual os arquivos de configuração da máquina virtual e os discos virtuais são armazenados.
--allowAllExtraConfig	N/A	Converte todas as opções de configuração extras no formato VMX.

Opção	Valor	Descrição
--net:"eth0 Network"	<i>portgroup_on_vc_for_eth0</i>	A rede de destino para a rede eth0 do Appliance.  <b>Importante</b> Deve ser diferente da rede de destino do eth1.
--net:"eth1 Network"	<i>portgroup_on_vc_for_eth1</i>	A rede de destino para a rede eth1 do Appliance.  <b>Importante</b> Deve ser diferente da rede de destino do eth0.
--name	<i>vm_name_on_vc</i>	O nome da máquina virtual para o Appliance.
--diskMode	thin ou thick	O formato do disco para os arquivos de configuração da máquina virtual e os discos virtuais.
--prop:"vami.ip0.VMware_vCloud_Director"	<i>eth0_ip_address</i>	Endereço IP do eth0. Usado para o acesso à interface do usuário e à API. Nesse endereço, a pesquisa inversa de DNS determina e define o nome do host do dispositivo.
--prop:"vami.ip1.VMware_vCloud_Director"	<i>eth1_ip_address</i>	Endereço IP do eth1. Usado para acessar serviços internos, incluindo o serviço de banco de dados PostgreSQL incorporado.
--prop:"vami.DNS.VMware_vCloud_Director"	<i>dns_ip_address</i>	O endereço IP do servidor do nome de domínio para o dispositivo.
--prop:"vami.domain.VMware_vCloud_Director"	<i>domain_name</i>	O domínio de pesquisa DNS. Aparece como o primeiro elemento no caminho de pesquisa.
--prop:"vami.gateway.VMware_vCloud_Director"	<i>gateway_ip_address</i>	O endereço IP do gateway padrão para o dispositivo.
--prop:"vami.netmask0.VMware_vCloud_Director"	<i>Máscara de rede</i>	A máscara de rede ou o prefixo da interface eth0.
--prop:"vami.netmask1.VMware_vCloud_Director"	<i>Máscara de rede</i>	A máscara de rede ou o prefixo da interface eth1.
--prop:"vami.searchpath.VMware_vCloud_Director"	<i>list_of_domain_names</i>	O caminho de pesquisa do domínio do dispositivo.  Uma lista de nomes de domínio separados por vírgulas ou espaços.
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"	<i>true ou false</i>	Habilita ou desabilita o acesso <b>raiz</b> do SSH ao dispositivo.
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"	<i>true ou false</i>	Determina se deve-se continuar ou não o uso da senha inicial após o primeiro login.

Opção	Valor	Descrição
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"	<code>nfs_mount_path</code>	O endereço IP e o caminho de exportação do servidor NFS externo. Usado somente para uma célula primária.
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"	<code>ntp_server_ip_address</code>	O endereço IP do servidor de horário.
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"	<code>varoot_password</code>	A senha raiz inicial do dispositivo. Deve conter pelo menos oito caracteres, um caractere maiúsculo, um caractere minúsculo, um dígito numérico e um caractere especial.  <b>Importante</b> A senha raiz inicial se torna a senha do armazenamento de chaves. A implantação do cluster requer que todas as células tenham a mesma senha raiz durante a implantação inicial. Após a conclusão do processo de inicialização, você poderá alterar a senha raiz em qualquer célula desejada.
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"	<code>db_password</code>	A senha do banco de dados do usuário do <b>vcloud</b> . Usado somente para uma célula primária.
--prop:"vcloudwiz.admin_email.VMware_vCloud_Director"	<code>admin_email_address</code>	O endereço de email da conta do <b>administrador do sistema</b> . Usado somente para uma célula primária.
--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director"	<code>admin_firstname</code>	O nome da conta do <b>administrador do sistema</b> . Usado somente para uma célula primária.
--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director"	<code>admin_password</code>	A senha para a conta do <b>administrador do sistema</b> . Usado somente para uma célula primária.
--prop:"vcloudwiz.admin_undef.VMware_vCloud_Director"	<code>admin_username</code>	O nome de usuário para a conta do <b>administrador do sistema</b> . Usado somente para uma célula primária.
--prop:"vcloudwiz.inst_id.VMware_vCloud_Director"	<code>inst_id</code>	A ID de instalação do vCloud Director. Usado somente para uma célula primária.
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"	<code>sys_name</code>	O nome da pasta do vCenter Server a criar para esta instalação do vCloud Director.

Opção	Valor	Descrição
<code>--prop:"vcloudnet.routes0.VMware_vCloud_Director</code>	<code>ip_address1 cidr, ip_address2, ...</code>	Opcional. Rotas estáticas para a interface do eth0. Deve ser uma lista das especificações de rota separadas por vírgulas. Uma especificação de rota deve consistir em um endereço IP do gateway e, opcionalmente, uma especificação de rede Classless Inter-Domain Routing (CIDR) (prefixo/bits). Por exemplo, <b>172.16.100.253 172.16.100/19, 172.16.200.253</b> .
<code>--prop:"vcloudnet.routes1.VMware_vCloud_Director</code>	<code>ip_address1 cidr, ip_address2, ...</code>	Opcional. Rotas estáticas para a interface do eth1. Deve ser uma lista das especificações de rota separadas por vírgulas. Uma especificação de rota deve consistir em um endereço IP do gateway e, opcionalmente, uma especificação de rede Classless Inter-Domain Routing (CIDR) (prefixo/bits). Por exemplo, <b>172.16.100.253 172.16.100/19, 172.16.200.253</b> .

Opção	Valor	Descrição
--deploymentOption	primary-small,primary-large, standby-small, standby-large ou cell	<p>O tipo e o tamanho do dispositivo que você deseja implantar.</p> <p>Os tamanhos de dispositivo do primário-pequeno e em espera-pequeno são adequados para sistemas de laboratório ou de teste. Os tamanhos primário-grande e em espera-grande atendem aos requisitos mínimos de dimensionamento para sistemas de produção. Dependendo da carga de trabalho, talvez seja necessário adicionar recursos adicionais.</p> <ul style="list-style-type: none"> <li>■ O primary-small implanta o dispositivo com 12 GB de RAM e 2 vCPUs como o primeiro membro de um grupo de servidores do vCloud Director. O banco de dados incorporado na célula primária é configurado como o banco de dados do vCloud Director. O nome do banco de dados é vcloud e o usuário do banco de dados é vcloud.</li> <li>■ O primary-large implanta o dispositivo com 24 GB de RAM e 4 vCPUs como o primeiro membro de um grupo de servidores do vCloud Director. O banco de dados incorporado na célula primária é configurado como o banco de dados do vCloud Director. O nome do banco de dados é vcloud e o usuário do banco de dados é vcloud.</li> <li>■ O standby-small implanta o dispositivo com 12 GB de RAM e 2 vCPUs como o segundo ou o terceiro membro de um grupo de servidores do vCloud Director com uma configuração de alta disponibilidade de banco de dados. O banco de dados incorporado em uma célula em espera é configurado em um modo de replicação com o banco de dados primário.</li> <li>■ O standby-large implanta o dispositivo com 24 GB de RAM e 4 vCPUs como o segundo ou o terceiro membro de um grupo de servidores do vCloud</li> </ul>

Opção	Valor	Descrição
		<p>Director com uma configuração de alta disponibilidade de banco de dados. O banco de dados incorporado em uma célula em espera é configurado em um modo de replicação com o banco de dados primário.</p> <ul style="list-style-type: none"> <li>■ O <code>cell</code> implanta o dispositivo com 8 GB de RAM e 2 vCPUs como um membro subsequente em um grupo de servidores do vCloud Director. O banco de dados incorporado em uma célula de aplicativo vCD não é usado. A célula do aplicativo vCD se conecta ao banco de dados primário.</li> </ul> <p><b>Importante</b> As células primária e em espera em um grupo de servidores do vCloud Director devem ter o mesmo tamanho. Um cluster de alta disponibilidade de banco de dados pode consistir em uma célula primária-pequena e duas em espera-pequenas, ou consistir em uma única célula primária grande e em duas em espera-grandes.</p> <p>Após a implantação, você poderá reconfigurar o tamanho do dispositivo.</p>
<code>--powerOn</code>	<code>path_to_ova</code>	Liga a máquina virtual após a implantação.

## Um exemplo de comando para a implantação do vCloud Director Appliance primário

**Importante** Antes de executar o comando do VMware OVF Tool, substitua as senhas `vcloudapp.varoot-passwordVMware_vCloud_Director`, `vcloudconf.db_pwdVMware_vCloud_Director` e `vcloudconf.admin_pwd.VMware_vCloud_Director` por suas próprias senhas seguras.

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
```

```
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

## Um exemplo de comando para a implantação do vCloud Director Appliance de espera

**Importante** Antes de executar o comando do VMware OVF Tool, substitua a senha `vcloudapp.varoot-password.VMware_vCloud_Director` pela sua própria senha segura.

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
```



```
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \  
--deploymentOption="standby-small" \  
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \  
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

# Criação e gerenciamento de certificados SSL do dispositivo vCloud Director

## 7

O dispositivo vCloud Director usa SSL para proteger comunicações entre clientes e servidores. Cada dispositivo vCloud Director deve oferecer suporte a dois endpoints SSL diferentes: para HTTPS e para comunicações de proxy do console.

Esses endpoints podem ser endereços IP separados, ou um único endereço IP com duas portas diferentes. Cada endpoint requer seu próprio certificado SSL. Você pode usar o mesmo certificado (por exemplo, um certificado curinga) para ambos os endpoints.

Este capítulo inclui os seguintes tópicos:

- [Implantar o dispositivo vCloud Director com certificados curinga assinados para comunicação HTTPS e via proxy de console](#)
- [Criar e importar certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director](#)
- [Importar chaves privadas e certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director](#)
- [Substituir um certificado de interface de usuário de gerenciamento do dispositivo vCloud Director e PostgreSQL incorporado autoassinado](#)
- [Renovar os certificados do dispositivo vCloud Director](#)

## Implantar o dispositivo vCloud Director com certificados curinga assinados para comunicação HTTPS e via proxy de console

Você pode implantar o dispositivo vCloud Director com certificados curinga assinados. Você pode usar esses certificados para proteger um número ilimitado de servidores que são subdomínios do nome de domínio listado no certificado.

Por padrão, ao implantar dispositivos do vCloud Director, o vCloud Director gera certificados autoassinados e os utiliza para configurar a célula do vCloud Director para comunicação HTTPS ou via proxy de console.

Quando você implanta um dispositivo primário com êxito, a lógica de configuração do dispositivo copia o arquivo `responses.properties` do dispositivo primário para o armazenamento do serviço de transferência compartilhada NFS comum em `/opt/vmware/vcloud-director/data/transfer`. Outros dispositivos implantados para esse grupo de servidores do vCloud Director usam esse arquivo para se configurarem automaticamente. O arquivo `responses.properties` inclui um caminho para o armazenamento de chaves de certificados SSL, que inclui os certificados autoassinados gerados automaticamente `user.keystore.path`. Por padrão, esse caminho é para um arquivo de armazenamento de chaves que é local para cada dispositivo.

Depois de implantar o dispositivo primário, você pode reconfigurá-lo para usar certificados assinados. Para obter mais informações sobre como criar o armazenamento de chaves com certificados assinados, consulte [Criar e importar certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director](#).

Se os certificados assinados que você usar no dispositivo primário vCloud Director forem certificados curinga assinados, eles poderão ser aplicados a todos os outros dispositivos no grupo de servidores do vCloud Director, ou seja, células em espera e células de aplicativo do vCloud Director. Você pode usar a implantação do dispositivo com certificados curinga assinados para comunicação HTTPS e via proxy de console, para configurar as células adicionais com os certificados SSL curinga assinados.

### Pré-requisitos

- Verifique se o armazenamento de chaves que contém os certificados SSL curinga assinados para os aliases HTTPS e de proxy de console está disponível no dispositivo primário, ou seja, `/opt/vmware/vcloud-director/certificates.ks`.
  - Se precisar criar pares de chaves e importar arquivos de certificado assinados por CA, consulte [Criar e importar certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director](#).
  - Se você já tiver sua própria chave privada e arquivos de certificado assinados por CA, consulte [Importar chaves privadas e certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director](#).
- Verifique se a senha privada para as chaves no armazenamento de chaves corresponde à senha do armazenamento de chaves. A senha do armazenamento de chaves deve corresponder à senha raiz inicial usada ao implantar todos os dispositivos, por exemplo,

```
/opt/vmware/vcloud-director/jre/bin/keytool -keypasswd -alias http_or_consoleproxy -keystore /opt/vmware/vcloud-director/certificates.ks -storetype jceks -storepass root-password
```

### Procedimentos

- 1 Copie o novo arquivo `certificates.ks` contendo os certificados corretamente assinados do dispositivo primário para o compartilhamento de transferência em `/opt/vmware/vcloud-director/data/transfer/`.

- 2 Altere as permissões de proprietário e grupo no arquivo de armazenamento de chaves para **vcloud**.

```
chown vcloud.vcloud /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

- 3 Verifique se o proprietário do arquivo de armazenamento de chaves tem permissões de leitura e gravação.

```
chmod 0750 /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

- 4 No dispositivo primário, execute o comando para importar os novos certificados assinados para a instância do vCloud Director.

Esse comando também atualiza o arquivo `responses.properties` no compartilhamento de transferência, modificando a variável `user.keystore.path` de forma que ela aponte para o arquivo de armazenamento de chaves no compartilhamento de transferência.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/data/transfer/certificates.ks --keystore-password root-password
```

- 5 Para que os novos certificados assinados tenham efeito, reinicie o serviço `vmware-vcd` no dispositivo primário.

```
service vmware-vcd restart
```

- 6 Implante a célula em espera e os dispositivos de células de aplicativo usando a senha raiz inicial que corresponde à senha do armazenamento de chaves.

## Resultados

Todos os dispositivos recém-instalados que usam o mesmo armazenamento do serviço de transferência compartilhado NFS são configurados com os mesmos certificados SSL curinga assinados que são usados pelo dispositivo primário.

## Criar e importar certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director

Criar e importar certificados assinados por uma autoridade de certificação (CA) fornece o mais alto nível de confiança para comunicações SSL e ajuda a proteger as conexões dentro da nuvem.

Cada servidor do vCloud Director requer dois certificados SSL para proteger as comunicações entre clientes e servidores. Cada servidor do vCloud Director deve oferecer suporte a dois endpoints SSL diferentes: para HTTPS e para comunicações de proxy do console.

No dispositivo do vCloud Director, esses dois endpoints compartilham o mesmo endereço IP ou nome de host, mas usam duas portas distintas — 443 para HTTPS e 8443 para comunicações de proxy do console. Cada endpoint deve ter seu próprio certificado SSL. Você pode usar o mesmo certificado para ambos os endpoints, por exemplo, usando um certificado curinga.

Os certificados para ambos os endpoints devem incluir um nome distinto X.500 e uma extensão de Nome Alternativo de Requerente X.509

Se você já tiver sua própria chave privada e arquivos de certificado assinados pela autoridade de certificação, siga o procedimento descrito em [Importar chaves privadas e certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director](#).

---

**Importante** Na implantação, o dispositivo do vCloud Director gera certificados autoassinados com um tamanho de chave de 2048 bits. Você deve avaliar os requisitos de segurança da instalação antes de escolher um tamanho de chave apropriado. Tamanhos de chaves menores que 1024 bits não são mais suportados pelo NIST Special Publication 800-131A.

---

A senha do armazenamento de chaves usada neste procedimento é a senha do usuário **root** e é representada como *root\_passwd*.

### Pré-requisitos

Familiarize-se com o comando do `keytool`. Você usa o `keytool` para importar certificados SSL assinados pela CA para o dispositivo do vCloud Director. O vCloud Director coloca uma cópia do `keytool` em `/opt/vmware/vcloud-director/jre/bin/keytool`.

### Procedimentos

- 1 Faça login diretamente ou conecte-se via SSH no console do dispositivo do vCloud Director como **root**.

- 2 Dependendo das necessidades do ambiente, escolha uma das opções a seguir.

Quando você implanta o dispositivo do vCloud Director, o vCloud Director gera automaticamente certificados autoassinados com um tamanho de chave de 2048 bits para o serviço HTTPS e o serviço de proxy do console.

- Se você quiser que sua autoridade de certificação assine os certificados gerados na implantação, pule para a [Etapa Etapa 5](#).
- Se você quiser gerar novos certificados com opções personalizadas, como um tamanho de chave maior, vá para a [Etapa Etapa 3](#).

- 3 Execute o comando para fazer backup do arquivo `certificates.ks` existente.

```
cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
```

- 4 Execute o comando para criar pares de chaves pública/privada para o serviço HTTPS e para o serviço de proxy do console.

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o /opt/vmware/vcloud-director/certificates.ks -w root_passwd
```

O comando cria ou atualiza um armazenamento de chaves em `certificates.ks` com a senha que você especificou. Os certificados são criados usando os valores padrão do comando. Dependendo da configuração de DNS do seu ambiente, o CN (Nome Comum) do emissor é definido como o endereço IP ou o FQDN de cada serviço. O certificado usa o comprimento de chave de 2048 bits padrão e expira um ano após a criação.

---

**Importante** Devido a restrições de configuração no dispositivo do vCloud Director, você deve usar o local `/opt/vmware/vcloud-director/certificates.ks` para o armazenamento de chaves de certificados.

---

**Observação** Use a senha **raiz** do dispositivo como a senha do armazenamento de chaves.

---

- 5 Crie solicitações de assinatura de certificado (CSR) para o serviço HTTPS e para o serviço de proxy do console.

---

**Importante** O dispositivo do vCloud Director compartilha o mesmo endereço IP e nome de host para o serviço HTTPS e o serviço de proxy do console. Por causa disso, os comandos de criação de CSR devem ter o mesmo DNS e IPs para o argumento de extensão do Nome Alternativo da Entidade (SAN).

---

- a Crie uma solicitação de assinatura de certificado no arquivo `http.csr`.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass root_password -certreq -alias http -file http.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

- b Crie uma solicitação de assinatura de certificado no arquivo `consoleproxy.csr`.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass root_password -certreq -alias consoleproxy -file consoleproxy.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

- 6 Envie as solicitações de assinatura de certificado para sua Autoridade de Certificação.

Se a sua autoridade de certificação exigir que você especifique um tipo de servidor da Web, use o Tomcat da Jakarta.

Você obtém os certificados assinados pela CA.

- 7 Copie os certificados assinados por CA, o certificado raiz de CA e quaisquer certificados intermediários para o dispositivo do vCloud Director.

- 8 Execute os comandos para importar os certificados assinados para o armazenamento de chaves JCEKS.

- a Importe o certificado raiz da Autoridade de Certificação do arquivo `root.cer` para o arquivo de armazenamento de chaves `certificates.ks`.

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias root -file root_certificate_file
```

- b Se tiver recebido certificados intermediários, importe-os do arquivo `intermediate.cer` para o arquivo de armazenamento de chaves `certificates.ks`.

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias intermediate -file intermediate_certificate_file
```

- c Importe o certificado do serviço HTTPS.

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias http -file http_certificate_file
```

- d Importe o certificado do serviço de proxy do console.

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias consoleproxy -file console_proxy_certificate_file
```

Os comandos substituem o arquivo `certificates.ks` pelas versões recém-criadas assinadas pela autoridade de certificação dos certificados.

- 9 Para verificar se os certificados estão importados, execute o comando para listar o conteúdo do arquivo do repositório de chaves.

```
keytool -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -list
```

- 10 Execute o comando para importar os certificados para a instância do vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password root_password
```

- 11 Para que os novos certificados assinados tenham efeito, reinicie o serviço do vCloud Director no dispositivo do `vmware-vcd`.

```
service vmware-vcd restart
```

#### Próximo passo

- Se você estiver usando certificados curinga, consulte [Implantar o dispositivo vCloud Director com certificados curinga assinados para comunicação HTTPS e via proxy de console](#).
- Se você não estiver usando certificados curinga, repita esse procedimento em todos os servidores do vCloud Director no grupo de servidores.

- Para obter mais informações sobre como substituir os certificados do banco de dados PostgreSQL incorporado e da interface de usuário de gerenciamento do dispositivo do vCloud Director, consulte [Substituir um certificado de interface de usuário de gerenciamento do dispositivo vCloud Director e PostgreSQL incorporado autoassinado](#).

## Importar chaves privadas e certificados SSL assinados pela autoridade de certificação para o dispositivo do vCloud Director

Se você tiver sua própria chave privada e arquivos de certificado assinados por CA, antes de importar os armazenamentos de chaves para o ambiente do vCloud Director, deverá criar arquivos de armazenamento de chaves nos quais importar os certificados e as chaves privadas para o serviço de proxy de HTTPS e do console.

### Pré-requisitos

- Familiarize-se com o comando do `keytool`. Você usa o `keytool` para importar certificados SSL assinados pela CA para o dispositivo do vCloud Director. O vCloud Director coloca uma cópia do `keytool` em `/opt/vmware/vcloud-director/jre/bin/keytool`.
- Copie os certificados intermediários, o certificado CA raiz, o serviço HTTPS assinado pela CA e as chaves privadas e certificados do serviço do Proxy de Console para o dispositivo.

### Procedimentos

- 1 Faça login diretamente ou conecte-se via SSH no console do dispositivo do vCloud Director como **root**.
- 2 Se você tiver certificados intermediários, execute o comando para combinar o certificado assinado pela CA raiz com os certificados intermediários e criar uma cadeia de certificados.

```
cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
```

- 3 Use o OpenSSL para criar arquivos de armazenamento de chaves PKCS12 intermediários para os serviços de proxy HTTPS e console com a chave privada, a cadeia de certificados, o alias respectivo e especifique uma senha para cada arquivo de armazenamento de chaves.

- a Crie o arquivo de armazenamento de chaves para o serviço HTTPS.

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.pfx -chain
```

- b Crie o arquivo de armazenamento de chaves para o serviço de proxy do console.

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.pfx -chain
```



- 4 Execute o comando para fazer backup do arquivo `certificates.ks` existente.

```
cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
```

- 5 Use o comando `keytool` para importar os armazenamentos de chaves PKCS12 para o armazenamento de chaves JCEKS.

- a Importe o armazenamento de chaves PKCS12 para o serviço HTTPS.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/vcloud-director/certificates.ks -deststoretype JCEKS -srckeystore http.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

- b Importe o armazenamento de chaves PKCS12 para o serviço de proxy do console.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/vcloud-director/certificates.ks -deststoretype JCEKS -srckeystore consoleproxy.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

- 6 Verifique se a importação dos certificados foi bem-sucedida.

```
keytool -storetype JCEKS -storepass keystore_password -keystore /opt/vmware/vcloud-director/certificates.ks -list
```

- 7 Execute o comando para importar os certificados assinados para a instância do vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password keystore_password
```

- 8 Para que os certificados assinados pela CA tenham efeito, reinicie o serviço do vCloud Director no dispositivo do `vmware-vcd`.

```
service vmware-vcd restart
```

#### Próximo passo

- Se você estiver usando certificados curinga, consulte [Implantar o dispositivo vCloud Director com certificados curinga assinados para comunicação HTTPS e via proxy de console](#).
- Se você não estiver usando certificados curinga, repita esse procedimento em todas as células de dispositivos do vCloud Director no grupo de servidores.
- Para obter mais informações sobre como substituir os certificados do banco de dados PostgreSQL incorporado e da interface de usuário de gerenciamento do dispositivo do vCloud Director, consulte [Substituir um certificado de interface de usuário de gerenciamento do dispositivo vCloud Director e PostgreSQL incorporado autoassinado](#).

## Substituir um certificado de interface de usuário de gerenciamento do dispositivo vCloud Director e PostgreSQL incorporado autoassinado

Por padrão, o banco de dados PostgreSQL incorporado e a interface do usuário de gerenciamento do dispositivo vCloud Director compartilham um conjunto de certificados SSL autoassinados. Para maior segurança, você pode substituir os certificados autoassinados por certificados assinados pela autoridade de certificação (CA).

Quando você implanta o dispositivo vCloud Director, ele gera certificados autoassinados com um período de validade de 365 dias. O dispositivo vCloud Director usa dois conjuntos de certificados SSL. O serviço vCloud Director usa um conjunto de certificados para comunicações de proxy HTTPS e do console. O banco de dados PostgreSQL incorporado e a interface de usuário de gerenciamento do dispositivo vCloud Director compartilham o outro conjunto de certificados SSL.

---

**Observação** O processo de substituir o banco de dados e os certificados de interface de usuário de gerenciamento de dispositivos não afeta os certificados para comunicações HTTPS e de proxy do console. A substituição de um dos conjuntos de certificados não significa que você deve substituir o outro conjunto.

---

### Procedimentos

- 1 Envie a solicitação de assinatura de certificado que está localizada em `/opt/vmware/appliance/etc/ssl/vcd_ova.csr` à CA para assinatura.
- 2 Se estiver substituindo o certificado do banco de dados primário, coloque todos os outros nós no modo de manutenção para evitar a possibilidade de perda de dados.
- 3 Substitua o certificado de formato PEM existente em `/opt/vmware/appliance/etc/ssl/vcd_ova.crt` pelo certificado assinado, obtido da sua autoridade de certificação na [Etapa 1](#).
- 4 Para selecionar o novo certificado, reinicie os serviços `vpostgres`, `nginx` e `vcd_ova_ui`.

```
systemctl restart nginx.service && systemctl restart vcd_ova_ui.service
```

```
systemctl restart vpostgres.service
```

- 5 Se estiver substituindo o certificado do banco de dados primário, retire todos os outros nós do modo de manutenção.

### Resultados

O novo certificado será importado para o truststore do vCloud Director em outras células do vCloud Director da próxima vez em que a função `appliance-sync` for executada. A operação pode demorar até 60 segundos.

## Renovar os certificados do dispositivo vCloud Director

Quando você implanta o dispositivo vCloud Director, ele gera certificados autoassinados com um período de validade de 365 dias. Se houver certificados prestes a expirar ou já expirados no seu ambiente, você poderá gerar novos certificados autoassinados. Você deve renovar os certificados para cada célula do vCloud Director individualmente.

O dispositivo vCloud Director usa dois conjuntos de certificados SSL. O serviço vCloud Director usa um conjunto de certificados para comunicações de proxy HTTPS e do console. O banco de dados PostgreSQL incorporado e a interface de usuário de gerenciamento do dispositivo vCloud Director compartilham o outro conjunto de certificados SSL.

É possível alterar ambos os conjuntos de certificados autoassinados. Como alternativa, se você usar certificados assinados por CA para as comunicações HTTPS e via proxy do console do vCloud Director, poderá alterar apenas o certificado da interface do usuário de gerenciamento de dispositivo e do banco de dados PostgreSQL incorporado. Certificados assinados por CA incluem uma cadeia de confiança completa enraizada em uma autoridade de certificação pública conhecida.

### Pré-requisitos

Se estiver renovando o certificado do nó primário em um cluster de alta disponibilidade de banco de dados, coloque todos os outros nós no modo de manutenção para evitar a perda de dados. Consulte [Como gerenciar uma célula](#).

### Procedimentos

- 1 Faça login diretamente ou conecte-se via SSH ao SO do dispositivo vCloud Director como **root**.
- 2 Para parar os serviços do vCloud Director, execute o seguinte comando.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u administrator cell --shutdown
```

- 3 Para gerar novos certificados auto-assinados, execute o seguinte comando.

```
/opt/vmware/appliance/bin/generate-certificates.sh <root-password>
```

Esse comando coloca automaticamente em uso os certificados recém-gerados para o banco de dados PostgreSQL incorporado e a UI de gerenciamento de dispositivo. Os servidores PostgreSQL e Nginx são reiniciados. O comando gera um novo armazenamento de chaves de certificados `/opt/vmware/vcloud-director/certificates.ks` com novos certificados autoassinados para a comunicação HTTPS e via proxy de console do vCloud Director, que são usados no [Etapa 4](#).

- 4 Se você não estiver usando certificados assinados por CA, execute o comando para importar os certificados autoassinados recém-gerados para o vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password <root-password>
```

## 5 Reinicie o serviço vCloud Director.

```
service vmware-vcd start
```

### Resultados

Os certificados autoassinados renovados estão visíveis na interface de usuário do vCloud Director.

O novo certificado PostgreSQL será importado para o truststore do vCloud Director em outras células do vCloud Director da próxima vez em que a função `appliance-sync` for executada. A operação pode demorar até 60 segundos.

### Próximo passo

Se necessário, um certificado autoassinado pode ser substituído por um certificado assinado por uma autoridade de certificação externa ou interna.

# Configuração do dispositivo do vCloud Director

## 8

Você pode visualizar o status das células em um cluster de alta disponibilidade de banco de dados, fazer o backup e a restauração do banco de dados incorporado e redefinir as configurações do dispositivo.

Depois de implantar o dispositivo do vCloud Director, você não poderá alterar os endereços IP de rede `eth0` e `eth1` ou o nome do host do dispositivo. Se quiser que o dispositivo do vCloud Director tenha endereços ou nome de host diferentes, deverá implantar um novo dispositivo.

Se você deve realizar a manutenção de um dispositivo que requer o desligamento do cluster de alta disponibilidade do banco de dados para evitar problemas de sincronização, primeiro encerre o dispositivo primário e, em seguida, os dispositivos em espera.

Este capítulo inclui os seguintes tópicos:

- [Visualizar o status das células em um cluster de alta disponibilidade de banco de dados](#)
- [Recuperar de uma falha de banco de dados primário em um cluster de alta disponibilidade](#)
- [Recuperar de uma falha de célula em espera em um cluster de alta disponibilidade](#)
- [Backup e restauração do banco de dados incorporado do dispositivo do vCloud Director](#)
- [Configurar o acesso externo ao banco de dados do vCloud Director](#)
- [Ativar ou desativar o acesso do SSH ao dispositivo do vCloud Director](#)
- [Editar as configurações de DNS do vCloud Director Appliance](#)
- [Editar as rotas estáticas para as interfaces de rede do dispositivo do vCloud Director](#)
- [Scripts de configuração no appliance vCloud Director](#)
- [Aumentar a capacidade do banco de dados PostgreSQL incorporado em um dispositivo do vCloud Director](#)
- [Modificar as configurações do PostgreSQL no dispositivo do vCloud Director](#)

## Visualizar o status das células em um cluster de alta disponibilidade de banco de dados

Para exibir o status das células primária e em espera em um cluster de alta disponibilidade (HA) do banco de dados do appliance, você pode fazer login na interface de usuário de gerenciamento do appliance de qualquer célula do cluster de HA do banco de dados.

O cluster de HA de banco de dados do appliance vCloud Director é composto por uma célula primária e duas em espera. Consulte [Implantações de dispositivo e configuração de alta disponibilidade do banco de dados](#).

### Procedimentos

- 1 Em um navegador da Web, acesse a interface de usuário de gerenciamento do appliance em `https://vcd_ip_address:5480`.
- 2 Faça login como **root**.
- 3 Para visualizar os detalhes sobre as células no cluster de HA de banco de dados, clique em **Disponibilidade do Banco de Dados do vCD**.

Propriedade	Descrição
Nome	O nome DNS da célula.
Função	Ela pode ser primária ou em espera. Um cluster de HA de banco de dados do appliance é composto por uma célula primária e duas em espera.
Status	Elas podem estar em execução, inacessíveis ou com falha. Um asterisco (*) indica o status da célula primária.
Seguintes	O nome da célula primária com a qual a célula em espera é replicada.

### Próximo passo

Se uma célula em espera não estiver em um estado em execução, implante uma nova célula em espera.

Se a célula principal não estiver em um estado de execução, [Recuperar de uma falha de banco de dados primário em um cluster de alta disponibilidade](#).

## Recuperar de uma falha de banco de dados primário em um cluster de alta disponibilidade

Se a célula primária não estiver sendo executada corretamente, para recuperar o banco de dados do vCloud Director, você poderá promover uma das células em espera para se tornar a nova célula primária. Depois, você deve implantar uma nova célula em espera.

Você pode usar esse fluxo de trabalho para reutilizar os endereços IP e o nome do host da célula primária com falha ao implantar a nova célula em espera.

#### Pré-requisitos

- Verifique se a célula primária está no estado não acessível ou com falha.
- Verifique se as duas células em espera estão no estado de execução.
- Familiarize-se com o procedimento para remover um dispositivo com falha do grupo de servidores do vCloud Director e do cluster de alta disponibilidade repmgr. Consulte [Cancelar o registro de uma célula primária com falha em um cluster de alta disponibilidade de banco de dados](#).

Consulte [Visualizar o status das células em um cluster de alta disponibilidade de banco de dados](#).

#### Procedimentos

- 1 Se possível, use a ferramenta de gerenciamento de células para encerrar o processo do vCloud Director. Na célula primária com falha, execute o seguinte comando.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 2 Desligue a VM primária com falha.
- 3 Faça login como **raiz** na interface de usuário de gerenciamento de appliances de uma célula em espera em execução, `https://standby_ip_address:5480`.
- 4 Na coluna **Função** para a célula em espera que você deseja que se torne a nova célula primária, clique em **Promover**.

A célula se torna a nova célula primária no estado de execução. A outra célula em espera está seguindo a célula primária recém-promovida.

- 5 Remova o dispositivo primário com falha do grupo de servidores do vCloud Director e do cluster de alta disponibilidade do repmgr.
- 6 Se quiser reutilizar o endereço IP e o nome de host da célula primária com falha, certifique-se de que o dispositivo primário com falha permaneça desligado ou exclua-o.
- 7 Implante um novo appliance em espera. Você pode [Iniciar a implantação do dispositivo do vCloud Director](#) ou pode [Implantação do dispositivo vCloud Director usando o VMware OVF Tool](#).

Após a implantação do novo dispositivo em espera, o estado do cluster deve ser Íntegro.

## Recuperar de uma falha de célula em espera em um cluster de alta disponibilidade

Se uma célula em espera não estiver funcionando corretamente, você poderá se recuperar da falha implantando uma nova célula em espera.

Se uma das células em espera estiver no estado `Unreachable` ou `Failed`, você poderá implantar uma nova célula. Para exibir o estado das células no cluster, consulte [Visualizar o status das células em um cluster de alta disponibilidade de banco de dados](#).

Você pode usar esse fluxo de trabalho para reutilizar os endereços IP e o nome do host da célula em espera com falha ao implantar uma nova célula em espera.

- 1 Se possível, use a ferramenta de gerenciamento de células para encerrar o processo do vCloud Director. Na célula em espera com falha, execute o seguinte comando.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 2 Desligue a VM em espera com falha.
- 3 Remova o dispositivo em espera com falha do grupo de servidores do vCloud Director e do cluster de alta disponibilidade repmgr. Consulte [Cancelar o registro de um nó em espera com falha ou inacessível em um cluster de alta disponibilidade de banco de dados](#).
- 4 Se quiser reutilizar o endereço IP e o nome DNS da célula em espera com falha, você deverá excluí-la ou garantir que ela permaneça desligada.
- 5 Implante um novo appliance em espera. Você pode [Iniciar a implantação do dispositivo do vCloud Director](#) ou pode [Implantação do dispositivo vCloud Director usando o VMware OVF Tool](#).

Após a implantação da nova célula em espera, o estado do cluster deve ser `Íntegro`.

## Backup e restauração do banco de dados incorporado do dispositivo do vCloud Director

Você pode fazer backup do banco de dados PostgreSQL incorporado do dispositivo do vCloud Director, que pode ajudá-lo a restaurar seu ambiente vCloud Director após uma falha.

### Fazer backup do banco de dados incorporado do dispositivo vCloud Director

Se o seu ambiente consiste em implantações de dispositivos vCloud Director com bancos de dados PostgreSQL incorporados, você pode fazer backup do banco de dados vCloud Director da célula primária. O arquivo `.tgz` resultante é armazenado no local de armazenamento do serviço de transferência compartilhada NFS.

#### Procedimentos

- 1 Faça o login diretamente ou via SSH na célula primária como **root**.
- 2 Navegue até `/opt/vmware/appliance/bin`.
- 3 Execute o comando `create-db-backup`.



## Resultados

No armazenamento do serviço de transferência compartilhada NFS, no diretório `vcloudapp.nfs_mount.VMware_vCloud_Director/pgdb-backup/`, você pode ver o arquivo recém-criado `db-backup-date_time_format.tgz`. O arquivo `.tgz` contém o arquivo de despejo de banco de dados e os arquivos `global.properties`, `responses.properties`, `certificates`, `proxycertificates` e `truststore` da célula primária.

## Restaurando um ambiente de dispositivo vCloud Director com uma configuração de banco de dados de alta disponibilidade

Se você tiver feito backup do banco de dados PostgreSQL incorporado de um ambiente de dispositivo vCloud Director com uma configuração de banco de dados de alta disponibilidade, poderá implantar um novo cluster de dispositivos e restaurar o banco de dados do dispositivo nele.

O fluxo de trabalho de restauração inclui três estágios principais.

- Copiando o arquivo `.tar` do backup do banco de dados incorporado a partir do armazenamento compartilhado NFS.
- Restaurar o banco de dados nas células primária e em espera do banco de dados incorporado.
- Implantar quaisquer células de aplicativo necessárias.

## Pré-requisitos

- Verifique se você tem um arquivo de backup `.tar` do banco de dados PostgreSQL incorporado. Consulte [Fazer backup do banco de dados incorporado do dispositivo vCloud Director](#).
- Implante uma célula de banco de dados primária e duas células de banco de dados em espera. Consulte [Capítulo 6 Implantação do vCloud DirectorAppliance](#).
- Se quiser que o novo cluster de dispositivos use o servidor NFS do ambiente anterior, crie e exporte um novo diretório no servidor NFS como o novo compartilhamento. O ponto de montagem existente não pode ser reutilizado.

## Procedimento

- 1 Nas células primária e em espera, faça login como **root** e execute o comando para interromper o serviço vCloud Director.

```
service vmware-vcd stop
```

- 2 Nas células primária e em espera, copie o arquivo de backup `.tar` para a pasta `/tmp`.

Se não houver espaço livre suficiente na pasta `do/tmp`, use outra localização para armazenar o arquivo `.tar`.

- 3 Nas células primária e em espera, descompacte o arquivo de backup em /tmp.

```
tar -zxvf db-backup-date_time_format.tgz
```

Na pasta /tmp, você pode ver as respostas de `global.properties`, `responses.properties`, `certificates`, `proxycertificates`, `truststore` e o arquivo de despejo de banco de dados denominado `vcloud_date_time_format`.

---

**Observação** O arquivo `truststore` está disponível somente para o vCloud Director 9.7.0.1 e versões posteriores.

---

- 4 Somente na célula primária, faça login como **root** no console e execute os comandos a seguir.
  - a Descarte o banco de dados `vcloud`.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

- b Execute o comando `pg_restore`.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/  
vcloud_date_time_name
```

- 5 Nas células primária e em espera, salve uma cópia dos arquivos de dados de configuração, substitua-os e reconfigure e inicie o serviço vCloud Director.
  - a Faça backup das propriedades, dos certificados e dos arquivos `truststore`.

Os arquivos `global.properties`, `responses.properties`, `certificates`, `proxycertificates` e `truststore` estão em `/opt/vmware/vcloud-director/etc/`.

---

**Observação** O arquivo `truststore` está disponível somente para o vCloud Director 9.7.0.1 e versões posteriores.

---

```
cd /opt/vmware/vcloud-director/etc  
mkdir -p backup  
cp global.properties responses.properties certificates proxycertificates truststore backup
```

- b Copie e substitua as propriedades, os certificados e os arquivos `truststore` dos arquivos de backup que você extraiu na [Etapa 3](#).

```
cd /tmp  
cp global.properties responses.properties certificates proxycertificates truststore /opt/  
vmware/vcloud-director/etc/.
```

---

**Observação** O arquivo `truststore` está disponível somente para o vCloud Director 9.7.0.1 e versões posteriores.

---

```
cp certificates /opt/vmware/vcloud-director/.
```

- c Faça backup do de repositório de chaves localizado em `/opt/vmware/vcloud-director/certificates.ks`.

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

- d Execute o comando para reconfigurar o serviço vCloud Director.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

Em que:

- A opção `--keystore-password` corresponde à senha do armazenamento de chaves para os certificados no dispositivo.
- A opção `--database-password` corresponde à senha do banco de dados que você definiu durante a implantação do dispositivo.
- A opção `--database-host` corresponde ao endereço IP da rede eth1 do dispositivo de banco de dados primário.
- O valor `--primary-ip` corresponde ao endereço IP de rede eth0 da célula do dispositivo que você está restaurando. Este não é o endereço IP da célula do banco de dados primário.
- A opção `--console-proxy-ip` corresponde ao endereço IP de rede eth0 do dispositivo que você está restaurando.


Para obter informações sobre solução de problemas, consulte [A reconfiguração do serviço do vCloud Director falha ao migrar ou restaurar para o dispositivo vCloud Director](#).

- e Execute o comando para iniciar o serviço vCloud Director.

```
service vmware-vcd start
```

Você pode monitorar o progresso da inicialização da célula em `/opt/vmware/vcloud-director/logs/cell.log`.

- 6 (Opcional) Implante células adicionais de aplicativo. Consulte [Capítulo 6 Implantação do vCloud DirectorAppliance](#).

- 7 Depois que todas as células do grupo de servidores terminarem o processo de inicialização, verifique se a restauração do seu ambiente vCloud Director foi bem-sucedida.
  - a Abra o vCloud Director Service Provider Admin Portal usando o endereço IP de rede `eth0` de qualquer célula do novo grupo de servidores, `https://eth0_IP_new_cell/provider`.
  - b Faça login no Service Provider Admin Portal com suas credenciais de **administrador de sistema** existentes.
  - c Confirme se os seus recursos do vSphere e de nuvem estão disponíveis no novo ambiente.
- 8 Após a verificação bem-sucedida da restauração do banco de dados, use o Service Provider Admin Portal para excluir as células desconectadas que pertencem ao ambiente antigo vCloud Director.
  - a No menu principal () , selecione **Recursos de Nuvem**.
  - b No painel esquerdo, clique em **Células da Nuvem**.
  - c Selecione uma célula inativa e clique em **Cancelar registro**.

## Configurar o acesso externo ao banco de dados do vCloud Director

Você pode ativar o acesso de determinados endereços IP externos ao banco de dados do vCloud Director que está incorporado no dispositivo principal.

Durante uma migração para o dispositivo do vCloud Director ou, se você planeja usar uma solução de backup de banco de dados de terceiros, talvez queira ativar o acesso externo ao banco de dados do vCloud Director incorporado.

### Procedimentos

- 1 Faça o login diretamente ou via SSH na célula primária como **root**.
- 2 Navegue até o diretório do banco de dados, `/opt/vmware/appliance/etc/pg_hba.d/`.
- 3 Crie um arquivo de texto contendo entradas para os endereços IP externos de destino semelhante a:

#TYPE	DATABASE	USER	ADDRESS	METHOD
host	vcloud	vcloud	<i>CIDR_notation</i>	md5

Por exemplo:

#TYPE	DATABASE	USER	ADDRESS	METHOD
host	vcloud	vcloud	172.168.100.5/32	md5
host	vcloud	vcloud	172.168.20.5/32	md5

Suas entradas são anexadas ao arquivo `pg_hba.conf` atualizado dinamicamente, que controla o acesso ao banco de dados primário no cluster de alta disponibilidade.

## Ativar ou desativar o acesso do SSH ao dispositivo do vCloud Director

Durante a implantação do dispositivo, você pode deixar desabilitado o acesso SSH ou habilitá-lo para o dispositivo. Após a implantação, será possível alternar a definição de acesso do SSH.

O daemon do SSH é executado no Appliance para ser usado pela função HA (alta disponibilidade) do banco de dados e para logins **raiz** remotos. Você pode desabilitar o acesso ao SSH para o usuário **raiz**. O acesso ao SSH para a função de HA do banco de dados permanece inalterado.

### Procedimentos

- 1 Se você quiser fazer alterações temporárias na propriedade OVF, por exemplo, para fins de teste, altere a propriedade no vCloud Director.
  - a Faça login diretamente ou usando um cliente SSH no console do dispositivo do vCloud Director como **root**.
  - b Execute o script para habilitar ou desabilitar o acesso **raiz** ao SSH.
    - Para habilitar o acesso **raiz** ao SSH, execute o script `/opt/vmware/appliance/bin/enable_root_login.sh`.
    - Para desabilitar o acesso **raiz** ao SSH, execute o script `/opt/vmware/appliance/bin/disable_root_login.sh`.
- 2 Se você quiser fazer alterações permanentes na propriedade OVF, use a interface de usuário do vSphere para definir o valor da propriedade do `vcloudapp.enable_ssh.VMware_vCloud_Director`.

---

**Observação** Você deve desligar a VM para alterar o valor da propriedade no vSphere.

---

- Para ativar o SSH, defina o valor do `vcloudapp.enable_ssh.VMware_vCloud_Director` como **True**.
- Para desativar o SSH, defina o valor do `vcloudapp.enable_ssh.VMware_vCloud_Director` como **False**.

## Editar as configurações de DNS do vCloud Director Appliance

Após a implantação, você pode alterar o(s) servidor(es) DNS do dispositivo do vCloud Director.

---

**Importante** Não é possível editar o nome de host do dispositivo. Você deve implantar um novo dispositivo com o nome de host desejado.

---

## Procedimentos

- 1 Se você quiser alterar as configurações de DNS temporariamente, por exemplo, para fins de teste, edite as configurações de DNS no vCloud Director.

- a Faça login diretamente ou usando um cliente SSH no console do dispositivo do vCloud Director como **root**.
- b (Opcional) Verifique a configuração do DNS atual executando o seguinte comando:

```
ovfenv --key vami.DNS.VMware_vCloud_Director
```

- c Altere o servidor ou servidores DNS.

Para especificar vários servidores DNS, defina *DNS\_server\_IP* como uma lista separada por vírgulas sem espaços.

```
ovfenv --key vami.DNS.VMware_vCloud_Director --value DNS_server_IP
```

- d Para que as alterações entrem em vigor, reinicie o serviço VAOS.

```
systemctl restart vaos.service
```

- 2 Se você quiser alterar as configurações de DNS permanentemente, use a interface de usuário do vSphere para definir o valor da propriedade do *vami.DNS.VMware\_vCloud\_Director* para o novo endereço IP do servidor DNS.

Para especificar vários servidores DNS, insira uma lista separada por vírgulas sem espaços.

---

**Observação** Você deve desligar a VM para alterar o valor da propriedade no vSphere.

---

## Editar as rotas estáticas para as interfaces de rede do dispositivo do vCloud Director

Você pode alterar as rotas estáticas das interfaces de rede *eth0* e *eth1* após a implantação inicial do vCloud Director.

## Procedimentos

- 1 Se você quiser alterar o valor da rota estática temporariamente, por exemplo, para fins de teste, edite as rotas estáticas no vCloud Director.

- a Faça login diretamente ou usando um cliente SSH no console do dispositivo do vCloud Director como **root**.
- b (Opcional) Verifique a configuração da rota estática atual.

- Para eth0, execute o seguinte comando.

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director
```

- Para eth1, execute o seguinte comando.

```
ovfenv --key vcloudnet.routes1.VMware_vCloud_Director
```

- c Altere o valor da rota estática.

As rotas estáticas devem estar em uma lista separada por vírgula das especificações de rota. Por exemplo, para eth0, você deve executar:

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director --value "172.16.100.253  
172.16.96.0/19, 172.16.100.253 192.168.100.0/24"
```

- Para eth0, execute o seguinte comando.

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director --value "new_static_routes0"
```

- Para eth1, execute o seguinte comando.

```
ovfenv --key vcloudnet.routes1.VMware_vCloud_Director --value "new_static_routes1"
```

- d Reinicie o serviço de rede no dispositivo do vCloud Director.

```
systemctl restart vcd-ova-netconfig.service
```

- 2 Se você quiser alterar o valor da rota estática permanentemente, altere a propriedade OVF usando a interface de usuário do vSphere.

As rotas estáticas devem estar em uma lista das especificações de rota separada por vírgula.

---

**Observação** Você deve desligar a VM para alterar o valor da propriedade no vSphere.

---

- Use a interface de usuário do vSphere para definir o valor da propriedade do `vcloudnet.routes0.VMware_vCloud_Director` para a nova cadeia de caracteres de especificação de rota.
- Use a interface de usuário do vSphere para definir o valor da propriedade do `vcloudnet.routes1.VMware_vCloud_Director` para a nova cadeia de caracteres de especificação de rota.

## Scripts de configuração no appliance vCloud Director

O appliance vCloud Director contém scripts de configuração específicos.

Diretório	Descrição
/opt/vmware/appliance/bin/	Os scripts de configuração de appliance.
/opt/vmware/appliance/etc/	Os arquivos de configuração do appliance.
/opt/vmware/appliance/etc/pg_hba.d/	O diretório no qual você pode adicionar entradas personalizadas ao arquivo pg_hba.conf. Consulte <a href="#">Configurar o acesso externo ao banco de dados do vCloud Director</a> .

## Aumentar a capacidade do banco de dados PostgreSQL incorporado em um dispositivo do vCloud Director

Se você não tiver espaço suficiente no disco do banco de dados PostgreSQL de um dispositivo do vCloud Director, poderá aumentar a capacidade do banco de dados PostgreSQL incorporado.

O banco de dados PostgreSQL reside no disco rígido 3. Ele tem um tamanho padrão de 80 GB. O procedimento pode ser feito enquanto os dispositivos estão operacionais.

**Importante** Você deve aumentar a capacidade de qualquer dispositivo em espera existente antes de aumentar a capacidade do dispositivo primário.

### Pré-requisitos

- Se o seu ambiente do vCloud Director tiver nós em espera, identifique os nós em espera e o nó primário e inicie o procedimento de um nó em espera. Para obter mais informações sobre como identificar as funções dos nós, consulte [Verificar o status de um cluster de alta disponibilidade do banco de dados](#).
- Se o seu ambiente do vCloud Director consistir em apenas um nó primário, execute o procedimento no nó primário.

### Procedimentos

- 1 Faça login no vSphere Client para aumentar a capacidade do disco rígido 3 para o tamanho desejado.

O tamanho do disco do banco de dados PostgreSQL em cada dispositivo em espera deve ser tão grande quanto o disco do banco de dados PostgreSQL no dispositivo primário.

- a Selecione a máquina virtual do dispositivo que você deseja alterar.
- b Selecione **Ações > Editar Configurações**.
- c Aumente o tamanho do **Disco rígido 3** e clique em **OK**.

O progresso da tarefa de reconfiguração aparece no painel **Tarefas recentes**.



## 2 Aumente o tamanho lógico do volume usado pelo banco de dados.

- a Faça login diretamente ou usando um cliente SSH no console do dispositivo do vCloud Director como **root**.
- b Para aplicar a alteração de redimensionamento do disco rígido ao SO, execute o seguinte comando.

```
echo 1 > /sys/class/scsi_device/2\:0\:2\:0/device/rescan
```

- c Para obter o espaço correto reconhecido na camada de volume físico, execute o seguinte comando.

```
pvresize /dev/sdc
```

- d (Opcional) Confirme o novo tamanho do volume físico executando o seguinte comando.

```
pvdisk
```

- e Redimensione o volume lógico executando o seguinte comando.

```
lvresize /dev/database_vg/vpostgres /dev/sdc
```

- f (Opcional) Confirme o novo tamanho do volume lógico executando o seguinte comando.

```
lvdisplay
```

## 3 Aumente o tamanho do sistema de arquivos para que ele consuma todo o volume lógico.

- a Para consumir o espaço adicional, execute o seguinte comando.

```
resize2fs /dev/database_vg/vpostgres
```

- b (Opcional) Para confirmar que o sistema de arquivos consumiu o espaço adicional, execute `df -h`.

O espaço adicional está disponível para o SO. A saída do sistema é semelhante a: `/dev/mapper/database_vg-vpostgres 157G 75G 82G 48% /var/vmware/vpostgres`

- 4 Se o seu ambiente não consistir em apenas um dispositivo primário e tiver outros nós em espera, repita a etapa 1 à etapa 3 em todos os outros nós em espera que tenham um banco de dados e, em seguida, repita a etapa 1 à etapa 3 no nó primário.

## Modificar as configurações do PostgreSQL no dispositivo do vCloud Director

Você pode alterar as configurações de PostgreSQL do dispositivo do vCloud Director usando o comando PostgreSQL `ALTER SYSTEM`.

O comando `ALTER SYSTEM` grava as alterações das configurações de parâmetro no arquivo `postgresql.auto.conf`, que tem precedência sobre o arquivo `postgresql.conf` durante a inicialização do PostgreSQL. Algumas configurações exigem uma reinicialização do serviço PostgreSQL, enquanto outras estão definidas dinamicamente e não exigem uma reinicialização. Não altere o arquivo `postgresql.conf`, pois essas alterações não persistem após a reinicialização.

## Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH no sistema operacional do dispositivo primário como **root**.

- 2 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 3 Use o comando PostgreSQL `ALTER SYSTEM` para alterar um parâmetro.

```
psql -c "ALTER SYSTEM set parâmetro='valor';"
```

- 4 Repita [Etapa 3](#) para cada parâmetro de configuração que você deseja alterar.

- 5 Se alguns dos parâmetros que você deseja alterar exigirem uma reinicialização do serviço PostgreSQL, reinicie o processo `vpostgres`.

```
systemctl restart vpostgres
```

- 6 Se o seu ambiente tiver nós em espera, copie o arquivo `postgresql.auto.conf` para os dispositivos em espera e reinicie o serviço PostgreSQL, se necessário.

- a Copie o `postgresql.auto.conf` do nó primário para um nó em espera.

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
```

- b Se alguns dos parâmetros no arquivo `postgresql.auto.conf` copiado exigirem que uma reinicialização tenha efeito, reinicie o processo `vpostgres` no nó em espera.

```
systemctl restart vpostgres
```

- c Repita [6.a](#) e [6.b](#) para cada nó em espera.

# Usando o conjunto de ferramentas do Replication Manager em uma configuração de cluster de alta disponibilidade

9

O conjunto de ferramentas de código-fonte aberto do repmgr faz parte do banco de dados PostgreSQL incorporado do dispositivo vCloud Director. Você pode usar o repmgr para configurar, monitorar e controlar a replicação PostgreSQL e o failover de banco de dados no seu cluster de alta disponibilidade do banco de dados vCloud Director.

Você pode usar a interface de linha de comando do repmgr para verificar o status e os eventos de um nó ou um cluster, para registrar ou cancelar o registro de um nó, para promover um nó em espera, trocar as funções de um nó primário e um nó em espera ou seguir um novo nó primário.

Para saber mais sobre a configuração da alta disponibilidade do banco de dados vCloud Director, consulte [Implantações de dispositivo e configuração de alta disponibilidade do banco de dados](#).

Para saber mais sobre o repmgr, visite [repmgr.org](http://repmgr.org).

Este capítulo inclui os seguintes tópicos:

- [Verificar o status de conectividade de um cluster de alta disponibilidade de banco de dados](#)
- [Verificar o status de replicação de um nó em um cluster de alta disponibilidade de banco de dados](#)
- [Verificar o status de um cluster de alta disponibilidade do banco de dados](#)
- [Detectando um nó primário antigo que volta a ficar online em um cluster de alta disponibilidade](#)
- [Alternar as funções da célula primária e de uma célula em espera em um cluster de alta disponibilidade de banco de dados](#)
- [Cancelar o registro de um nó em espera com falha ou inacessível em um cluster de alta disponibilidade de banco de dados](#)
- [Cancelar o registro de uma célula primária com falha em um cluster de alta disponibilidade de banco de dados](#)
- [Cancelar o registro de uma célula em espera em execução em um cluster de alta disponibilidade de banco de dados](#)

## Verificar o status de conectividade de um cluster de alta disponibilidade de banco de dados

Você pode usar o conjunto de ferramentas do gerenciador de replicações para verificar a conectividade entre os nós no cluster de alta disponibilidade do banco de dados.

### Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional de qualquer uma das células em execução no cluster.

- 2 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 3 Verifique a conectividade do cluster.

- O comando `repmgr cluster matrix` executa o comando `repmgr cluster show` em cada nó do cluster e apresenta o resultado como uma matriz.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf
cluster matrix
```

No exemplo a seguir, o nó 1 e o nó 2 estão ativados, e o nó 3 está desativado. Cada linha corresponde a um servidor e representa o resultado do teste de uma conexão de saída desse servidor.

As três entradas na terceira linha são marcadas com símbolo ?, pois o nó 3 está desativado, e não há informações sobre suas conexões de saída.

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	x
node 3	3	?	?	?

- O comando `repmgr cluster crosscheck` faz uma verificação cruzada das conexões entre cada combinação de nós e pode fornecer uma visão geral melhor da conectividade do cluster.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf
cluster crosscheck
```

No exemplo a seguir, o nó do qual você executa o comando `repmgr cluster crosscheck` mescla a saída do sistema da matriz de cluster com a saída dos outros nós e faz uma verificação cruzada entre os nós. Nesse caso, todos os nós estão em funcionamento, mas o firewall descarta pacotes originados do nó 1 e direcionados ao nó 3. Este é um exemplo de uma partição de rede assimétrica, na qual o nó 1 não pode enviar pacotes para o nó 3.

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	*
node 3	3	*	*	*

### Próximo passo

Para determinar o status geral da conectividade no cluster de alta disponibilidade do banco de dados, execute esses comandos em cada nó e compare os resultados.

## Verificar o status de replicação de um nó em um cluster de alta disponibilidade de banco de dados

Você pode usar o conjunto de ferramentas do gerenciador de replicações e o terminal interativo PostgreSQL para verificar o status de replicação de nós individuais em um cluster de alta disponibilidade do banco de dados.

### Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional de qualquer um dos nós em execução no cluster.
- 2 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 3 Verifique o status de replicação do nó.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf node status
```

A saída do sistema fornece informações sobre o nó, a versão PostgreSQL e os detalhes da replicação.

- 4 (Opcional) Para obter informações mais detalhadas, use o terminal interativo do PostgreSQL para verificar o status de replicação dos nós.

O terminal interativo PostgreSQL pode fornecer informações sobre se qualquer um dos registros de log recebidos dos nós em espera está atrasado em comparação aos logs enviados pelo nó primário.

- a Conectar ao terminal `psql`

```
/opt/vmware/vpostgres/current/bin/psql
```

- b Para expandir a exibição e facilitar a leitura dos resultados da consulta, execute o comando `set \x`.
- c Execute uma consulta de status de replicação dependendo da função do nó.

Opção	Ação
Execute uma consulta no nó primário.	<code>/opt/vmware/vpostgres/current/bin/psql</code>
Execute uma consulta em um nó em espera.	<code>select * from pg_stat_wal_receiver;</code>

## Verificar o status de um cluster de alta disponibilidade do banco de dados

Para solucionar problemas no seu cluster de alta disponibilidade do banco de dados, você deve monitorar o status dos nós e dos eventos nesse cluster.

### Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional de qualquer uma das células em execução no cluster.
- 2 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 3 Verifique o status do cluster.

A coluna **Upstream** mostra o nó primário atual.

```
/opt/vmware/vpostgres/current/bin/repmgr cluster show
```

A saída do console exibe as informações do cluster. No exemplo a seguir, o nó primário no cluster, nó 3, não está acessível.

```

ID | Name      | Role   | Status      | Upstream | Location | Connection string
---+-----+-----+-----+-----+-----+-----
Node 1 | Node name | standby | running    | Node 3 name | default | host=host IP address

```

```

user=repmgr dbname=repmgr
Node 2 | Node name | standby | running | Node 3 name | default | host=host IP address
user=repmgr dbname=repmgr
Node 3 | Node name | primary | ? unreachable | | default | host=host IP address
user=repmgr dbname=repmgr

```

No exemplo de saída de sistema a seguir, o nó 3 é o nó primário em um cluster íntegro em execução.

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	Node name	standby	running	Node3 name	default	host=host IP address user=repmgr dbname=repmgr
Node 2	Node name	standby	running	Node3 name	default	host=host IP address user=repmgr dbname=repmgr
Node 3	Node name	primary	*running		default	host=host IP address user=repmgr dbname=repmgr

#### 4 Verifique o log de eventos do cluster.

```

/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf cluster
event

```

A saída do sistema mostra eventos de criação, clonagem e registro no cluster.

#### Próximo passo

Se o status do nó primário for `unreachable` ou `failed`, você deverá promover um nó em espera.

Se o status de um nó em espera for `unreachable` ou `failed`, repare o nó e inicie o serviço PostgreSQL se ele não estiver em execução.

## Detectando um nó primário antigo que volta a ficar online em um cluster de alta disponibilidade

Se um nó primário no seu cluster falhar e depois voltar a ficar online quando você promover um nó em espera para ser o novo primário, isso causará imprecisões nos dados do `repmgr`. Você pode detectar irregularidades com o comando `repmgr cluster show`.

### Exemplo: Executando `repmgr cluster show` no nó primário antigo

No exemplo a seguir, executar o comando `repmgr cluster show` em um nó primário antigo que volta a ficar online resulta na seguinte saída do sistema.

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	Nome do nó 1	standby	!running as primary	Nome do nó 3	default	host=Endereço IP do host user=repmgr dbname=repmgr
Node 2	Nome do nó 2	standby	running	Nome do nó 3	default	host=Endereço IP do host user=repmgr dbname=repmgr

```
Node 3 | Nome do nó 3| primary | * running | | default | host= user=repmgr
dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is registered as standby but running as primary
```

No exemplo, o nó 1 é o nó primário atual no cluster.

Quando você executa o comando `repmgr cluster show`, receber o status `!running as primary` para um nó em espera indica que um nó primário anterior está em execução no cluster. Nesse caso, você deve encerrar e cancelar o registro do antigo nó primário.

## Exemplo: Executando `repmgr cluster show` no novo primário

No exemplo a seguir, executar o comando `repmgr cluster show` no novo nó primário resulta na seguinte saída do sistema.

```

ID | Name | Role | Status | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Nome do nó 1| primary | * running | | default | host=Endereço IP do host
user=repmgr dbname=repmgr
Node 2 | Nome do nó 2| standby | running | Nome do nó 1 | default | host=Endereço IP do host
user=repmgr dbname=repmgr
Node 3 | Nome do nó 3| primary | ! running | | default | host=Endereço IP do host
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 3(ID: Node 3) is running but the repmgr node record is inactive
```

Nesse caso, os dados do `repmgr` estão corretos. Eles indicam precisamente que o nó 1 está em execução e que é o nó primário atual. A mensagem de aviso sobre o nó 3, o primário antigo, indica que os dados do `repmgr` nesse nó não são precisos.

## Exemplo: Executando `repmgr cluster show` depois de promover um nó em espera, sem executar `standby follow` nos nós em espera restantes

No exemplo a seguir, você pode ver os dados do `repmgr` em cada nó em um cluster no qual o nó primário falhou. Um nó em espera foi promovido manualmente usando o comando `repmgr standby promote`, mas sem executar `repmgr standby follow` nos nós em espera restantes.

Quando você executar `repmgr cluster show` no novo primário, a saída do sistema representará os dados corretos do `repmgr`, mas o novo nó primário, o nó 2, não será seguido por nenhum dos nós em espera.

```

ID | Name | Role | Status | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Nome do nó 1| primary | * running | | default | host=Endereço IP do host
user=repmgr dbname=repmgr
Node 2 | Nome do nó 2| primary | ! running | | default | host=Endereço IP do host
user=repmgr dbname=repmgr
Node 3 | Nome do nó 3| standby | running | Nome do nó 1 | default | host=Endereço IP do host
```



```
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is running but the repmgr node record is inactive
```

O nó 1, que é o primeiro primário, e o nó 3, que é o nó em espera que segue o primário anterior, fornece dados do repmgr incorretos.

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	<i>Nome do nó 1</i>	primary	* running		default	host= <i>Endereço IP do host</i> user=repmgr dbname=repmgr
Node 2	<i>Nome do nó 2</i>	standby	! running as primary	<i>Nome do nó 1</i>	default	host= <i>Endereço IP do host</i> user=repmgr dbname=repmgr
Node 3	<i>Nome do nó 3</i>	standby	running	<i>Nome do nó 1</i>	default	host= <i>Endereço IP do host</i> user=repmgr dbname=repmgr

```
WARNING: following issues were detected
- node 2(ID: Node 2) is registered as standby but running as primary
```

## Exemplo: Executando repmgr cluster show em um nó em espera

Executar o comando em um nó em espera que está seguindo o primário atual resulta em uma saída do sistema com dados do repmgr precisos que são idênticos aos dados no primário atual.

Executar o comando em um nó em espera que está seguindo o primário anterior resulta em uma saída do sistema com dados do repmgr imprecisos que são idênticos aos dados no primário anterior.

## Entradas de log

Se um antigo nó primário que falhou voltar a ficar online depois de você promover um nó em espera para ser o novo primário, as seguintes entradas aparecerão no arquivo `update-repmgr-data.log` em todos os nós com dados do repmgr incorretos.

```
ERROR: An old primary is running in the repmgr cluster.
ERROR: Manual intervention is required to repair the repmgr cluster.
ERROR: The first step should be to shutdown and unregister the old primary.
```

## Alternar as funções da célula primária e de uma célula em espera em um cluster de alta disponibilidade de banco de dados

Você pode usar um comando do repmgr para trocar as funções do nó primário e de um dos nós em espera no cluster de alta disponibilidade do banco de dados durante uma manutenção planejada.

## Pré-requisitos

- Coloque todas as células do vCloud Director que fazem parte do cluster de alta disponibilidade no modo de manutenção.
- Verifique se todos os nós no cluster estão íntegros e online.

## Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional do nó em espera que você deseja promover.
- 2 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 3 (Opcional) Verifique se os pré-requisitos de troca são atendidos, executando o comando com a opção `--dry-run`.

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow --dry-run
```

- 4 Troque as funções da célula primária e da célula em espera.

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow
```

## Resultados

A última linha da saída do console indica que a troca de espera foi concluída com êxito.

## Próximo passo

- 1 Execute o comando **reconfigure-database** para atualizar o endereço IP do banco de dados em todas as células do vCloud Director. Consulte [Atualizar os endereços IP do banco de dados em células do vCloud Director](#).
- 2 Quando você reconfigurar as células do vCloud Director no grupo de servidores para apontar para o novo banco de dados primário, retire do modo de manutenção todas as células do vCloud Director que fazem parte do cluster de alta disponibilidade.

# Cancelar o registro de um nó em espera com falha ou inacessível em um cluster de alta disponibilidade de banco de dados

Você pode usar o `repmgr` em um nó em execução no cluster para cancelar o registro de um nó em espera com falha ou inacessível.

---

**Observação** Para que o nó primário funcione normalmente, pelo menos um nó em espera deve estar sempre em execução.

---

### Pré-requisitos

Para cancelar o registro de um nó em espera que não está em execução, você deve fornecer o ID do nó. Para encontrar o endereço IP, verifique o status do cluster e localize o nó. Nessa linha, use o valor do host da coluna cadeia de conexão para identificar o endereço IP do nó. Consulte [Verificar o status de um cluster de alta disponibilidade do banco de dados](#).

### Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional de qualquer um dos nós em execução no cluster.
- 2 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 3 Cancele o registro do nó com falha ou não acessível.

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister -f /opt/vmware/vpostgres/current/etc/repmgr.conf --node-id=ID
```

### Resultados

Cancelar o registro do nó remove as informações desse nó dos metadados do repmgr.

## Cancelar o registro de uma célula primária com falha em um cluster de alta disponibilidade de banco de dados

Se o nó primário no cluster de alta disponibilidade do banco de dados falhar e você promover um novo primário, deverá cancelar o registro do nó primário com falha para removê-lo do cluster e evitar dados de status do cluster inconsistentes.

### Pré-requisitos

- Para cancelar o registro de um nó primário que não está em execução, você deve fornecer o ID do nó. Para encontrar o endereço IP, verifique o status do cluster e localize o nó. Nessa linha, use o valor do host da coluna cadeia de conexão para identificar o endereço IP do nó. Consulte [Verificar o status de um cluster de alta disponibilidade do banco de dados](#).
- Verifique se o primário com falha está inativo e sem nenhum dos seguintes nós em espera e promova um novo primário.

### Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional de qualquer um dos nós em execução no cluster.
- 2 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 3 (Opcional) Para verificar se os pré-requisitos para cancelar o registro do nó foram atendidos, execute o comando com a opção `--dry-run`.

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=ID do nó --dry-run
```

- 4 Cancele o registro do nó.

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=ID do nó
```

## Resultados

A operação remove o nó dos metadados do repmgr.

# Cancelar o registro de uma célula em espera em execução em um cluster de alta disponibilidade de banco de dados

Se quiser usar um nó em outra função ou se quiser removê-lo do cluster de alta disponibilidade, você deverá cancelar seu registro.

Você pode executar esse comando durante a operação normal do sistema.

---

**Observação** Para que o nó primário funcione normalmente, pelo menos um nó em espera deve estar sempre em execução.

---

## Pré-requisitos

Para cancelar o registro de um nó em espera, é necessário fornecer o ID desse nó. Para encontrar o endereço IP, verifique o status do cluster e localize o nó. Nessa linha, use o valor do host da coluna cadeia de conexão para identificar o endereço IP do nó. Consulte [Verificar o status de um cluster de alta disponibilidade do banco de dados](#).

## Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional de qualquer um dos nós em execução no cluster.
- 2 Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- 3 Cancele o registro do nó.

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister --node-id=ID do nó -f /opt/vmware/vpostgres/current/etc/repmgr.conf
```

## Resultados

Cancelar o registro do nó remove o registro do nó em espera da tabela de metadados internos do conjunto de ferramentas do repmgr.

# Referência da ferramenta de gerenciamento de células

# 10

A ferramenta de gerenciamento de células é um utilitário de linha de comando que você pode usar para gerenciar uma célula ou um banco de dados do vCloud Director. Credenciais de superusuário ou administrador do sistema são necessárias para a maioria das operações.

A ferramenta de gerenciamento de célula é instalada em `/opt/vmware/vcloud-director/bin/`. Você pode usá-la para executar um único comando ou pode executá-la como um shell interativo.

## Listando comandos disponíveis

Para listar os comandos disponíveis da ferramenta de gerenciamento de células, use a seguinte linha de comando.

```
./cell-management-tool -h
```

## Usando o modo de shell

Você pode executar a ferramenta de gerenciamento de células como um shell interativo, invocando-a sem argumentos, conforme mostrado aqui.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool
Cell Management Tool v8.14.0.4146350 Type "help" for available subcommands. cmt>
```

No modo de shell, você pode digitar qualquer comando da ferramenta de gerenciamento de células no prompt `cmt>`, conforme mostrado neste exemplo.

```
cmt>cell -h
uso: cell [options] -a,--application-states exibir o estado de cada aplicativo na célula [PRETERIDO
- use o comando cell-application no lugar] -h,--help imprimir esta mensagem -i,--pid <arg> o id
do processo da célula [NECESSÁRIO se o nome de usuário não for especificado] -m,--maintenance
<arg> entrar normalmente no modo de manutenção na célula -p,--password <arg> senha de administrador
[OPCIONAL] -q,--quiesce <arg> desativar atividade na célula -s,--shutdown encerrar a célula
normalmente -t,--status exibir atividades na célula -tt,--status-verbose exibir uma descrição
detalhada das atividades na célula -u,--username <arg> nome de usuário do administrador [NECESSÁRIO
se o pid não for especificado] Observação: a senha de administrador será solicitada se ela não for
inserida na linha de comando. cmt>
```

O comando retornará para o prompt `cmt>` ao concluir a execução. Para sair do modo de shell, digite **exit** no prompt `cmt>`.

## Exemplo: Ajuda para uso da ferramenta de gerenciamento de células

Este exemplo executa um único comando não interativo que lista os comandos disponíveis da ferramenta de gerenciamento de células.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
usage: cell-management-tool -h,--help print this message Comandos disponíveis: cell - Manipula a
célula e os componentes principais certificates - Reconfigura os certificados SSL da célula . . .
Para obter ajuda específica do comando: cell-management-tool <commandName> -h
```

- [Configurar uma instalação do vCloud Director](#)

Use o comando `system-setup` da ferramenta de gerenciamento de célula para inicializar o banco de dados do grupo de servidores com uma conta de administrador do sistema e informações relacionadas.

- [Habilitar o vCloud Director Web Console](#)

No vCloud Director 10.0, o vCloud Director Web Console (interface de usuário baseada em Flex) está obsoleto, desativado por padrão, e a URL do Web Console é redirecionada para as páginas iniciais do HTML5 correspondentes para provedores de serviços e tenants. Você pode usar a ferramenta de gerenciamento de célula para habilitar o Web Console.

- [Desativar o acesso do provedor de serviços ao endpoint da API herdada](#)

A partir do vCloud Director 10.0, você pode usar endpoints separados de login do vCloud Director OpenAPI para o provedor de serviços e de acesso de tenant ao vCloud Director.

- [Como gerenciar uma célula](#)

Use o subcomando `cell` da ferramenta de gerenciamento de célula para suspender o agendador de tarefas para que novas tarefas não possam ser iniciadas, para exibir o status de tarefas ativas, para controlar o modo de manutenção da célula ou para encerrar a célula normalmente.

- [Como gerenciar aplicativos de célula](#)

Use o comando `cell-application` da ferramenta de gerenciamento de célula para controlar o conjunto de aplicativos que a célula executa na inicialização.

- [Como atualizar as propriedades de conexão do banco de dados](#)

Você pode atualizar as propriedades de conexão do banco de dados do vCloud Director usando o subcomando `reconfigure-database` da ferramenta de gerenciamento de célula.

- **Detectar e reparar dados corrompidos do agendador**

O vCloud Director usa o Agendador de trabalhos Quartz para coordenar as operações assíncronas (trabalhos) em execução no sistema. Se o banco de dados do agendador Quartz for corrompido, você poderá não conseguir desativar o sistema com êxito. Use o comando `fix-scheduler-data` da ferramenta de gerenciamento de célula para verificar se há dados corrompidos do agendador do banco de dados e reparar esses dados conforme necessário.

- **Como gerar certificados autoassinados para os endpoints de proxy de console e HTTP**

Use o comando `generate-certs` da ferramenta de gerenciamento de célula para gerar certificados SSL autoassinados para os endpoints de proxy de console e HTTP

- **Substituindo certificados para os endpoints de proxy de console e HTTP**

Use o comando `certificates` da ferramenta de gerenciamento de célula para substituir certificados SSL para os endpoints de proxy de console e HTTP.

- **Importação de certificados SSL de serviços externos**

Use o comando `import-trusted-certificates` da ferramenta de gerenciamento de célula para importar certificados a serem usados no estabelecimento de conexões seguras com serviços externos, como o AMQP e o banco de dados do vCloud Director.

- **Gerenciamento da lista de codificações SSL permitidas**

Use o comando `ciphers` da ferramenta de gerenciamento de célula para configurar os pacotes de codificação que a célula oferece para usar durante o processo de handshake de SSL.

- **Gerenciar a lista de protocolos SSL permitidos**

Use o comando `ssl-protocols` da ferramenta de gerenciamento de célula para configurar o conjunto de protocolos SSL que a célula oferece para usar durante o processo de handshake de SSL.

- **Como configurar a coleção de métricas**

Use o comando `configure-metrics` da ferramenta de gerenciamento de célula para configurar o conjunto de métricas a serem coletadas.

- **Configuração de um banco de dados de métricas do Cassandra**

Use o comando `cassandra` da ferramenta de gerenciamento de célula para conectar a célula a um banco de dados de métricas opcional.

- **Recuperação da senha do administrador do sistema**

Se você souber o nome de usuário e senha do banco de dados do vCloud Director, poderá usar o comando `recover-password` da ferramenta de gerenciamento de célula para recuperar a senha do administrador do sistema do vCloud Director.

- **Atualizar o status de falha de uma tarefa**

Use o comando `fail-tasks` da ferramenta de gerenciamento de célula para atualizar o status de conclusão associado a tarefas que estavam em execução quando a célula foi encerrada deliberadamente. Você não pode usar o comando `fail-tasks`, a menos que todas as células tenham sido encerradas.

- **Configurar o tratamento de mensagens de auditoria**

Use o comando `configure-audit-syslog` da ferramenta de gerenciamento de célula para configurar a forma como o sistema registra as mensagens de auditoria.

- **Configurar modelos de e-mail**

Use o comando `manage-email` da ferramenta de gerenciamento de célula para gerenciar os modelos que o sistema usa ao criar alertas de e-mail.

- **Encontrar VMs órfãs**

Use o comando `find-orphan-vm` da ferramenta de gerenciamento de célula para encontrar referências a máquinas virtuais que estão presentes no banco de dados do vCenter, mas não no banco de dados do vCloud Director.

- **Entrar ou sair do Programa de aperfeiçoamento da experiência do cliente da VMware**

Para entrar ou sair do Programa de aperfeiçoamento da experiência do cliente (CEIP) da VMware, você pode usar o subcomando `configure-ceip` da ferramenta de gerenciamento de célula.

- **Atualização das definições de configuração do aplicativo**

Com o subcomando `manage-config` da ferramenta de gerenciamento de célula, você pode atualizar diferentes definições de configuração de aplicativo, como atividades de limitação de catálogo.

- **Como configurar a limitação da sincronização de catálogo**

Quando você tem muitos itens de catálogo publicados em ou inscritos de outras organizações, para evitar a sobrecarga do sistema durante as sincronizações de catálogo, pode configurar a limitação da sincronização de catálogo. Você pode usar o subcomando `manage-config` da ferramenta de gerenciamento de célula para configurar a limitação da sincronização de catálogo limitando o número de itens de biblioteca que podem ser sincronizados ao mesmo tempo.

- **Solucionar problemas de falha no acesso à interface do usuário do vCloud Director**

Para visualizar e atualizar os endereços IP e as entradas DNS válidos para as células do vCloud Director em seu ambiente do vCloud Director, você pode usar o subcomando do `manage-config` da ferramenta de gerenciamento de célula.

- **Depuração da detecção de VM do vCenter**

Usando o subcomando `debug-auto-import` da ferramenta de gerenciamento de célula, você pode investigar o motivo pelo qual o mecanismo para descobrir vApps ignora uma ou mais VMs do vCenter.



### ■ Como regenerar endereços MAC para redes estendidas multissite

Se você associar dois sites do vCloud Director configurados com o mesmo ID de instalação, poderá encontrar conflitos de endereço MAC em redes estendidas nesses sites. Para evitar tais conflitos, você deve regenerar os endereços MAC em um dos sites com base em uma propagação personalizada que seja diferente do ID de instalação.

### ■ Atualizar os endereços IP do banco de dados em células do vCloud Director

Você pode usar a ferramenta de gerenciamento de células para atualizar os endereços IP das células do vCloud Director em um cluster de alta disponibilidade de banco de dados.

## Configurar uma instalação do vCloud Director

Use o comando `system-setup` da ferramenta de gerenciamento de célula para inicializar o banco de dados do grupo de servidores com uma conta de administrador do sistema e informações relacionadas.

Depois de configurar todos os servidores no grupo de servidores do vCloud Director e conectá-los ao banco de dados, você poderá criar a conta de administrador inicial do sistema e inicializar o banco de dados do vCloud Director com informações relacionadas com uma linha de comando da seguinte forma:

```
cell-management-tool system-setup options
```

Você não pode executar esse comando em um sistema que já foi configurado. Todas as opções, exceto `--unattended` e `--password`, devem ser especificadas.

**Tabela 10-1. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `system-setup`**

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--email</code>	O endereço de e-mail para o administrador do sistema que você está criando.	O endereço de e-mail do administrador do sistema é armazenado no banco de dados do vCloud Director.
<code>--full-name</code>	O nome completo do administrador do sistema que você está criando.	O nome completo do administrador do sistema é armazenado no banco de dados do vCloud Director.

**Tabela 10-1. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando system-setup (continuação)**

Opção	Argumento	Descrição
--installation-id	Um número inteiro no intervalo de 1 a 63	O ID de instalação dessa instalação do vCloud Director. O sistema usa o ID de instalação ao gerar endereços MAC para NICs virtuais.  <b>Observação</b> Se você planeja criar redes estendidas entre instalações do vCloud Director numa implantação multi-site, considere definir um ID exclusivo de instalação para cada instalação do vCloud Director.
--password	A senha do administrador do sistema que você está criando. Necessária quando você usa a opção --unattended . Se você não usar a opção --unattended , o comando solicitará a senha se você não a fornecer na linha de comando.	O administrador do sistema fornece essa senha ao se autenticar no vCloud Director.
--serial-number	O número de série (chave de licença) para essa instalação.	Opcional. Deverá ser um número de série válido do vCloud Director.
--system-name	O nome a ser usado para a pasta do vCenter Server do vCloud Director.	Essa instalação do vCloud Director é representada por uma pasta com esse nome em cada vCenter Server no qual ela se registra.
--unattended	Nenhum	Opcional. O comando não solicita entrada adicional quando chamado com essa opção.
--user	O nome de usuário do administrador do sistema que você está criando.	O administrador do sistema fornece esse nome de usuário ao se autenticar no vCloud Director.

## Exemplo: Especifique as configurações de sistema do vCloud Director

Um comando como esse especifica todas as configurações de sistema de uma nova instalação do vCloud Director. Como `--unattended` e `--password` não foram especificados, o comando solicita que você forneça e confirme a senha a ser criada para o administrador do sistema.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool system-setup \ --user admin --
full-name "VCD System Administrator" --email vcd-admin@example.com --system-name VCD --installation-
id 2
Please enter the new password for user admin (password must have more than 6 characters):

Re-enter the password to confirm:

Username: admin
Full name: VCD System Administrator
Email: vcd-admin@example.com
System name: VCD
Installation ID: 2
Are you sure you want to use these parameters? [Y/n]:y
Creating admin user.
Setting system details.
Completing system setup.
System setup is complete.
```

## Habilitar o vCloud Director Web Console

No vCloud Director 10.0, o vCloud Director Web Console (interface de usuário baseada em Flex) está obsoleto, desativado por padrão, e a URL do Web Console é redirecionada para as páginas iniciais do HTML5 correspondentes para provedores de serviços e tenants. Você pode usar a ferramenta de gerenciamento de célula para habilitar o Web Console.

### Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional de qualquer uma das células do vCloud Director.
- 2 Habilite o Web Console usando a ferramenta de gerenciamento de célula.
  - Para habilitar o Web Console para todos os usuários, execute o seguinte comando.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n flex.ui.enabled -v true
```

- Para habilitar o Web Console apenas para administradores do sistema, execute o seguinte comando.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n flex.ui.enabled -v sys-
admin-only
```

Tabela 10-2. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `manage-config`

Opção	Argumento	Descrição
<code>--name (-n)</code>	<code>flex.ui.enabled</code>	O sinalizador para habilitar ou desativar o Web Console.
<code>--value (-v)</code>	<code>false</code> (padrão)	<p>O argumento <code>false</code> desativa o Web Console. Esse é o comportamento padrão.</p> <ul style="list-style-type: none"> <li>■ <code>base_cell_URL/</code> - nenhum redirecionamento, recarrega a página de login.</li> <li>■ <code>base_cell_URL/cloud</code> - redireciona para <code>/provider</code>.</li> <li>■ <code>base_cell_URL/cloud/login.jsp</code> - redireciona para <code>/provider</code>.</li> <li>■ <code>base_cell_URL/cloud/org/organization_name</code> - redireciona para <code>/tenant/organization_name</code>.</li> </ul>
	<code>true</code>	<p>O argumento <code>true</code> habilita o Web Console.</p> <ul style="list-style-type: none"> <li>■ <code>base_cell_URL/</code> - nenhum redirecionamento, recarrega a página de login.</li> <li>■ <code>base_cell_URL/cloud</code> - nenhum redirecionamento.</li> <li>■ <code>base_cell_URL/cloud/login.jsp</code> - nenhum redirecionamento.</li> <li>■ <code>base_cell_URL/cloud/org/organization_name</code> - nenhum redirecionamento.</li> </ul>
	<code>sys-admin-only</code>	<p>O argumento <code>sys-admin-only</code> habilita o Web Console para administradores de sistema.</p> <ul style="list-style-type: none"> <li>■ <code>base_cell_URL/</code> - nenhum redirecionamento, recarrega a página de login.</li> <li>■ <code>base_cell_URL/cloud</code> - nenhum redirecionamento.</li> <li>■ <code>base_cell_URL/cloud/login.jsp</code> - nenhum redirecionamento.</li> <li>■ <code>base_cell_URL/cloud/org/organization_name</code> - redireciona para <code>/tenant/organization_name</code>.</li> </ul>

- 3 Reinicie a célula do vCloud Director para que as alterações entrem em vigor.

```
service vmware-vcd restart
```

#### Próximo passo

- Para acessar o vCloud Director Web Console, navegue até `https://hostname.domain.tld/cloud` e faça login como um administrador de sistema ou navegue até `https://vcloud.example.com/cloud/org/myOrg` para fazer login na sua organização. Para obter mais informações sobre o vCloud Director Web Console, consulte o *Guia do Administrador do vCloud Director* versão 9.7 e o *Guia do Usuário do vCloud Director* versão 9.7.
- Para desativar o vCloud Director Web Console e retornar ao comportamento padrão, execute o seguinte comando.

```
cell-management-tool manage-config -n flex.ui.enabled -v false
```

## Desativar o acesso do provedor de serviços ao endpoint da API herdada

A partir do vCloud Director 10.0, você pode usar endpoints separados de login do vCloud Director OpenAPI para o provedor de serviços e de acesso de tenant ao vCloud Director.

O vCloud Director 10.0 introduz dois novos endpoints do OpenAPI que você pode usar para aumentar a segurança restringindo o acesso ao vCloud Director.

- `/cloudapi/1.0.0/sessions/provider` - Endpoint do OpenAPI para o login do provedor de serviços. Os tenants não podem acessar o vCloud Director usando este endpoint.
- `/cloudapi/1.0.0/sessions/` - Endpoint do OpenAPI para o login do tenant. Os provedores de serviços não podem acessar o vCloud Director usando esse endpoint.

Por padrão, os administradores de provedor e os usuários da organização podem acessar o vCloud Director fazendo login no endpoint da API do `/api/sessions`.

Usando o subcomando `manage-config` da ferramenta de gerenciamento de célula, você pode desativar o acesso do provedor de serviços ao endpoint da API do `/api/sessions` e, como resultado, limitar o login do provedor ao novo endpoint do `/cloudapi/1.0.0/sessions/provider` OpenAPI que é acessível apenas para os provedores de serviços.

#### Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional de qualquer uma das células do vCloud Director.
- 2 Para bloquear o acesso do provedor ao endpoint da API do `/api/sessions`, use a ferramenta de gerenciamento de célula e execute o seguinte comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n  
vcloud.api.legacy.nonprovideronly -v true
```

## Resultados

O endpoint da API do `/api/sessions` não está mais acessível para provedores de serviços. Os provedores de serviços podem usar o novo endpoint do OpenAPI `/cloudapi/1.0.0/sessions/provider` para acessar o vCloud Director. Os tenants podem acessar o vCloud Director usando o endpoint da API `/api/sessions` e o novo endpoint do OpenAPI `/cloudapi/1.0.0/sessions/`.

## Próximo passo

Para habilitar o acesso do provedor ao endpoint da API do `/api/sessions`, execute o seguinte comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v false
```

## Como gerenciar uma célula

Use o subcomando `cell` da ferramenta de gerenciamento de célula para suspender o agendador de tarefas para que novas tarefas não possam ser iniciadas, para exibir o status de tarefas ativas, para controlar o modo de manutenção da célula ou para encerrar a célula normalmente.

Para gerenciar uma célula, use uma linha de comando da seguinte forma:

```
cell-management-tool cell -u sysadmin-username -p sysadmin-password opção
```

onde *sysadmin-username* e *sysadmin-password* são o nome de usuário e a senha do **administrador do sistema**.

**Observação** Por motivos de segurança, você pode omitir a senha. Nesse caso, o comando solicita que você digite a senha sem exibi-la na tela.

Como alternativa ao fornecimento de credenciais do **administrador do sistema**, você pode usar a opção `--pid` e fornecer o ID de processo da célula. Para encontrar o ID de processo da célula, use um comando como este:

```
cat /var/run/vmware-vcd-cell.pid
```

**Tabela 10-3. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `cell`**

Opção	Argumento	Descrição
<code>--help</code> (-h)	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--pid</code> (-i)	ID de processo da célula	Você pode usar essa opção em vez de <code>-username</code> .

**Tabela 10-3. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `cell` (continuação)**

Opção	Argumento	Descrição
<code>--maintenance</code> (-m)	true ou false	Define a célula no modo de manutenção.  O argumento <code>true</code> desativa a atividade na célula e coloca a célula no modo de manutenção.  O argumento <code>false</code> tira a célula do modo de manutenção.
<code>--password</code> (-p)	Senha do <b>administrador do sistema</b> do vCloud Director	Opcional se a opção <code>--username</code> for usada.  Se você omitir essa opção, o comando solicitará que você digite a senha sem exibi-la na tela.
<code>--quiesce</code> (-q)	true ou false	Desativa a atividade na célula.  O argumento <code>true</code> suspende o programador.  O argumento <code>false</code> reinicia o programador.
<code>--shutdown</code> (-s)	Nenhum	Encerra normalmente os serviços do vCloud Director no servidor.
<code>--status</code> (-t)	Nenhum	Exibe informações sobre o número de tarefas em execução na célula e o status da célula.
<code>--status-verbose</code> (-tt)	Nenhum	Exibe informações detalhadas sobre as tarefas em execução na célula e o status da célula.
<code>--username</code> (-u)	Nome de usuário do <b>administrador do sistema</b> do vCloud Director.	Você pode usar essa opção em vez de <code>--pid</code> .

## Como gerenciar aplicativos de célula

Use o comando `cell-application` da ferramenta de gerenciamento de célula para controlar o conjunto de aplicativos que a célula executa na inicialização.

O vCloud Director executa uma série de aplicativos que fornecem serviços que os clientes do vCloud Director necessitam. A célula inicia um subconjunto desses aplicativos por padrão. Normalmente, todos os membros desse subconjunto são necessários para suportar uma instalação do vCloud Director.

Para exibir ou alterar a lista de aplicativos que são executados quando a célula é iniciada, use uma linha de comando com o seguinte formato:

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell-application command
```

### **sysadmin-username**

Nome de usuário de um administrador do sistema do vCloud Director

### **sysadmin-password**

Senha do administrador do sistema do vCloud Director. Você deverá usar a senha se ela contiver caracteres especiais.

**Observação** Você pode fornecer a senha de administrador do sistema do vCloud Director na linha do comando `cell-management-tool`, mas é mais seguro omitir a senha. Isso faz com que o `cell-management-tool` solicite a senha, que não aparece na tela quando você a digita.

Como alternativa ao fornecimento de credenciais de administrador do sistema, você pode usar a opção `--pid` e fornecer o ID de processo da célula. Para encontrar o ID de processo da célula, use um comando como este:

```
cat /var/run/vmware-vcd-cell.pid
```

### **command**

subcomando `cell-application`.

**Tabela 10-4. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `cell-application`**

Comando	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--application-states</code>	Nenhuma	Lista os aplicativos de célula e seus estados atuais.
<code>--disable</code>	ID do aplicativo	Impede que este aplicativo de célula seja executado na inicialização da célula.
<code>--enable</code>	ID do aplicativo	Permite que este aplicativo de célula seja executado na inicialização da célula.
<code>--pid (-i)</code>	ID de processo da célula	Você pode usar essa opção em vez de <code>-u</code> ou <code>-u</code> e <code>-p</code> .
<code>--list</code>	Nenhum	Liste todos os aplicativos de célula e mostre se eles estão ativados para execução na inicialização da célula.
<code>--password (-p)</code>	Senha do administrador do vCloud Director	Opcional. O comando solicitará a senha se você não a fornecer na linha de comando.



**Tabela 10-4. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando cell-application (continuação)**

Comando	Argumento	Descrição
--set	Lista separada por ponto-e-vírgula de IDs do aplicativo.	Especifique o conjunto de aplicativos de célula que são executados na inicialização da célula. Esse comando substitui o conjunto existente de aplicativos de célula que são executados na inicialização da célula. Use --enable ou --disable para alterar o estado de inicialização de um único aplicativo.
--username (-u)	Nome de usuário do administrador do vCloud Director.	Obrigatório se não especificar --pid

## Exemplo: Listar aplicativos de célula e seus estados de inicialização

A seguinte linha de comando cell-management-tool requer credenciais de administrador do sistema e retorna a lista de aplicativos de célula e seus estados de inicialização.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell-
application --list
Please enter the administrator password:
```

name	id	enabled	description
Networking	com.vmware.vc...	true	Exposes NSX api endpoints directly from vCD.
Console Proxy	com.vmware.vc...	true	Proxies VM console data connection...
Cloud Proxy	com.vmware.vc...	true	Proxies TCP connections from a tenant site.
Compute Service Broker	com.vmware.vc...	true	Allows registering with a service control...
Maintenance Application	com.vmware.vc...	false	Indicates to users the cell is undergo ...
Core Cell Application	com.vmware.vc...	true	Main cell application, Flex UI and REST API.

## Como atualizar as propriedades de conexão do banco de dados

Você pode atualizar as propriedades de conexão do banco de dados do vCloud Director usando o subcomando reconfigure-database da ferramenta de gerenciamento de célula.

Durante a instalação do vCloud Director ou o processo de implantação do dispositivo vCloud Director, você configura as propriedades de tipo de banco de dados e conexões de banco de dados. Consulte [Capítulo 5 Instalar o vCloud Director no Linux](#) e [Capítulo 6 Implantação do vCloud DirectorAppliance](#).

Após concluir a configuração do banco de dados do vCloud Director, você pode atualizar as conexões de banco de dados usando o subcomando `reconfigure-database`. Você pode mover o banco de dados existente do vCloud Director para um novo host, alterar o nome de usuário do banco de dados e a senha ou ativar uma conexão SSL com um banco de dados PostgreSQL.

```
cell-management-tool reconfigure-database options
```

**Importante** As alterações feitas executando o comando `reconfigure-database` são gravadas no arquivo de configuração global `global.properties` e o arquivo de resposta `responses.properties` da célula. Antes de executar o comando, verifique se o arquivo de resposta está presente em `/opt/vmware/vcloud-director/etc/responses.properties` e é gravável. Para obter informações sobre como proteger e reutilizar o arquivo de resposta, consulte [Capítulo 5 Instalar o vCloud Director no Linux](#).

Se você não usar a opção `--pid`, deverá reiniciar a célula para aplicar as alterações.

**Tabela 10-5. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `reconfigure-database`**

Opção	Argumento	Descrição
<code>--help</code> ( <code>-h</code> )	Nenhum	Fornecer um resumo das opções disponíveis nessa categoria.
<code>--database-host</code> ( <code>-dbhost</code> )	Endereço IP ou nome de domínio completo do host do banco de dados do vCloud Director	Atualiza o valor da propriedade <code>database.jdbcUrl</code> .  <b>Importante</b> O comando valida apenas o formato do valor.
<code>--database-instance</code> ( <code>-dbinstance</code> )	Instância do banco de dados SQL Server.	Opcional. Usado se o tipo de banco de dados for <code>sqlserver</code> .  <b>Importante</b> Se você incluir essa opção, deverá fornecer o mesmo valor que especificou ao configurar o banco de dados pela primeira vez.
<code>--database-name</code> ( <code>-dbname</code> )	O nome do serviço do banco de dados.	Atualiza o valor da propriedade <code>database.jdbcUrl</code> .
<code>--database-password</code> ( <code>-dbpassword</code> )	Senha para o usuário do banco de dados.	Atualiza o valor da propriedade <code>database.password</code> . A senha que você digita é criptografada antes de ser armazenada como um valor de propriedade.
<code>--database-port</code> ( <code>-dbport</code> )	O número da porta usado pelo serviço do banco de dados no host do banco de dados.	Atualiza o valor da propriedade <code>database.jdbcUrl</code> .  <b>Importante</b> O comando valida apenas o formato do valor.

Tabela 10-5. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `reconfigure-database` (continuação)

Opção	Argumento	Descrição
<code>--database-type</code> ( <code>-dbtype</code> )	O tipo de banco de dados. Um destes: ■ <code>sqlserver</code> ■ <code>postgres</code>	Atualiza o valor da propriedade do <code>database.jdbcUrl</code> .
<code>--database-user</code> ( <code>-dbuser</code> )	Nome de usuário do usuário de banco de dados.	Atualiza o valor da propriedade do <code>database.user</code> .
<code>--database-ssl</code>	<code>true</code> ou <code>false</code>	Usado se o tipo de banco de dados for <code>postgres</code> . Configura o banco de dados do PostgreSQL para solicitar uma conexão SSL do vCloud Director.
<code>--pid</code> ( <code>-i</code> )	O ID de processo da célula.	Opcional. Executa uma reconfiguração ativa em uma célula do vCloud Director em execução. Não requer uma reinicialização da célula.  Se for usado com o <code>--private-key-path</code> , você poderá executar o comando em células locais e remotas imediatamente.
<code>--private-key-path</code>	Nome do caminho para a Private Key da célula.	Opcional. Todas as células no grupo de servidores encerram normalmente, atualizam suas propriedades de banco de dados e reiniciam.  <b>Importante</b> Todas as células devem permitir conexões SSH pelo superusuário sem uma senha.
<code>--remote-sudo-user</code>	Um nome de usuário com direitos de <code>sudo</code> .	Usado com a opção <code>--private-key-path</code> quando o usuário remoto é diferente de <b>raiz</b> .  Para o dispositivo, você pode usar essa opção para o usuário <b>postgres</b> , por exemplo, <code>--remote-sudo-user=postgres</code> .

Quando você usa as opções `--database-host` e `--database-port`, o comando valida o formato dos argumentos, mas não testa a acessibilidade de rede da combinação de host e porta nem a presença de um banco de dados do tipo especificado.

Se você usar a opção de `--private-key-path`, todas as células deverão ser configuradas para permitir conexões SSH do superusuário sem uma senha. Para executar uma verificação, por exemplo, você pode executar o seguinte comando do Linux:

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

Esse exemplo define a sua identidade como `vcloud` e, em seguida, faz uma conexão SSH à célula em *cell-ip* como raiz, mas não fornece a senha raiz. Se a private key em *private-key-path* na célula local puder ser lida pelo usuário `vcloud.vcloud`, e a chave pública correspondente estiver presente no arquivo `authorized-keys` para o usuário raiz em *cell-ip*, o comando será bem-sucedido.

**Observação** O usuário do `vcloud`, o grupo do `vcloud` e a conta do `vcloud.vcloud` são criados pelo instalador do vCloud Director para ser usado como uma identidade com a qual os processos do vCloud Director são executados. O usuário do `vcloud` não tem nenhuma senha.

## Exemplo: Alterar o nome de usuário e a senha do banco de dados do vCloud Director

Para alterar o nome de usuário e a senha do banco de dados do vCloud Director, deixando todas as outras propriedades de conexão como originalmente configuradas, você pode executar o comando a seguir:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \ -dbuser vcd-dba -dbpassword P@55w0rd
```

## Exemplo: Atualizar o endereço IP do banco de dados do vCloud Director por meio da reconfiguração ativa em todas as células

Se você for um usuário não raiz com direitos de `sudo`, para alterar o endereço IP do banco de dados do vCloud Director em todas as células imediatamente, você pode executar o seguinte comando:

```
[sudo@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \ --dbhost db_ip_address -i $(service vmware-vcd pid cell) --private-key-path=path_to_private-key \ --remote-sudo-user=non-root-user
```

## Detectar e reparar dados corrompidos do agendador

O vCloud Director usa o Agendador de trabalhos Quartz para coordenar as operações assíncronas (trabalhos) em execução no sistema. Se o banco de dados do agendador Quartz for corrompido, você poderá não conseguir desativar o sistema com êxito. Use o comando `fix-scheduler-data` da ferramenta de gerenciamento de célula para verificar se há dados corrompidos do agendador do banco de dados e reparar esses dados conforme necessário.

Para verificar se há dados corrompidos no agendador, use uma linha de comando com o seguinte formato:

```
cell-management-tool fix-scheduler-data options
```

**Tabela 10-6. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `fix-scheduler-data`**

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--dbuser</code>	Nome do usuário de banco de dados do vCloud Director.	Deve ser fornecido na linha de comando.
<code>--dbpassword</code>	Senha do usuário de banco de dados do vCloud Director.	Solicitado se não for fornecido.

## Como gerar certificados autoassinados para os endpoints de proxy de console e HTTP

Use o comando `generate-certs` da ferramenta de gerenciamento de célula para gerar certificados SSL autoassinados para os endpoints de proxy de console e HTTP

Cada grupo de servidores do vCloud Director deve oferecer suporte a dois endpoints SSL: um para o serviço HTTP e outro para o serviço de proxy do console. O endpoint do serviço HTTP oferece suporte ao vCloud Director Service Provider Admin Portal, ao vCloud Director Tenant Portal e à API do vCloud. O endpoint de proxy de console remoto oferece suporte a conexões VMRC para vApps e VMs.

O comando `generate-certs` da ferramenta de gerenciamento de célula automatiza o procedimento [Criar certificados SSL autoassinados para o vCloud Director no Linux](#).

Para gerar novos certificados SSL autoassinados e adicioná-los a um armazenamento de chaves novo ou existente, use uma linha de comando da seguinte forma:

```
cell-management-tool generate-certs options
```

**Tabela 10-7. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `generate-certs`**

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--expiration (-x)</code>	<i>days-until-expiration</i>	Número de dias até que os certificados expirem. O padrão é 365

**Tabela 10-7. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando generate-certs (continuação)**

Opção	Argumento	Descrição
--issuer (-i)	<i>name=value</i> [, <i>name=value, ...</i> ]	Nome distinto X.509 do emissor do certificado. O padrão é <i>CN=FQDN</i> , em que <i>FQDN</i> será o nome de domínio completo da célula ou seu endereço IP se nenhum nome de domínio completo estiver disponível. Se você especificar vários pares de valor e atributo, separe-os por vírgulas e coloque o argumento inteiro entre aspas.
--httpcert (-j)	Nenhum	Gere um certificado para o endpoint de http.
--key-size (-s)	<i>key-size</i>	Tamanho do par de chaves expresso como um número inteiro de bits. O padrão é 2048. Os tamanhos de chave menores do que 1024 não têm suporte pela Publicação Especial NIST 800-131A.
--keystore-pwd (-w)	<i>keystore-password</i>	Senha para o armazenamento de chaves desse host.
--out (-o)	<i>keystore-pathname</i>	Nome de caminho completo para o armazenamento de chaves desse host.
--consoleproxycert (-p)	Nenhum	Gere um certificado para o endpoint de proxy de console.

**Observação** Para manter a compatibilidade com versões anteriores desse subcomando, omitir ambos `-j` e `-p` tem o mesmo resultado que fornecer ambos `-j` e `-p`.

## Exemplo: Criação de certificados autoassinados

Dois desses exemplos pressupõem um armazenamento de chaves em `/tmp/cell.ks` que tem a senha `kspw`. Esse armazenamento de chaves será criado se ainda não existir.

Esse exemplo cria os novos certificados usando os padrões. O nome do emissor é definido como `CN=Unknown`. O certificado usa o comprimento de chave de 2048 bits padrão e expira um ano após a criação.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool generate-certs -j -p -o /tmp/cell.ks -w kspw
New keystore created and written to /tmp/cell.ks.
```

Esse exemplo cria um novo certificado somente para o endpoint de http. Ele também especifica valores personalizados para o nome do emissor e o tamanho da chave. O nome do emissor é definido como CN=Test, L=London, C=GB. O novo certificado para a conexão http tem uma chave de 4096 bits e expira 90 dias após a criação. O certificado existente para o endpoint de proxy do console não é afetado.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool generate-certs -j -o /tmp/cell.ks -w kspw -i "CN=Test, L=London, C=GB" -s 4096 -x 90
New keystore created and written to /tmp/cell.ks.
```

**Importante** O arquivo de armazenamento de chaves e o diretório no qual ele é armazenado devem ser legíveis pelo usuário vcloud.vcloud. O instalador do vCloud Director cria esse usuário e grupo.

## Substituindo certificados para os endpoints de proxy de console e HTTP

Use o comando `certificates` da ferramenta de gerenciamento de célula para substituir certificados SSL para os endpoints de proxy de console e HTTP.

O comando `certificates` da ferramenta de gerenciamento de célula automatiza o processo de substituição de certificados existentes por novos certificados armazenados em um armazenamento de chaves JCEKS. Use o comando `certificates` para substituir certificados autoassinados por certificados assinados ou substituir certificados prestes a expirar por certificados novos. Para criar um armazenamento de chaves JCEKS contendo certificados assinados, consulte [Criar certificados SSL autoassinados para o vCloud Director no Linux](#).

Para substituir os certificados SSL de um ou ambos os endpoints, use um comando da seguinte forma:

```
cell-management-tool certificates options
```

Tabela 10-8. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `certificates`

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--config (-c)</code>	nome de caminho completo para o arquivo <code>global.properties</code> da célula	O padrão é <code>\$VCLLOUD_HOME/etc/global.properties</code> .
<code>--https (-j)</code>	Nenhum	Substitua o arquivo de armazenamento de chaves chamado <code>certificates</code> usado pelo endpoint de http.

Tabela 10-8. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `certificates` (continuação)

Opção	Argumento	Descrição
<code>--consoleproxyks (-p)</code>	Nenhum	Substitua o arquivo de armazenamento de chaves chamado <code>proxycertificates</code> usado pelo endpoint de proxy do console.
<code>--responses (-r)</code>	nome de caminho completo para o arquivo <code>responses.properties</code> da célula	O padrão é <code>\$VCLLOUD_HOME/etc/responses.properties</code> .
<code>--keystore (-k)</code>	<i>keystore-pathname</i>	Nome de caminho completo para um armazenamento de chaves JCEKS que contém os certificados assinados. Forma curta <code>-s</code> preterida substituída por <code>-k</code> .
<code>--keystore-password (-w)</code>	<i>keystore-password</i>	Senha para o armazenamento de chaves JCEKS referenciado pela opção <code>--keystore</code> . Substitui as opções <code>-kpassword</code> e <code>--keystorepwd</code> preteridas.

## Exemplo: Substituição de certificados

Você pode omitir as opções `--config` e `--responses`, a menos que esses arquivos tenham sido movidos de suas localizações padrão. Neste exemplo, um armazenamento de chaves em `/tmp/my-new-certs.ks` tem a senha `kspw`. Este exemplo substitui o certificado de endpoint de `http` existente da célula por um certificado encontrado no `/tmp/my-new-certs.ks`

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool certificates -j -k /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

**Observação** Você deverá reiniciar a célula depois de substituir os certificados.

## Importação de certificados SSL de serviços externos

Use o comando `import-trusted-certificates` da ferramenta de gerenciamento de célula para importar certificados a serem usados no estabelecimento de conexões seguras com serviços externos, como o AMQP e o banco de dados do vCloud Director.



Antes que ele possa fazer uma conexão segura com um serviço externo, o vCloud Director deve estabelecer uma cadeia de confiança válida para esse serviço importando os certificados do serviço para seu próprio truststore. Para importar certificados confiáveis para o truststore da célula, use um comando da seguinte forma:

```
cell-management-tool import-trusted-certificates options
```

**Tabela 10-9. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando import-trusted-certificates**

Opção	Argumento	Descrição
--help (-h)	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
--destination	nome do caminho	Nome completo do caminho para o truststore de destino. O padrão será /opt/vmware/vcloud-director/etc/certificates se não for fornecido na linha de comando.
--destination-password	cadeia de caracteres	Senha para o truststore de destino. O padrão será o valor de vcloud.ssl.truststore.password se não for fornecido na linha de comando.
--destination-type	tipo de armazenamento de chaves	Tipo de armazenamento de chaves do truststore de destino. Pode ser JKS ou JCEKS. O padrão é JCEKS.
--force	Nenhum	Substitui os certificados existentes no truststore de destino.
--source	nome do caminho	Nome completo do caminho para o arquivo PEM de origem.

## Exemplo: Como importar certificados confiáveis

Este exemplo importa os certificados de /tmp/demo.pem para o armazenamento de chaves local do vCloud Director em /opt/vmware/vcloud-director/etc/certificates. O vCloud Director armazena a senha do armazenamento de chaves em um formato criptografado que o comando import-trusted-certificates descriptografa.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool import-trusted-certificates --source /tmp/demo.pem
```

## Gerenciamento da lista de codificações SSL permitidas

Use o comando `ciphers` da ferramenta de gerenciamento de célula para configurar os pacotes de codificação que a célula oferece para usar durante o processo de handshake de SSL.

Quando um cliente faz uma conexão SSL com uma célula do vCloud Director, a célula oferece para usar apenas as codificações configuradas na sua lista padrão de codificações permitidas. Várias codificações não estão nessa lista, porque não são seguras o suficiente para proteger a conexão ou porque são conhecidas por contribuir com falhas de conexão SSL. Quando você instala ou atualiza o vCloud Director, o script de instalação ou atualização examina os certificados da célula. Se qualquer um dos certificados for criptografado usando uma codificação que não está na lista de codificações permitidas, o script modificará a configuração da célula para permitir o uso dessa codificação e exibirá um aviso. Você pode continuar usando os certificados existentes, apesar da dependência dessas codificações, ou pode realizar as seguintes etapas para substituir os certificados e reconfigurar a lista de codificações permitidas:

- 1 Crie novos certificados que não usam nenhuma das codificações não autorizadas. Você pode usar `cell-management-tool ciphers -a`, conforme mostrado em [Listar todas as codificações permitidas](#) para listar todas as codificações permitidas na configuração padrão.
- 2 Use o comando `cell-management-tool certificates` para substituir os certificados existentes da célula pelos novos.
- 3 Use o comando `cell-management-tool ciphers` para reconfigurar a lista de codificações permitidas para excluir quaisquer codificações não usadas pelos novos certificados. A exclusão dessas codificações pode acelerar a conexão SSL com a célula, pois o número de codificações oferecidas durante o handshake é reduzido para o mínimo prático.

**Importante** Como o console do VMRC requer o uso das codificações AES256-SHA e AES128-SHA, não é possível desautorizar os clientes do vCloud Director se eles usarem o console do VMRC.

Para gerenciar a lista de codificações SSL permitidas, use uma linha de comando com o seguinte formato:

```
cell-management-tool ciphers options
```

**Tabela 10-10. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `ciphers`**

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornece um resumo dos comandos disponíveis nessa categoria.
<code>--all-allowed (-a)</code>	Nenhuma	Lista todas as codificações permitidas.

**Tabela 10-10. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando ciphers (continuação)**

Opção	Argumento	Descrição
<code>--compatible-reset (-c)</code>	Nenhum	Redefine para a lista padrão de codificações permitidas e também permite codificações usadas pelos certificados desta célula.
<code>--disallow (-d)</code>	Lista separada por vírgulas de nomes de codificação, conforme publicado em <a href="https://www.openssl.org/docs/man1.0.2/man1/ciphers.html">https://www.openssl.org/docs/man1.0.2/man1/ciphers.html</a>	Desautoriza as codificações na lista separada por vírgulas especificada.
<code>--list (-l)</code>	Nenhuma	Lista as codificações configuradas atualmente.
<code>--reset (-r)</code>	Nenhuma	Redefine para a lista padrão de codificações permitidas. Se os certificados da célula usarem codificações não autorizadas, você não poderá fazer uma conexão SSL com a célula até instalar novos certificados que usam uma codificação permitida.

## Exemplo: Listar todas as codificações permitidas

Use a opção `--all-allowed (-a)` para listar todos as codificações que a célula atualmente tem permissão para oferecer durante um handshake de SSL.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
* TLS_DHE_DSS_WITH_AES_256_CBC_SHA
* TLS_DHE_DSS_WITH_AES_128_CBC_SHA
* TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
* TLS_DHE_RSA_WITH_AES_256_CBC_SHA
* TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
```

```
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

## Exemplo: Desautorizar duas codificações

Use a opção `--disallow (-d)` para remover uma ou mais codificações da lista de codificações permitidas. Essa opção requer pelo menos um nome de codificação. Você pode fornecer vários nomes de codificação numa lista separada por vírgulas. Você pode obter nomes para essa lista da saída de `ciphers -a`. Este exemplo remove duas codificações listadas no exemplo anterior.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -d
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

## Gerenciar a lista de protocolos SSL permitidos

Use o comando `ssl-protocols` da ferramenta de gerenciamento de célula para configurar o conjunto de protocolos SSL que a célula oferece para usar durante o processo de handshake de SSL.

Quando um cliente faz uma conexão SSL com uma célula do vCloud Director, a célula oferece para usar apenas os protocolos configurados na sua lista de protocolos SSL permitidos. Vários protocolos, incluindo TLSv1, SSLv3 e SSLv2Hello, não estão na lista padrão, pois são conhecidos por apresentarem sérias vulnerabilidades de segurança.

Para gerenciar a lista de protocolos SSL permitidos, use uma linha de comando com o seguinte formato:

```
cell-management-toolssl-protocolsoptions
```

**Tabela 10-11. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `ssl-protocols`**

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--all-allowed (-a)</code>	Nenhuma	Lista todos os protocolos SSL que o vCloud Director pode suportar.
<code>--disallow (-d)</code>	Lista separada por vírgulas de nomes de protocolo SSL.	Reconfigura a lista de protocolos SSL não permitidos para aqueles especificados na lista.

**Tabela 10-11. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `ssl-protocols` (continuação)**

Opção	Argumento	Descrição
<code>--list (-l)</code>	Nenhuma	Lista o conjunto de protocolos SSL permitidos que o vCloud Director está atualmente configurado para suportar.
<code>--reset (-r)</code>	Nenhuma	Redefine a lista de protocolos SSL configurados para o padrão de fábrica

**Importante** Você deve reinicializar a célula depois de executar `ssl-protocols --disallow` ou `ssl-protocols reset`

## Exemplo: Lista protocolos SSL permitidos e configurados

Use a opção `--all-allowed (-a)` para listar todos os protocolos SSL que a célula pode ter permissão para oferecer durante um handshake de SSL.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

* TLSv1.2
* TLSv1.1
* TLSv1
* SSLv3
* SSLv2Hello
```

Essa lista normalmente é um superconjunto dos protocolos SSL que a célula está configurada para suportar. Para listar esses protocolos SSL, use a opção `--list (-l)`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

* TLSv1.2
* TLSv1.1
```

## Exemplo: Reconfigura a lista de protocolos SSL não permitidos

Use a opção `--disallow (-d)` para reconfigurar a lista de protocolos SSL não permitidos. Essa opção requer uma lista separada por vírgulas do subconjunto de protocolos permitidos produzidos por `ssl-protocols -a`.

Este exemplo atualiza a lista de protocolos SSL permitidos para incluir TLSv1. Versões do VMware® vCenter™ anteriores à 5.5 Update 3e requerem o TLSv1.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -d SSLv3,SSLv2Hello
```

Você deve reiniciar a célula após executar esse comando.

## Como configurar a coleção de métricas

Use o comando `configure-metrics` da ferramenta de gerenciamento de célula para configurar o conjunto de métricas a serem coletadas.

O vCloud Director pode coletar métricas que fornecem informações atuais e históricas sobre o consumo de recursos e o desempenho da máquina virtual. Use esse subcomando para configurar as métricas que o vCloud Director coleta. Use o subcomando `cell-management-tool cassandra` para configurar um banco de dados Cassandra Apache para uso como um repositório de métricas do vCloud Director. Consulte [Configuração de um banco de dados de métricas do Cassandra](#).

Para configurar as métricas que o vCloud Director coleta, use uma linha de comando da seguinte forma:

```
cell-management-tool configure-metrics --metrics-config pathname
```

**Tabela 10-12. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `configure-metrics`**

Comando	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--repository-host</code> (obsoleto)	Nome do host ou endereço IP do host do KairosDB	Obsoleto. Use a opção <code>--cluster-nodes</code> do subcomando <code>cell-management-tool cassandra</code> para configurar um banco de dados Cassandra Apache para uso como um repositório de métricas do vCloud Director.
<code>--repository-port</code> (obsoleto)	A porta KairosDB a ser usada.	Obsoleto. Use a opção <code>--port</code> do subcomando <code>cell-management-tool cassandra</code> para configurar um banco de dados Cassandra Apache para uso como um repositório de métricas do vCloud Director.
<code>--metrics-config</code>	nome do caminho	Caminho para o arquivo de configuração de métricas

## Exemplo: Como configurar uma conexão do banco de dados de métricas

Este exemplo configura a coleção de métricas conforme especificado no arquivo `/tmp/metrics.groovy`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool configure-metrics --metrics-config /tmp/metrics.groovy
```

O serviço de coleta de métricas do vCloud Director implementa um subconjunto das métricas coletadas pelo vSphere Performance Manager. Consulte a documentação do vSphere Performance Manager para obter mais informações sobre os nomes de métricas e os parâmetros de coleta. O arquivo `metrics-config` cita um ou mais nomes de métrica e fornece os parâmetros de coleta de cada métrica citada. Por exemplo:

```
configuration {
  metric("cpu.usage.average")
  metric("cpu.usagemhz.average")
  metric("cpu.usage.maximum")
  metric("disk.used.latest") {
    currentInterval=300
    historicInterval=300
    entity="VM"
    instance=""
    minReportingInterval=1800
    aggregator="AVERAGE"
  }
}
```

Há suporte para os seguintes nomes de métrica.

Tabela 10-13. Nomes de métrica

Nome de métrica	Descrição
<code>cpu.usage.average</code>	Modo de host da CPU média usada ativamente desta máquina virtual como uma porcentagem do total disponível. Inclui todos os núcleos em todos os soquetes.
<code>cpu.usagemhz.average</code>	Modo de host da CPU média usada ativamente desta máquina virtual como uma medição bruta. Inclui todos os núcleos em todos os soquetes.
<code>cpu.usage.maximum</code>	Modo de host da CPU máxima usada ativamente desta máquina virtual como uma porcentagem do total disponível. Inclui todos os núcleos em todos os soquetes.
<code>mem.usage.average</code>	Memória usada por esta máquina virtual como uma porcentagem do total de memória configurada.
<code>disk.provisioned.latest</code>	Espaço de armazenamento alocado a este disco rígido virtual no centro de dados virtual da organização contentora.
<code>disk.used.latest</code>	Armazenamento usado por todos os discos rígidos virtuais.
<code>disk.read.average</code>	Taxa de leitura média de todos os discos rígidos virtuais.
<code>disk.write.average</code>	Taxa de gravação média de todos os discos rígidos virtuais.

**Observação** Quando uma máquina virtual tem vários discos, as métricas são relatadas de forma agregada para todos os discos. As métricas de CPU são uma agregação de todos os soquetes e núcleos.

Para cada métrica nomeada, você pode especificar os seguintes parâmetros de coleta.

**Tabela 10-14. Parâmetros de coleta de métricas**

Nome do parâmetro	Valor	Descrição
currentInterval	Quantidade de segundos em número inteiro.	O intervalo em segundos a ser usado ao consultar os valores de métrica disponíveis mais recentes (para consultas de métricas atuais). Se não for especificado, o padrão será 20. Valores maiores do que 20 só têm suporte para as métricas de nível 1, conforme definido pelo vSphere Performance Manager.
historicInterval	Quantidade de segundos em número inteiro.	O intervalo em segundos a ser usado ao consultar os valores de métricas históricas. Se não for especificado, o padrão será 20. Valores maiores do que 20 só têm suporte para as métricas de nível 1, conforme definido pelo vSphere Performance Manager.
entity	Um destes: HOST, VM	O tipo de objeto VC para o qual a métrica está disponível. Se não for especificado, o padrão será a VM. Nem todas as métricas estão disponíveis para todas as entidades.
instance	Um identificador de instância PerfMetricId do vSphere Performance Manager.	Indica se deve ser realizada a recuperação de dados para instâncias individuais de uma métrica (núcleos da CPU individuais, por exemplo), um agregado de todas as instâncias ou ambos. Um valor de "*" coleta todas as métricas, instâncias e agregados. Uma cadeia de caracteres vazia, "", coleta apenas os dados agregados. Uma cadeia de caracteres específica como "DISKFILE" coleta dados apenas para essa instância. Se não for especificado, o padrão será "*" .
minReportingInterval	Quantidade de segundos em número inteiro.	Especifica um intervalo de agregação padrão em questão de segundos para uso ao relatar dados de séries de tempo. Fornece maior controle sobre o relatório de granularidade quando a granularidade do intervalo de coleção não é suficiente. O padrão é 0 (nenhum intervalo de geração de relatórios dedicado)
aggregator	Um destes: AVERAGE, MINIMUM, MAXIMUM e SUMMATION	O tipo de agregação a ser executado durante o minReportingInterval. Se não for especificado, o padrão será AVERAGE.

## Configuração de um banco de dados de métricas do Cassandra

Use o comando `cassandra` da ferramenta de gerenciamento de célula para conectar a célula a um banco de dados de métricas opcional.



O vCloud Director pode coletar métricas que fornecem informações atuais e históricas sobre o consumo de recursos e o desempenho da máquina virtual. Use esse subcomando para configurar um banco de dados Cassandra Apache para uso como um repositório de métricas do vCloud Director. Use o subcomando `cell-management-tool configure-metrics` para ferramenta para configurar o conjunto de métricas a serem coletadas. Consulte [Como configurar a coleção de métricas](#).

Os dados de métricas históricas são armazenados em um banco de dados Cassandra Apache. Consulte [Instalar e configurar um banco de dados Cassandra para armazenar dados de métricas de históricos](#) para obter mais informações sobre como configurar o software de banco de dados opcional para armazenar e recuperar as métricas de desempenho.

Para criar uma conexão entre o vCloud Director e um banco de dados Cassandra Apache, use uma linha de comando da seguinte forma:

```
cell-management-tool cassandra options
```

**Tabela 10-15. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `cassandra`**

Comando	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo das opções disponíveis para esse comando.
<code>--add-rollup</code>	Nenhum	Atualiza o esquema de métricas para incluir métricas acumuladas. Consulte <a href="#">Instalar e configurar um banco de dados Cassandra para armazenar dados de métricas de históricos</a> .
<code>--cluster-nodes</code>	<i>address</i> [, <i>address</i> ... ]	Lista separada por vírgula dos nós do cluster Cassandra a serem usados para as métricas do vCloud Director.
<code>--clean</code>	Nenhum	Remova as definições de configuração do Cassandra do banco de dados do vCloud Director.
<code>--configure</code>	Nenhum	Configure vCloud Director para uso com um cluster Cassandra existente.
<code>--dump</code>	Nenhum	Despeje a configuração de conexão atual.
<code>--keyspace</code>	cadeia de caracteres	Defina o nome de keyspace do vCloud Director no Cassandra como <i>cadeia de caracteres</i> . O padrão é <code>vcloud_metrics</code> .

**Tabela 10-15. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando cassandra (continuação)**

Comando	Argumento	Descrição
<code>--offline</code>	Nenhum	Configure o Cassandra para uso pelo vCloud Director, mas não teste a configuração por conexão com o vCloud Director.
<code>--password</code>	cadeia de caracteres	Senha do usuário do banco de dados Cassandra
<code>--port</code>	número inteiro	Porta à qual se conectar em cada nó de cluster. O padrão é 9042.
<code>--ttl</code>	número inteiro	Mantenha os dados de métricas por dias de <i>número inteiro</i> . Defina o <i>número inteiro</i> como 0 para manter os dados de métricas para sempre.
<code>--update-schema</code>	Nenhum	Inicializa o esquema do Cassandra para manter os dados de métricas do vCloud Director.
<code>--username</code>	cadeia de caracteres	Nome de usuário do usuário do banco de dados Cassandra.

## Exemplo: Configure uma conexão do banco de dados Cassandra

Use um comando como esse, em que *node1-ip*, *node2-ip*, *node3-ip* e *node4-ip* são o endereço IP dos membros do cluster Cassandra. A porta padrão (9042) é usada. Os dados de métricas são mantidos por 15 dias.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --configure --create-schema \
--cluster-nodes node1-ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P@55w0rd' --ttl 15
```

Você deve reiniciar a célula após a conclusão desse comando.

## Recuperação da senha do administrador do sistema

Se você souber o nome de usuário e senha do banco de dados do vCloud Director, poderá usar o comando `recover-password` da ferramenta de gerenciamento de célula para recuperar a senha do administrador do sistema do vCloud Director.

Com o comando `recover-password` da ferramenta de gerenciamento de célula, um usuário que conhece o nome de usuário e a senha do banco de dados do vCloud Director pode recuperar a senha do administrador do sistema do vCloud Director.

Para recuperar a senha do administrador do sistema, use uma linha de comando da seguinte forma:

```
cell-management-tool recover-password options
```

**Tabela 10-16. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `recover-password`**

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--dbuser</code>	Nome do usuário de banco de dados do vCloud Director.	Deve ser fornecido na linha de comando.
<code>--dbpassword</code>	Senha do usuário de banco de dados do vCloud Director.	Solicitado se não for fornecido.

## Atualizar o status de falha de uma tarefa

Use o comando `fail-tasks` da ferramenta de gerenciamento de célula para atualizar o status de conclusão associado a tarefas que estavam em execução quando a célula foi encerrada deliberadamente. Você não pode usar o comando `fail-tasks`, a menos que todas as células tenham sido encerradas.

Quando você desativar uma célula usando o comando `cell-management-tool -q`, as tarefas em execução deverão ser encerradas normalmente dentro de alguns minutos. Se as tarefas continuarem a ser executadas em uma célula que foi desativada, o superusuário poderá encerrar a célula, o que força a falha das tarefas em execução. Após um desligamento que forçou o encerramento da execução de tarefas, o superusuário pode executar `cell-management-tool fail-tasks` para atualizar o status de conclusão dessas tarefas. A atualização do status de conclusão de uma tarefa dessa maneira é opcional, mas ajuda a manter a integridade dos logs do sistema, identificando claramente as falhas causadas por uma ação administrativa.

Para gerar uma lista de tarefas que ainda estão em execução em uma célula desativada, use uma linha de comando com o seguinte formato:

```
cell-management-tool -u sysadmin-username cell --status-verbose
```

**Tabela 10-17. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando fail-tasks**

Comando	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornece um resumo dos comandos disponíveis nessa categoria.
<code>--message (-m)</code>	Texto da mensagem.	O texto da mensagem a ser colocado no status de conclusão da tarefa.

## Exemplo: Tarefas de falha em execução na célula

Este exemplo atualiza o status de conclusão de tarefa associado a uma tarefa que ainda estava em execução quando a célula foi encerrada.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool fail-tasks -m "administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system, Organization: org1
Would you like to fail the tasks listed above?
```

Digite **y** para atualizar a tarefa com um status de conclusão de **desligamento administrativo**. Digite **n** para permitir que a tarefa continue em execução.

**Observação** Se várias tarefas forem retornadas na resposta, você deverá decidir falhar todas ou não executar nenhuma ação. Não é possível escolher um subconjunto de tarefas para falhar.

## Configurar o tratamento de mensagens de auditoria

Use o comando `configure-audit-syslog` da ferramenta de gerenciamento de célula para configurar a forma como o sistema registra as mensagens de auditoria.

Serviços em todas as mensagens de log de auditoria de célula do vCloud Director para o banco de dados vCloud Director, onde elas são preservadas por 90 dias. Para preservar as mensagens de auditoria por mais tempo, você pode configurar serviços do vCloud Director para enviar as mensagens de auditoria para o utilitário Linux `syslog` além do banco de dados do vCloud Director.

O script de configuração do sistema permite que você especifique como as mensagens de auditoria são tratadas. Consulte "Configurar rede e conexões do banco de dados" no *Guia de instalação e atualização do vCloud Director*. As opções de registro especificadas durante a configuração do sistema são preservadas em dois arquivos: `global.properties` e `responses.properties`. Você pode alterar a configuração de registro de mensagens de auditoria em ambos os arquivos com uma linha de comando da ferramenta de gerenciamento de célula do seguinte formato:

```
cell-management-toolconfigure-audit-syslog options
```

As alterações feitas com este subcomando de ferramenta de gerenciamento de células são preservadas nos arquivos `global.properties` e `responses.properties` da célula. As alterações não entrarão em vigor até você reiniciar a célula.

**Tabela 10-18. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `configure-audit-syslog`**

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--disable (-d)</code>	Nenhuma	Desativa o registro de eventos de auditoria para <code>syslog</code> . Registra eventos de auditoria somente no banco de dados do vCloud Director. Esta opção desfaz a definição dos valores de <code>audit.syslog.host</code> e das propriedades <code>audit.syslog.portem</code> , <code>global.properties</code> e <code>responses.properties</code> .
<code>--syslog-host (-loghost)</code>	Endereço IP ou nome de domínio totalmente qualificado do host do servidor de <code>syslog</code>	Esta opção define o valor da propriedade <code>audit.syslog.host</code> para o endereço especificado ou o nome de domínio totalmente qualificado.
<code>--syslog-port (-logport)</code>	Inteiro no intervalo de 0 a 65535	Esta opção define o valor da propriedade <code>audit.syslog.port</code> para o número inteiro especificado.

Quando você especifica um valor para `--syslog-host`, `--syslog-port` ou ambos, o comando valida que o valor especificado tem o formato correto, mas não testa a combinação de host e porta para acessibilidade de rede ou a presença de um serviço `syslog` em execução.

## Exemplo: Alterar o nome do host do servidor de `syslog`

**Importante** As alterações feitas usando esse comando são gravadas no arquivo de configuração global e no arquivo de resposta. Antes de executar esse comando, verifique se o arquivo de resposta está presente (em `/opt/vmware/vcloud-director/etc/responses.properties`) e é gravável. Consulte "Proteger e reutilizar o arquivo de resposta" no *Guia de upgrade e atualização do vCloud Director*.

Para alterar o host ao qual as mensagens `syslog` são enviadas, use um comando como este:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool configure-audit-syslog -loghost
syslog.example.com
Using default port 514
```

Este exemplo presume que o novo host escuta mensagens syslog na porta padrão.

O comando atualiza `global.properties` e `responses.properties`, mas as alterações não entrarão em vigor até que você reinicie a célula.

## Configurar modelos de e-mail

Use o comando `manage-email` da ferramenta de gerenciamento de célula para gerenciar os modelos que o sistema usa ao criar alertas de e-mail.

O sistema é configurado por padrão para enviar alertas de e-mail que notificam os administradores do sistema sobre eventos e condições que provavelmente exigirão sua intervenção. A lista de destinatários de e-mail pode ser atualizada usando a API do vCloud ou o Console da Web. Você pode substituir o conteúdo de e-mail padrão para cada tipo de alerta usando uma linha de comando da ferramenta de gerenciamento de célula do seguinte formato:

```
cell-management-tool manage-email options
```

**Tabela 10-19. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `manage-email`**

Opção	Argumento	Descrição
<code>--help</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--delete</code>	nome do modelo	O nome do modelo a ser excluído.
<code>--lookup</code>	nome do modelo	Esse argumento é opcional. Se você não o fornecer, o comando retornará uma lista de todos os nomes de modelo.
<code>--locale</code>	localidade do modelo	Por padrão, esse comando opera em modelos na localidade en-US. Use essa opção para especificar uma localidade diferente.
<code>--set-template</code>	nome do caminho para um arquivo que contém um modelo de e-mail atualizado	Esse arquivo deve estar acessível no host local e legível pelo usuário <code>vcloud.vcloud</code> . Por exemplo, <code>/tmp/my-email-template.txt</code>

## Exemplo: Atualizar um modelo de e-mail

O comando seguinte substitui o conteúdo atual do modelo de e-mail

DISK\_STORAGE\_ALERT\_VDCS pelo conteúdo que você criou em um arquivo denominado /tmp/DISK\_STORAGE\_ALERT\_VDCS-new.txt.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-email --set-template
DISK_STORAGE_ALERT_VDCS /tmp/DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s): $pvdcList
"

Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from $productName
The $datastore is used by the followingProvider VDC(s): $pvdcList
"

VCD Email notification details:
name                : DISK_STORAGE_ALERT_VDCS
description         : Alert when used disk storage exceeds threshold
config key          : email.template.DISK_STORAGE_ALERT_VDCS.en-US
template placeholders : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcList]
template content    : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcList
```

## Encontrar VMs órfãs

Use o comando `find-orphan-vms` da ferramenta de gerenciamento de célula para encontrar referências a máquinas virtuais que estão presentes no banco de dados do vCenter, mas não no banco de dados do vCloud Director.

As máquinas virtuais que são referenciadas no banco de dados do vCenter, mas não no banco de dados do vCloud Director, são consideradas VMs órfãs, pois o vCloud Director não pode acessá-las, mesmo que possam estar consumindo recursos de cálculo e armazenamento. Esse tipo de incompatibilidade de referência pode surgir por vários motivos, incluindo cargas de trabalho de alto volume, erros de banco de dados e ações administrativas. O comando `find-orphan-vms` permite que um administrador liste essas VMs para que elas possam ser removidas ou reimportadas para o vCloud Director. Seu comando tem provisão para especificar um armazenamento de confiança alternativo, que poderá ser necessário se você estiver trabalhando com instalações do vCloud Director ou do vCenter que usam certificados autoassinados.

Use um comando com o seguinte formato:

```
cell-management-tool find-orphan-vms options
```

**Tabela 10-20. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `find-orphan-vm`**

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--enableVerifyHostname</code>	Nenhuma	Ativa a parte de verificação do nome do host do handshake de SSL.
<code>--host</code>	Obrigatório	Endereço IP ou nome de domínio totalmente qualificado da instalação do vCloud Director para pesquisar VMs órfãs.
<code>--output-file</code>	nome do caminho ou -	Nome do caminho completo do arquivo no qual a lista de VMs órfãs deve ser gravada. Especifique um nome de caminho de - para gravar a lista na saída padrão.
<code>--password (-p)</code>	Obrigatório	Senha de administrador do sistema do vCloud Director.
<code>--port</code>	Porta HTTPS do vCloud Director.	Especifique isso somente se você não quiser que esse comando use a porta HTTPS padrão do vCloud Director.
<code>--trustStore</code>	Nome do caminho completo para um arquivo de armazenamento de confiança Java.	Especifique isso somente se você não quiser que esse comando use o arquivo de armazenamento de confiança padrão do vCloud Director.
<code>--trustStorePassword</code>	Senha para o <code>--trustStore</code> especificado	Obrigatório somente se você usar <code>--trustStore</code> para especificar um arquivo de armazenamento de confiança alternativo.
<code>--trustStoreType</code>	O tipo de <code>--trustStore</code> especificado (PKCS12, JCEKS, ...)	Obrigatório somente se você usar <code>--trustStore</code> para especificar um arquivo de armazenamento de confiança alternativo.
<code>--user (-u)</code>	Obrigatório	Nome de usuário do administrador do sistema do vCloud Director.
<code>--vc-name</code>	Obrigatório	Nome do vCenter para pesquisar VMs órfãs.
<code>--vc-password</code>	Obrigatório	Senha do administrador do vCenter.
<code>--vc-user</code>	Obrigatório	Nome de usuário do administrador do vCenter.



## Exemplo: Encontrar VMs órfãs

Este exemplo consulta um único vCenter Server. Como `--output-file` é especificado como `-`, os resultados são retornados na saída padrão.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vm \
--host 10.20.30.40 -u vcenter1 -vc-name vcenter1 -vc-password P055w0rd --vc-user admin --output-file -
Querying for VC by name 10.20.30.40
Querying all vdc's associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc->resource pool mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc->VM Moref mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Processing 956 VM's on 5 VDC's across 20 resource pools
Analysis complete.
VDC: "ExampleOrgVDC [urn:vcloud:vdc:1a97...]" (org: "ExampleOrg") ResPool: primary (1a97...) [moref:
"resgroup-30515"]
The following 22 orphan VMs were discovered:
Orphan VM: "indDisk100-0-95411 (cbc358a0-e199-4024-8fff-2e5cfce20953)" (parent name: "Test VMs",
parent moref : "group-v30533")
...
Orphan VM: "indDisk12-0-51259 (0bbb4115-673e-4c84-ba26-6875159655e0)" (parent name: "Test VMs",
parent moref : "group-v30533")
```

## Entrar ou sair do Programa de aperfeiçoamento da experiência do cliente da VMware

Para entrar ou sair do Programa de aperfeiçoamento da experiência do cliente (CEIP) da VMware, você pode usar o subcomando `configure-ceip` da ferramenta de gerenciamento de célula.

Este produto participa do Programa de aperfeiçoamento da experiência do cliente (“CEIP”) da VMware. Detalhes referentes à coleta de dados através do CEIP e os fins para os quais ela é utilizada pela VMware estão estabelecidos no Trust & Assurance Center em <http://www.vmware.com/trustvmware/ceip.html>. Você pode usar a ferramenta de gerenciamento de células para participar ou sair do CEIP da VMware para este produto a qualquer momento.

```
cell-management-tool
configure-ceip
options
```

Caso prefira não participar do CEIP da VMware para este produto, execute esse comando com a opção `--disable`.

**Tabela 10-21. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `configure-ceip`**

Opção	Argumento	Descrição
<code>--help</code> ( <code>-h</code> )	Nenhum	Fornece um resumo dos comandos disponíveis nessa categoria.
<code>--disable</code>	Nenhuma	Sai do Programa de aperfeiçoamento da experiência do cliente da VMware.
<code>--enable</code>	Nenhum	Entra no Programa de aperfeiçoamento da experiência do cliente da VMware.
<code>--status</code>	Nenhuma	Exibe o status de participação atual no Programa de aperfeiçoamento da experiência do cliente da VMware.

## Exemplo: Sair do Programa de aperfeiçoamento da experiência do cliente da VMware

Para sair do Programa de aperfeiçoamento da experiência do cliente da VMware, use um comando como este:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
disableParticipation disabled
```

Após executar esse comando, o sistema não enviará mais informações para o Programa de aperfeiçoamento da experiência do cliente da VMware.

Para confirmar o status atual da participação no Programa de aperfeiçoamento da experiência do cliente da VMware, use um comando como este:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
statusParticipation disabled
```

## Atualização das definições de configuração do aplicativo

Com o subcomando `manage-config` da ferramenta de gerenciamento de célula, você pode atualizar diferentes definições de configuração de aplicativo, como atividades de limitação de catálogo.

**Tabela 10-22. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `manage-config`**

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornece um resumo das opções disponíveis com esse subcomando.
<code>--delete (-d)</code>	Nenhum	Remove a definição de configuração de destino.
<code>--lookup (-l)</code>	Nenhum	Procure o valor da definição de configuração de destino.
<code>--name (-n)</code>	Nome da configuração	O nome da definição de configuração de destino. Necessário para as opções <code>-d</code> , <code>-l</code> e <code>-v</code> .
<code>--value (-v)</code>	Valor da definição de configuração	Adiciona ou atualiza o valor da definição de configuração de destino.

Por exemplo, você pode usar o subcomando `manage-config` para [Como configurar a limitação da sincronização de catálogo](#).

## Como configurar a limitação da sincronização de catálogo

Quando você tem muitos itens de catálogo publicados em ou inscritos de outras organizações, para evitar a sobrecarga do sistema durante as sincronizações de catálogo, pode configurar a limitação da sincronização de catálogo. Você pode usar o subcomando `manage-config` da ferramenta de gerenciamento de célula para configurar a limitação da sincronização de catálogo limitando o número de itens de biblioteca que podem ser sincronizados ao mesmo tempo.

Quando um catálogo inscrito inicia uma sincronização de catálogo, o catálogo publicado primeiro baixa os itens de biblioteca do repositório do vCenter Server para o armazenamento do serviço de transferência do vCloud Director e, em seguida, cria links de download para o catálogo inscrito. Você pode limitar o número de itens de biblioteca que todos os catálogos publicados podem baixar ao mesmo tempo. Você pode limitar o número de itens da biblioteca que todos os catálogos inscritos podem sincronizar ao mesmo tempo. Você pode limitar o número de itens de biblioteca que um único catálogo inscrito pode sincronizar ao mesmo tempo.

Você pode usar o subcomando `manage-config` da ferramenta de gerenciamento de célula para atualizar as definições de configuração de limitação de catálogo. Para obter informações sobre como usar o subcomando `manage-config`, consulte [Atualização das definições de configuração do aplicativo](#).

Tabela 10-23. Definições de configuração para otimização do catálogo

Definição de configuração	Valor padrão	Descrição
<code>vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit</code>	30	O limite de itens de biblioteca que todos os catálogos publicados na instância do vCloud Director podem baixar do vCenter Server para o vCloud Director ao mesmo tempo. Se o número total de itens de biblioteca publicados para download na instância do vCloud Director for maior do que o limite, os itens de biblioteca serão divididos em partes de acordo com o limite e baixados em uma sequência.
<code>vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit</code>	30	O limite dos itens de biblioteca que todos os catálogos inscritos em uma instância do vCloud Director podem sincronizar ao mesmo tempo. Se o número total de itens de biblioteca inscritos para sincronização na instância do vCloud Director for maior do que esse limite, os itens serão divididos em partes de acordo com esse limite e sincronizados em uma sequência.
<code>contentLibrary.item.sync.batch.size</code>	10	O limite dos itens de biblioteca que um único catálogo inscrito pode sincronizar ao mesmo tempo. Se um catálogo inscrito tentar sincronizar um número de itens de biblioteca maior do que o limite, os itens serão divididos em partes de acordo com o limite e sincronizados em uma sequência.

## Exemplo: Como configurar a limitação de sincronização para catálogos inscritos

O seguinte comando define o limite de cinco para itens de biblioteca que um único catálogo inscrito pode sincronizar ao mesmo tempo.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
contentLibrary.item.sync.batch.size -v 5
```

Se um catálogo inscrito contiver 13 itens de biblioteca, a sincronização do catálogo será realizada em três partes sequenciais. A primeira parte contém cinco itens, a segunda parte contém os próximos cinco itens, e a última parte contém os três itens restantes.

## Solucionar problemas de falha no acesso à interface do usuário do vCloud Director

Para visualizar e atualizar os endereços IP e as entradas DNS válidos para as células do vCloud Director em seu ambiente do vCloud Director, você pode usar o subcomando do `manage-config` da ferramenta de gerenciamento de célula.

### Problema

Não é possível acessar o vCloud Director Service Provider Admin Portal ou o vCloud Director Tenant Portal após um login bem-sucedido.

Depois de inserir suas credenciais na tela de login, a seguinte mensagem de erro é exibida: **Falha ao iniciar. Foi encontrado um erro durante a inicialização.** Isso pode ser causado por problemas como acessar o aplicativo por meio de uma URL pública não permitida ou baixa conectividade.

### Causa

O vCloud Director usa uma implementação de filtro de Compartilhamento de Recursos entre Origens (CORS) para manter uma lista de todos os endpoints válidos que você pode usar para acessar o Service Provider Admin Portal e o vCloud Director Tenant Portal.

A lista de filtragem CORS é preenchida e atualizada durante a configuração da célula. Ela contém entradas HTTP e HTTPS com endereços IP e nomes DNS para todas as células no grupo de servidores. Ela também contém um endereço IP público que é usado pelo balanceador de carga que faz parte do grupo de servidores do vCloud Director.

Durante a configuração da célula das implantações do dispositivo, a lista não é atualizada com os nomes DNS das células do vCloud Director e você não pode usar o nome DNS de uma célula para acessá-la.

### Solução

- 1 Faça login ou SSH como **raiz** para uma das células no grupo de servidores.
- 2 Para listar as URLs válidas que você pode usar para acessar as células do vCloud Director no seu ambiente, execute a seguinte linha de comando.

```
[root@cell /opt/vmware/vcloud-director/bin]# ./cell-management-tool manage-config -n  
webapp.allowed.origins -l
```

A saída do sistema é uma lista que contém entradas HTTP e HTTPS com endereços IP e nomes DNS para todas as células no grupo de servidores. Ela também contém um endereço IP público que é usado pelo balanceador de carga que faz parte do grupo de servidores do vCloud Director.

A lista é uma cadeia de caracteres separada por vírgula sem espaços entre as entradas.

- 3** (Opcional) Para atualizar a configuração de configuração do `webapp.allowed.origins`, execute a seguinte linha de comando. Na linha de comando, o parâmetro de valor da configuração é uma lista de endereços IP e nomes DNS em uma cadeia de caracteres separada por vírgula sem espaços entre as entradas.

```
[root@cell /opt/vmware/vcloud-director/bin]# ./cell-management-tool manage-config -n
webapp.allowed.origins -v "comma_separated_list_of_URLs_without_spaces"
```

## Depuração da detecção de VM do vCenter

Usando o subcomando `debug-auto-import` da ferramenta de gerenciamento de célula, você pode investigar o motivo pelo qual o mecanismo para descobrir vApps ignora uma ou mais VMs do vCenter.

Na configuração padrão, um VDC de organização detecta automaticamente as VMs do vCenter que são criadas nos pools de recursos que dão suporte ao VDC. Consulte a descoberta e a adoção de informações de vApps no *Guia do Portal de Administração do Provedor de Serviços do vCloud Director*. Se uma VM do vCenter não aparecer em um vApp descoberto, você poderá executar o subcomando `debug-auto-import` em relação a essa VM ou VDC.

```
cell-management-tool debug-auto-import options
```

O subcomando `debug-auto-import` retorna uma lista de VMs do vCenter e informações sobre as possíveis razões pelas quais as VMs são ignoradas pelo mecanismo de detecção. A lista também inclui VMs do vCenter que foram descobertas, mas não foram importadas no VCD de organização.

**Tabela 10-24. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `debug-auto-import`**

Opção	Argumento	Descrição
<code>--help</code> (-h)	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--org</code>	Nome da organização	Opcional. Lista as informações sobre as VMs ignoradas para a organização especificada.
<code>--vm</code>	Nome de VM ou parte de um nome de VM	Lista as informações sobre as VMs ignoradas que contêm o nome especificado da VM.  Opcional se a opção <code>--org</code> for usada.

## Exemplo: Depure a detecção de VM do vCenter pelo nome da VM test

O comando a seguir retorna informações sobre VMs ignoradas do vCenter em todas as organizações.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool debug-auto-import -vm test
```

```
VM with name:vm22-test (09ad258c-0cb0-4f69-a0a6-201cf3fe7d6b), moref vm-50 in VC testbed-vc can be skipped for the following reasons:
```

- 1) Virtual machine is already imported in vCD or is managed by vCD
- 2) Virtual machine is created by vCD

```
VM with name:test-vm1 (32210d0d-ef64-4637-b1d6-6400743a6bd9), moref vm-44 in VC testbed-vc can be skipped for the following reasons:
```

- 1) Virtual machine is not present in a vCD managed resource pool

```
VM with name:import-test3, moref vm-52inVC testbed-vc can be skippedforthe following reasons:
```

- 1) Virtual machine autoimport is either pending,in-progress or has failed and pendingforretry

Nesse exemplo, a saída do sistema retorna informações sobre três VMs do vCenter que são ignoradas pelo mecanismo de detecção e cujos nomes contêm a cadeia de caracteres test. A VM import-test3 é um exemplo de uma VM que foi descoberta, mas não foi importada no VDC.

## Como regenerar endereços MAC para redes estendidas multissite

Se você associar dois sites do vCloud Director configurados com o mesmo ID de instalação, poderá encontrar conflitos de endereço MAC em redes estendidas nesses sites. Para evitar tais conflitos, você deve regenerar os endereços MAC em um dos sites com base em uma propagação personalizada que seja diferente do ID de instalação.

Durante a configuração inicial do vCloud Director, você define um ID de instalação. O vCloud Director usa o ID de instalação para regenerar os endereços MAC para as interfaces de rede da máquina virtual. Duas instalações do vCloud Director configuradas com o mesmo ID de instalação podem gerar endereços MAC idênticos. Endereços MAC duplicados podem causar conflitos em redes estendidas entre dois sites associados.

Antes de criar redes estendidas entre sites associados configurados com o mesmo ID de instalação, você deve regenerar os endereços MAC em um dos sites usando o subcomando `mac-address-management` da ferramenta de gerenciamento de célula.

```
cell-management-tool mac-address-management options
```

Para gerar novos endereços MAC, você define uma propagação personalizada que seja diferente do ID de instalação. A propagação não substitui o ID de instalação, mas o banco de dados armazena a propagação mais recente como um segundo parâmetro de configuração, que substitui o ID de instalação.

Você executa o subcomando `mac-address-management` desde um membro arbitrário do vCloud Director do grupo de servidores. O comando é executado no banco de dados do vCloud Director, para que você execute o comando uma vez para um grupo de servidores.

**Importante** A regeneração de endereços MAC requer algum tempo de inatividade do vCloud Director. Antes de iniciar a regeneração, você deve desativar as atividades em todas as células no grupo de servidores.

**Tabela 10-25. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `mac-address-management`**

Opção	Argumento	Descrição
<code>--help</code> (-h)	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--regenerate</code>	Nenhum	Exclui todos os endereços MAC que não estão em uso e gera novos endereços MAC com base na propagação atual. Se não houver nenhuma propagação definida anteriormente, os endereços MAC serão regenerados com base no ID de instalação. Os endereços MAC que estiverem em uso serão mantidos.
<b>Observação</b> Todas as células no grupo de servidores devem ser inativas. Para obter informações sobre a desativação das atividades em uma célula, consulte <a href="#">Como gerenciar uma célula</a> .		



**Tabela 10-25. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `mac-address-management` (continuação)**

Opção	Argumento	Descrição
<code>--regenerate-with-seed</code>	Um número de propagação de 0 a 63	Define uma nova propagação personalizada no banco de dados, exclui todos os endereços MAC que não estão em uso e gera novos endereços MAC com base na propagação recentemente definida. Os endereços MAC que estiverem em uso serão mantidos.  <b>Observação</b> Todas as células no grupo de servidores devem ser inativas. Para obter informações sobre a desativação das atividades em uma célula, consulte <a href="#">Como gerenciar uma célula</a> .
<code>--show-seed</code>	Nenhum	Retorna a propagação atual e o número de endereços MAC que estão em uso para cada propagação.

**Importante** Os endereços MAC que estiverem em uso serão mantidos. Para alterar um endereço MAC que está em uso para um endereço MAC regenerado, você deve redefinir o endereço MAC da interface de rede. Para obter informações sobre a edição de propriedades da máquina virtual, consulte o *Guia do Portal de Tenants do vCloud Director*.

## Exemplo: Como regenerar os endereços MAC com base em uma nova propagação personalizada

O comando a seguir define a propagação atual como 9 e regenera todos os endereços MAC que não são usados com base na propagação recentemente definida:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --regenerate-with-seed 9
Successfully removed 65,535 unused MAC addresses.
Successfully generated new MAC addresses.
```

## Exemplo: Como visualizar a propagação atual e o número de endereços MAC em uso para cada propagação

O comando a seguir retorna informações sobre a propagação atual e o número de endereços MAC por propagação:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --show-seed
Current MAC address seed is '9' and based on MacAddressSeed config.
MAC address seed    9 is in use by    12 MAC addresses
MAC address seed    1 is in use by     1 MAC addresses
```

Nesse exemplo, a saída do sistema mostra que a propagação atual é 9 e, com base nela, há 12 endereços MAC. Além disso, há um endereço MAC que se baseia em uma propagação anterior ou no ID de instalação de 1.

## Atualizar os endereços IP do banco de dados em células do vCloud Director

Você pode usar a ferramenta de gerenciamento de células para atualizar os endereços IP das células do vCloud Director em um cluster de alta disponibilidade de banco de dados.

### Pré-requisitos

Para atualizar os endereços IP das células em um cluster de alta disponibilidade de banco de dados, você deve fornecer o endereço IP da célula primária atual. Para encontrar o endereço IP, verifique o status do cluster para localizar qual nó tem a função primária. O nó deve estar em execução. Nessa linha, use o valor de host da coluna *Cadeia de conexão* para identificar o endereço IP. Consulte [Verificar o status de um cluster de alta disponibilidade do banco de dados](#).

### Procedimentos

- 1 Faça login ou conecte-se via SSH como **root** no sistema operacional de qualquer um das células no cluster.
- 2 Verifique se a célula está em execução nesse nó.

```
service vmware-vcd pid cell
```

Se o ID de processo da célula não for nulo, a célula do vCloud Director estará em execução, e você poderá alterar o endereço IP do banco de dados sem reiniciar a célula do vCloud Director.

- 3 Para atualizar os endereços IP em todas as células no grupo de servidores, execute o seguinte comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address --pid cell process ID --remote-sudo-user postgres --private-key-path /opt/vmware/vcloud-director/id_rsa
```

A saída do sistema indica a reconfiguração bem-sucedida.

- 4 (Opcional) Verifique se cada célula do vCloud Director está apontando para o endereço IP correto do banco de dados.

```
grep "database.jdbcUrl" /opt/vmware/vcloud-director/etc/global.properties
```

A saída do sistema indica que a célula foi atualizada.

- 5 Se qualquer uma das células não for atualizada, execute o comando para reconfigurá-la.

- Se a célula não estiver em execução, execute o seguinte comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host  
primary node IP address
```

- Se a célula estiver em execução, execute o seguinte comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host  
primary node IP address -i cell process ID
```

- 6 Se você tiver reconfigurado uma célula que não está em execução, execute o comando para reiniciar o serviço `vmware-vcd`.

- a Execute o comando para interromper o serviço.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid cell) -s
```

- b Execute o comando para iniciar o serviço.

```
systemctl start vmware-vcd
```

# Após você instalar o vCloud Director ou implantar o dispositivo do vCloud Director

## 11

Depois de criar o grupo de servidores do vCloud Director, você poderá instalar os arquivos de Sysprep da Microsoft e o banco de dados Cassandra. Se você estiver usando um banco de dados do PostgreSQL, poderá configurar o SSL e ajustar alguns parâmetros no banco de dados.

Após a criação do dispositivo do vCloud Director, você pode usar os recursos de rede do vSphere para adicionar uma nova placa de interface de rede (NIC). Consulte as informações em [Adicionar um adaptador de rede a uma máquina virtual](#) no guia *Administração de máquinas virtuais do vSphere*.

Este capítulo inclui os seguintes tópicos:

- [Instalar arquivos do Microsoft Sysprep nos servidores](#)
- [Alterar o fuso horário do dispositivo do vCloud Director](#)
- [Personalizar endereços públicos](#)
- [Instalar e configurar um banco de dados Cassandra para armazenar dados de métricas de históricos](#)
- [Realizar configurações adicionais no banco de dados PostgreSQL externo](#)

## Instalar arquivos do Microsoft Sysprep nos servidores

Se a sua nuvem exigir suporte à personalização de convidados para determinados sistemas operacionais da Microsoft mais antigos, você deverá instalar os arquivos apropriados do Microsoft Sysprep em cada membro do grupo de servidores.

Os arquivos Sysprep são necessários apenas para alguns sistemas operacionais da Microsoft mais antigos. Se a sua nuvem não precisar suportar a personalização de convidado para esses sistemas operacionais, não será necessário instalar os arquivos do Sysprep.

Para instalar os arquivos binários do Sysprep, copie-os para um local específico no servidor. Você deve copiar os arquivos para cada membro do grupo de servidores.

### Pré-requisitos

Verifique se você tem acesso aos arquivos binários Sysprep de 32 e 64 bits para Windows 2003 e Windows XP.

## Procedimentos

- 1 Faça login no servidor de destino como **raiz**.
- 2 Altere o diretório para `$VCLLOUD_HOME/guestcustomization/default/windows`.

```
[root@cell1 /]# cd /opt/vmware/vcloud-director/guestcustomization/default/windows
```

- 3 Crie um diretório chamado `sysprep`.

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep
```

- 4 Para cada sistema operacional convidado que requer arquivos binários do Sysprep, crie um subdiretório de `$VCLLOUD_HOME/guestcustomization/default/windows/sysprep`.

Os nomes de subdiretório são específicos de um sistema operacional convidado.

**Tabela 11-1. Atribuições de subdiretório para arquivos Sysprep**

SO Convidado	Subdiretório a ser criado em <code>\$VCLLOUD_HOME/guestcustomization/default/windows/sysprep</code>
Windows 2003 (32 bits)	svr2003
Windows 2003 (64 bits)	svr2003-64
Windows XP (32 bits)	xp
Windows XP (64 bits)	xp-64

Por exemplo, para criar um subdiretório para conter arquivos binários do Sysprep para o Windows XP, use o seguinte comando do Linux.

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep/xp
```

- 5 Copie os arquivos binários do Sysprep para o local apropriado em cada servidor do vCloud Director no grupo de servidores.
- 6 Certifique-se de que os arquivos do Sysprep sejam legíveis pelo usuário do `vcloud.vcloud`.

Use o comando `chown` do Linux para fazer isso.

```
[root@cell1 /]# chown -R vcloud:vcloud $VCLLOUD_HOME/guestcustomization
```

## Resultados

Quando os arquivos do Sysprep são copiados para todos os membros do grupo de servidores, você pode executar a personalização de convidados em máquinas virtuais em sua nuvem. Você não precisa reiniciar o vCloud Director depois que os arquivos do Sysprep são copiados.

## Alterar o fuso horário do dispositivo do vCloud Director

Depois de implantar com êxito o dispositivo do vCloud Director, você pode alterar o fuso horário do sistema do dispositivo. Todas as instâncias do dispositivo do vCloud Director no

grupo de servidores e o armazenamento do servidor de transferência devem usar as mesmas configurações.

#### Pré-requisitos

- Implante o dispositivo do vCloud Director. Consulte [Capítulo 6 Implantação do vCloud DirectorAppliance](#).
- Altere o fuso horário de armazenamento do servidor de transferência para o novo fuso horário do dispositivo primário do vCloud Director.

#### Procedimentos

- 1 Usando um console da Web ou um Console Remoto para o nó principal, na parte inferior esquerda da janela do console, selecione **Definir Fuso Horário**.
- 2 Selecione um local, um país e uma região de fuso horário.  
O fuso horário selecionado recentemente aparece na parte inferior esquerda da janela do console.
- 3 Faça login no console do dispositivo do vCloud Director como **raiz**.
- 4 Para garantir que o dispositivo do vCloud Director use o novo fuso horário, reinicie o serviço do `vmware-vcd`.
- 5 Repita as [Etapas 1 a Etapa 4](#) para qualquer célula de aplicativo e em espera na sua implantação do vCloud Director.

## Personalizar endereços públicos


Para atender aos requisitos de balanceador de carga ou de proxy, você pode alterar os endereços da Web do endpoint padrão para o Portal da Web do vCloud Director, a API do vCloud e o proxy do console.

Se você tiver implantado o vCloud DirectorAppliance, deverá configurar o endereço de proxy do console público do vCloud Director, pois o dispositivo usa um único endereço IP com a porta personalizada 8443 para o serviço de proxy do console. Consulte [Etapa 6](#).

#### Pré-requisitos

Somente o **administrador do sistema** pode personalizar os endpoints públicos.

#### Procedimentos

- 1 No menu principal () , selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, clique em **Endereços Públicos**.
- 3 Clique em **Editar** para personalizar os endpoints públicos.

**4** Para personalizar as URLs do vCloud Director, edite os endpoints do **Portal da Web**.

- a Insira uma URL pública personalizada do vCloud Director para conexões HTTP (não seguras).
- b Insira a URL pública personalizada do vCloud Director para conexões HTTPS (seguras) e clique em **Carregar** para carregar os certificados que estabelecem a cadeia de confiança para esse endpoint.

A cadeia de certificados deve corresponder ao certificado usado pelo endpoint de serviço, que é o certificado carregado para cada armazenamento de chaves de célula do vCloud Director com o alias `consoleproxy`. Não há suporte para a terminação SSL das conexões de proxy do console em um balanceador de carga. A cadeia de certificados deve incluir um certificado de endpoint, certificados intermediários e um certificado raiz no formato PEM sem uma chave privada.

**5** (Opcional) Para personalizar as URLs da REST API do vCloud e do OpenAPI, desative a opção **Usar as Configurações do Portal da Web**.

- a Insira uma URL base HTTP personalizada.

Por exemplo, se você definir a URL base HTTP como **`http://vcloud.exemplo.com`**, poderá acessar a API do vCloud em `http://vcloud.exemplo.com/API` e poderá acessar o vCloud OpenAPI em `http://vcloud.exemplo.com/cloudapi`.

- b Insira uma URL de base da REST API de HTTPS e clique em **Carregar** para carregar os certificados que estabelecem a cadeia de confiança para esse endpoint.

Por exemplo, se você definir a URL base da API REST HTTPS como **`https://vcloud.exemplo.com`**, poderá acessar a API do vCloud em `https://vcloud.exemplo.com/API` e o vCloud OpenAPI em `https://vcloud.exemplo.com/cloudapi`.

A cadeia de certificados deverá corresponder ao certificado usado pelo endpoint de serviço, que é o certificado carregado para cada armazenamento de chaves de célula do vCloud Director com o alias `http`, ou ao certificado VIP do balanceador de carga se for usada uma terminação SSL. A cadeia de certificados deve incluir um certificado de endpoint, certificados intermediários e um certificado raiz no formato PEM sem uma chave privada.

**6** Insira um endereço de proxy personalizado do console público do vCloud Director.

Esse endereço é o nome de domínio totalmente qualificado (FQDN) do servidor do vCloud Director ou do balanceador de carga com o número da porta. A porta padrão é 443.

---

**Importante** O vCloud DirectorAppliance usa o NIC do seu `eth0` com a porta personalizada 8443 para o serviço de proxy do console.

---

Por exemplo, para uma instância do vCloud Director Appliance com FQDN `vcloud.example.com`, insira **`vcloud.exemplo.com:8443`**.

O vCloud Director usa o endereço de proxy do console ao abrir uma janela de console remoto em uma VM.

- 7 Para salvar as alterações, clique em **Salvar**.

## Instalar e configurar um banco de dados Cassandra para armazenar dados de métricas de históricos

O vCloud Director pode coletar métricas que fornecem informações atuais e de históricos sobre o desempenho da máquina virtual e o consumo de recursos para as máquinas virtuais que estão em sua nuvem. Dados para métricas de históricos são armazenados em um cluster do Cassandra.

O Cassandra é um banco de dados de código-fonte aberto que você pode usar para fornecer o repositório de backup para uma solução dimensionável e de alto desempenho para coletar dados de séries de tempo como métricas de máquinas virtuais. Se você quiser que o vCloud Director tenha suporte para a recuperação de métricas de históricos de máquinas virtuais, será necessário instalar e configurar um cluster do Cassandra e usar o `cell-management-tool` para conectar o cluster ao vCloud Director. A recuperação das métricas atuais não exige o software de banco de dados opcional.

### Pré-requisitos

- Verifique se o vCloud Director está instalado e em execução antes de configurar o software do banco de dados opcional.
- Se você ainda não estiver familiarizado com o Cassandra, reveja o material em <http://cassandra.apache.org/>.
- Consulte o *Notas da Versão do vCloud Director* para obter uma lista das versões do Cassandra compatíveis para uso como banco de dados de métricas. Você pode baixar o Cassandra de <http://cassandra.apache.org/download/>.
- Instale e configure o cluster do Cassandra:
  - O cluster do Cassandra deve incluir pelo menos, quatro máquinas virtuais implantadas em dois ou mais hosts.
  - Dois nós de propagação do Cassandra são necessários.
  - Ative a criptografia de cliente para nó do Cassandra. Consulte <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html>.
  - Ative a autenticação do usuário do Cassandra. Consulte <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html>.
  - Ative o Java Native Access (JNA) versão 3.2.7 ou posterior em cada cluster do Cassandra.
  - A criptografia de nó para nó do Cassandra é opcional.



- O uso de SSL com o Cassandra é opcional. Se você decidir não ativar o SSL para Cassandra, será necessário definir o parâmetro de configuração `cassandra.use.ssl` para 0 no arquivo `global.properties` em cada célula (`$VCLLOUD_HOME/etc/global.properties`)

## Procedimentos

- 1 Use o utilitário `cell-management-tool` para configurar uma conexão entre o vCloud Director e os nós no cluster do Cassandra.

O comando do exemplo a seguir, `node1-ip`, `node2-ip`, `node3-ip` e `node4-ip` são o endereço IP dos membros do cluster do Cassandra. A porta padrão (9042) é usada. Os dados de métricas são mantidos por 15 dias.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --configure --
create-schema \ --cluster-nodes node1-ip,node2-ip,node3-ip, node4-ip \ --username admin --
password 'P@55w0rd' --ttl 15
```

Para obter informações sobre como usar a ferramenta de gerenciamento de célula, consulte [Capítulo 10 Referência da ferramenta de gerenciamento de células](#).

- 2 (Opcional) Se você está atualizando o vCloud Director da versão 9.1, use a `cell-management-tool` para configurar o banco de dados de métricas para armazenar métricas acumuladas.

Execute um comando semelhante ao exemplo a seguir:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --add-rollup \ --
username admin --password 'P@55w0rd'
```

- 3 Reinicie cada célula do vCloud Director.

## Realizar configurações adicionais no banco de dados PostgreSQL externo

Depois de criar o seu grupo de servidores do vCloud Director, você pode configurar o banco de dados PostgreSQL externo para exigir conexões SSL das células do vCloud Director e ajustar alguns parâmetros de banco de dados para obter um desempenho ideal.

Conexões mais seguras exigem um certificado SSL bem-assinado, o que inclui uma cadeia confiável completa cuja raiz seja uma autoridade de certificação pública conhecida. Como alternativa, você pode usar um certificado SSL autoassinado ou um certificado SSL assinado por uma autoridade de certificação particular, mas deve importar o certificado para o truststore do vCloud Director.

Para obter um desempenho ideal para os requisitos e a especificação do seu sistema, você pode ajustar as configurações do banco de dados e os parâmetros de vácuo automático no arquivo de configuração de banco de dados.

## Procedimentos

### 1 Configurar conexões SSL entre o vCloud Director e o banco de dados PostgreSQL.

- a Se você usou um certificado autoassinado ou particular para o banco de dados PostgreSQL externo, de cada célula do vCloud Director, execute o comando para importar o certificado do banco de dados para o truststore do vCloud Director.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool import-trusted-  
certificates --source path_to_self-signed_or_private_cert
```

- b Execute o comando para habilitar conexões SSL entre o vCloud Director e o PostgreSQL.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool reconfigure-database --  
database-ssl true
```

Você pode executar o comando em relação a todas as células do grupo de servidores usando a opção `--private-key-path`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool reconfigure-database --  
database-ssl true --private-key-path path_to_private_key
```

Para obter mais informações sobre como usar a ferramenta de gerenciamento de célula, consulte [Capítulo 10 Referência da ferramenta de gerenciamento de células](#).

### 2 Edite as configurações do banco de dados no arquivo `postgresql.conf` para a especificação do seu sistema.

Por exemplo, para um sistema com 16 GB de memória, você pode usar o fragmento a seguir.

```
max_connections = 500  
# Set effective cache size to 50% of total memory.  
effective_cache_size = 8GB  
# Set shared buffers to 25% of total memory  
shared_buffers = 4GB
```

### 3 Edite os parâmetros de vácuo automático no arquivo `postgresql.conf` para seus requisitos.

Para cargas de trabalho típicas do vCloud Director, você pode usar o fragmento a seguir.

```
autovacuum = on  
track_counts = on  
autovacuum_max_workers = 3  
autovacuum_naptime = 1min  
autovacuum_vacuum_cost_limit = 2400
```

O sistema define um valor de `autovacuum_vacuum_scale_factor` personalizado para a atividade e as tabelas de `activity_parameters`.

## Próximo passo

Se você editou o arquivo `postgresql.conf`, deve reiniciar o banco de dados.

# Atualizando o vCloud Director

# 12

Para fazer upgrade do vCloud Director para uma nova versão, encerre os serviços do vCloud Director em todas as células no grupo de servidores, instale a nova versão em cada servidor, faça upgrade do banco de dados do vCloud Director e reinicie as células do vCloud Director.

Se o seu grupo de servidores vCloud Director existente consistir em instalações do do vCloud Director no Linux, você poderá usar o instalador vCloud Director para Linux para atualizar seu ambiente. Como alternativa, você pode migrar seu ambiente para um dispositivo do vCloud Director 10.0. Consulte [Capítulo 13 Migrando para o dispositivo do vCloud Director](#).

Se o seu grupo de servidores vCloud Director existente consistir em uma implantação de dispositivo do vCloud Director 9.5, você só poderá migrar seu ambiente para uma versão mais recente do dispositivo do vCloud Director. Use o instalador do vCloud Director para Linux para fazer upgrade do ambiente existente somente como parte do fluxo de trabalho de migração. Consulte [Migrando para o dispositivo do vCloud Director](#).

Para instalações do vCloud Director no Linux, você pode executar um upgrade orquestrado ou fazer o upgrade manualmente do vCloud Director. Consulte [Realizar uma atualização orquestrada de uma instalação do vCloud Director](#) ou [Atualizar manualmente uma instalação do vCloud Director](#). Com o upgrade orquestrado, você executa um único comando que atualiza todas as células no grupo de servidores e no banco de dados. Com o upgrade manual, você atualiza cada célula e o banco de dados em uma sequência.

Para o upgrade da versão 9.7 para a versão 10.0 do dispositivo do vCloud Director, consulte [Fazer upgrade do dispositivo do vCloud Director](#).

Iniciando com o vCloud Director 9.5:

- Os bancos de dados Oracle não têm suporte. Se a sua instalação existente do vCloud Director usar um banco de dados Oracle, consulte a tabela [Caminhos de upgrade e migração](#).
- Não há suporte para a ativação e a desativação de hosts ESXi. Antes de iniciar o upgrade, você deve habilitar todos os hosts do ESXi. Você pode colocar os hosts do ESXi no modo de manutenção usando o vSphere Client.

- O vCloud Director usa Java com suporte LDAP aprimorado. Se você estiver usando um servidor LDAPS, para evitar falhas de logon LDAP, deverá verificar se tem um certificado construído corretamente. Para obter informações, consulte as *Alterações da versão do Java 8* em <https://www.java.com>.

A partir do vCloud Director 10.0, os bancos de dados Microsoft SQL Server não têm suporte.

Quando você atualiza o vCloud Director, a nova versão deve ser compatível com os seguintes componentes de sua instalação existente:

- O software de banco de dados que você está usando atualmente para o banco de dados do vCloud Director. Para obter mais informações, consulte a tabela Caminhos de upgrade e migração.
- A versão do VMware vSphere® que você está usando atualmente.
- A versão do VMware NSX® que você está usando no momento.
- Qualquer componente de terceiros que interaja diretamente com o vCloud Director.

Para obter informações sobre a compatibilidade do vCloud Director com outros produtos VMware e com bancos de dados de terceiros, consulte as *Matrizes de interoperabilidade de produtos VMware* em [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php). Se você planeja fazer upgrade dos componentes do vSphere ou do NSX como parte do upgrade do vCloud Director, deverá fazer o upgrade deles após o upgrade do vCloud Director. Consulte [Capítulo 14 Depois de atualizar ou migrar o vCloud Director](#).

Depois de atualizar pelo menos um servidor vCloud Director, você pode atualizar o banco de dados vCloud Director. O banco de dados armazena informações sobre o estado de tempo de execução do servidor, incluindo o estado de todas as tarefas vCloud Director que estão sendo executadas. Para garantir que nenhuma informação de tarefa inválida permaneça no banco de dados após um upgrade, você deve verificar se não há tarefas ativas em qualquer servidor antes de começar o upgrade.

O upgrade também preserva os seguintes artefatos, que não são armazenados no banco de dados vCloud Director:

- Arquivos de propriedades locais e globais são copiados para a nova instalação.
- Arquivos do Microsoft Sysprep usados para suporte de personalização de guest são copiados para a nova instalação.

O upgrade requer tempo de inatividade suficiente do vCloud Director para atualizar todos os servidores no grupo de servidor e no banco de dados. Se você estiver usando um balanceador de carga, poderá configurá-lo para retornar uma mensagem, por exemplo, `O sistema está offline para upgrade`.

## Fluxos de trabalho e caminhos de upgrade e migração

Ambiente de origem	Ambiente de destino	
	vCloud Director 10.0 no Linux com um banco de dados PostgreSQL externo	Dispositivo do vCloud Director 10.0 com um banco de dados PostgreSQL incorporado
vCloud Director 9.0 e 9.1 com um banco de dados Oracle externo	<ol style="list-style-type: none"> <li>1 Para o vCloud Director 9.0 no Linux, faça upgrade do vCloud Director para a versão 9.1. Consulte <a href="#">Fazendo upgrade do vCloud Director</a>.</li> <li>2 Migre o banco de dados Oracle para um banco de dados PostgreSQL. Consulte <a href="#">Migrar para um banco de dados PostgreSQL</a>.</li> <li>3 Faça upgrade do seu ambiente para o vCloud Director 10.0 no Linux. Consulte <a href="#">Realizar uma atualização orquestrada de uma instalação do vCloud Director</a> ou <a href="#">Atualizar manualmente uma instalação do vCloud Director</a>.</li> </ol>	<ol style="list-style-type: none"> <li>1 Para o vCloud Director 9.0 no Linux, faça upgrade do vCloud Director para a versão 9.1. Consulte <a href="#">Fazendo upgrade do vCloud Director</a>.</li> <li>2 Migre o banco de dados Oracle para um banco de dados PostgreSQL. Consulte <a href="#">Migrar para um banco de dados PostgreSQL</a>.</li> <li>3 Faça upgrade do seu ambiente para o vCloud Director 10.0 no Linux. Consulte <a href="#">Realizar uma atualização orquestrada de uma instalação do vCloud Director</a> ou <a href="#">Atualizar manualmente uma instalação do vCloud Director</a>.</li> <li>4 Migre para o dispositivo do vCloud Director 10.0. Consulte <a href="#">Migrando o vCloud Director com um banco de dados externo PostgreSQL para um dispositivo do vCloud Director</a>.</li> </ol>
Dispositivo do vCloud Director 9.5 com um banco de dados PostgreSQL externo	Sem suporte	<ol style="list-style-type: none"> <li>1 Faça upgrade do seu ambiente para o vCloud Director 10.0 no Linux. Consulte <a href="#">Realizar uma atualização orquestrada de uma instalação do vCloud Director</a> ou <a href="#">Atualizar manualmente uma instalação do vCloud Director</a>.</li> <li>2 Migre para o dispositivo do vCloud Director 10.0. Consulte <a href="#">Migrando o vCloud Director com um banco de dados externo PostgreSQL para um dispositivo do vCloud Director</a>.</li> </ol>

Ambiente de origem	Ambiente de destino	
	vCloud Director 10.0 no Linux com um banco de dados PostgreSQL externo	Dispositivo do vCloud Director 10.0 com um banco de dados PostgreSQL incorporado
vCloud Director 9.0, 9.1 e 9.5 no Linux com um banco de dados PostgreSQL externo	Faça upgrade do seu ambiente para o vCloud Director 10.0 no Linux. Consulte <a href="#">Realizar uma atualização orquestrada de uma instalação do vCloud Director</a> ou <a href="#">Atualizar manualmente uma instalação do vCloud Director</a> .	<ol style="list-style-type: none"> <li>1 Faça upgrade do seu ambiente para o vCloud Director 10.0 no Linux. Consulte <a href="#">Realizar uma atualização orquestrada de uma instalação do vCloud Director</a> ou <a href="#">Atualizar manualmente uma instalação do vCloud Director</a>.</li> <li>2 Migre para o dispositivo do vCloud Director 10.0. Consulte <a href="#">Migrando o vCloud Director com um banco de dados externo PostgreSQL para um dispositivo do vCloud Director</a>.</li> </ol>
vCloud Director 9.0, 9.1 e 9.5 no Linux com um banco de dados Microsoft SQL Server externo	<ol style="list-style-type: none"> <li>1 Faça upgrade do seu ambiente para o vCloud Director 9.7 no Linux. Consulte <a href="#">Fazendo upgrade do vCloud Director</a>.</li> <li>2 Migre o banco de dados Microsoft SQL Server para um banco de dados PostgreSQL. Consulte <a href="#">Migrar para um banco de dados PostgreSQL</a>.</li> <li>3 Faça upgrade do seu ambiente para o vCloud Director 10.0 no Linux. Consulte <a href="#">Realizar uma atualização orquestrada de uma instalação do vCloud Director</a> ou <a href="#">Atualizar manualmente uma instalação do vCloud Director</a>.</li> </ol>	<ol style="list-style-type: none"> <li>1 Faça upgrade do seu ambiente para o vCloud Director 9.7 no Linux. Consulte <a href="#">Fazendo upgrade do vCloud Director</a>.</li> <li>2 Migre para o dispositivo do vCloud Director 9.7. Consulte <a href="#">Migrando o vCloud Director com um banco de dados Microsoft SQL externo para um dispositivo do vCloud Director</a>.</li> <li>3 Faça upgrade do seu ambiente para o dispositivo do vCloud Director 10.0. Consulte <a href="#">Fazer upgrade do dispositivo do vCloud Director</a>.</li> </ol>
vCloud Director 9.7 no Linux com um banco de dados Microsoft SQL Server externo	<ol style="list-style-type: none"> <li>1 Migre o banco de dados Microsoft SQL Server para um banco de dados PostgreSQL. Consulte <a href="#">Migrar para um banco de dados PostgreSQL</a>.</li> <li>2 Faça upgrade do seu ambiente para o vCloud Director 10.0 no Linux. Consulte <a href="#">Realizar uma atualização orquestrada de uma instalação do vCloud Director</a> ou <a href="#">Atualizar manualmente uma instalação do vCloud Director</a>.</li> </ol>	<ol style="list-style-type: none"> <li>1 Migre para o dispositivo do vCloud Director 9.7. Consulte <a href="#">Migrando o vCloud Director com um banco de dados Microsoft SQL externo para um dispositivo do vCloud Director</a>.</li> <li>2 Faça upgrade do seu ambiente para o dispositivo do vCloud Director 10.0. Consulte <a href="#">Fazer upgrade do dispositivo do vCloud Director</a>.</li> </ol>

Ambiente de origem	Ambiente de destino	
	vCloud Director 10.0 no Linux com um banco de dados PostgreSQL externo	Dispositivo do vCloud Director 10.0 com um banco de dados PostgreSQL incorporado
vCloud Director 9.7 no Linux com um banco de dados PostgreSQL externo	Faça upgrade do seu ambiente para o vCloud Director 10.0 no Linux. Consulte <a href="#">Realizar uma atualização orquestrada de uma instalação do vCloud Director</a> ou <a href="#">Atualizar manualmente uma instalação do vCloud Director</a> .	<ol style="list-style-type: none"> <li>1 Migre para o dispositivo do vCloud Director 9.7. Consulte <a href="#">Migrando o vCloud Director com um banco de dados PostgreSQL externo para um dispositivo do vCloud Director</a>.</li> <li>2 Faça upgrade do seu ambiente para o dispositivo do vCloud Director 10.0. Consulte <a href="#">Fazer upgrade do dispositivo do vCloud Director</a>.</li> </ol>
Dispositivo do vCloud Director 9.7 com um banco de dados PostgreSQL incorporado	Sem suporte	Faça upgrade do seu ambiente para o dispositivo do vCloud Director 10.0. Consulte <a href="#">Fazer upgrade do dispositivo do vCloud Director</a> .
vCloud Director 10.0 no Linux com um banco de dados PostgreSQL externo	N/A	Migre para o dispositivo do vCloud Director 10.0. Consulte <a href="#">Migrando o vCloud Director com um banco de dados externo PostgreSQL para um dispositivo do vCloud Director</a> .

Este capítulo inclui os seguintes tópicos:

- [Fazer upgrade do dispositivo do vCloud Director](#)
- [Reverter um dispositivo do vCloud Director quando um upgrade falhar](#)
- [Fazer upgrade do dispositivo do vCloud Director usando o Repositório de Atualização da VMware](#)
- [Realizar uma atualização orquestrada de uma instalação do vCloud Director](#)
- [Atualizar manualmente uma instalação do vCloud Director](#)
- [Referência do utilitário de atualização de banco de dados](#)

## Fazer upgrade do dispositivo do vCloud Director

Você pode fazer upgrade do dispositivo do vCloud Director da versão 9.7 para a 10.0 ou fazer upgrade do vCloud Director 10.0 para uma versão de patch.

Durante o upgrade da implantação do dispositivo do vCloud Director, o serviço vCloud Director para de funcionar, e um certo tempo de inatividade pode ser esperado. O tempo de inatividade depende do tempo necessário para fazer upgrade de cada dispositivo do vCloud Director e executar o script de atualização do banco de dados vCloud Director. O número de células de

trabalho no grupo de servidores vCloud Director será reduzido até que você pare o serviço vCloud Director no último dispositivo vCloud Director. Um balanceador de carga configurado adequadamente na frente dos endpoints HTTP do vCloud Director deve parar o roteamento do tráfego para as células que estão paradas.

Depois de aplicar o upgrade a cada dispositivo do vCloud Director e o upgrade do banco de dados estiver concluído, você deverá reinicializar cada dispositivo do vCloud Director.

### Pré-requisitos

Tire um instantâneo do dispositivo primário do vCloud Director.

- 1 Faça login na instância do vCenter Server na qual reside o dispositivo primário do vCloud Director do seu cluster de alta disponibilidade do banco de dados.
- 2 Navegue até o dispositivo primário do vCloud Director, clique com o botão direito do mouse nele e clique em **Ligar/Desligar > Encerrar SO Convidado**.
- 3 Clique com o botão direito do mouse no dispositivo e clique em **Instantâneo > Tirar Instantâneo**. Insira um nome e, opcionalmente, uma descrição para o instantâneo e clique em **OK**.
- 4 Clique com o botão direito do mouse no dispositivo do vCloud Director e clique em **Ligar/Desligar > Ligar**.
- 5 Verifique se todos os nós na configuração de alta disponibilidade do banco de dados estão em bom estado. Consulte [Verificar o status de um cluster de alta disponibilidade do banco de dados](#).

### Procedimentos

- 1 Em um navegador da Web, faça login na interface do usuário de gerenciamento do dispositivo de uma instância de dispositivo vCloud Director para identificar o dispositivo primário, `https://appliance_ip_address:5480`.  
  
Anote o nome do dispositivo primário. Você deve fazer o upgrade do dispositivo primário antes das células em modo de espera e de aplicativos. Você deverá usar o nome do dispositivo primário ao fazer backup do banco de dados.
- 2 Faça o download do pacote de atualização referente ao dispositivo para o qual você deseja fazer o upgrade.

---

**Observação** Primeiro, você deve fazer o upgrade do dispositivo primário.

---

O vCloud Director é distribuído como um arquivo executável com um nome no formato `VMware_vCloud_Director_v.v.v.v-nnnnnnnn_update.tar.gz`, em que `v.v.v.v` representa a versão do produto e `nnnnnnnn`, o número da compilação. Por exemplo, `VMware_vCloud_Director_10.0.0.4424-14420378_update.tar.gz`.

- 3 Crie o diretório `local-update-package` para extrair o pacote de atualização.

```
mkdir /tmp/local-update-package
```



- 4 Extraia o pacote de atualização no diretório recém-criado.

```
tar -zxvf VMware_vCloud_Director_v.v.v-nnnnnnnn_update.tar.gz \
-C /tmp/local-update-package
```

- 5 Defina o diretório local-update-package como o repositório de atualização.

```
vamicli update --repo file:///tmp/local-update-package
```

- 6 Verifique se há atualizações para conferir se você estabeleceu corretamente o repositório.

```
vamicli update --check
```

A versão do upgrade aparece como Atualização Disponível.

- 7 Encerre o vCloud Director executando o seguinte comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 8 Aplique o upgrade disponível.

```
vamicli update --install latest
```

- 9 Repita os passos de 2 a 8 nas células restantes em modo de espera e de aplicativos.

- 10 No dispositivo primário, faça backup do banco de dados do dispositivo vCloud Director incorporado.

```
/opt/vmware/appliance/bin/create-db-backup
```

- 11 Em qualquer dispositivo, execute o utilitário upgrade do banco de dados vCloud Director.

```
/opt/vmware/vcloud-director/bin/upgrade
```

- 12 Reinicie cada dispositivo do vCloud Director.

```
shutdown -r now
```

#### Próximo passo

- Se o upgrade for bem-sucedido, você poderá excluir o instantâneo do dispositivo do vCloud Director.
- Se o upgrade não for bem-sucedido, você poderá reverter o dispositivo do vCloud Director para o instantâneo que tirou antes do upgrade. Consulte [Reverter um dispositivo do vCloud Director quando um upgrade falhar](#).

## Reverter um dispositivo do vCloud Director quando um upgrade falhar

Se o upgrade de um dispositivo do vCloud Director falhar, você poderá usar o instantâneo do dispositivo que tirou antes do upgrade e reverter o dispositivo do vCloud Director.

Antes de iniciar a reversão, conclua o procedimento descrito em [Verificar o status de um cluster de alta disponibilidade do banco de dados](#). Anote os IDs de nó dos nós em espera no cluster.

- 1 Reverta o dispositivo primário do vCloud Director para o instantâneo que você tirou antes de iniciar o upgrade.

Leia como restaurar instantâneos da máquina virtual usando as opções de reversão. Consulte [Restaurar instantâneos de VM usando reversão](#) no *Guia de Administração de Máquinas Virtuais do vSphere*.

- 2 Ligue a célula primária do dispositivo do vCloud Director.
- 3 Faça login diretamente ou usando um cliente SSH no sistema operacional de cada célula do dispositivo do vCloud Director. Você deve fazer login como usuário **root**.
- 4 Pare os serviços do vCloud Director em todas as células do dispositivo.

```
service vmware-vcd stop
```

- 5 Use a célula primária do vCloud Director para cancelar o registro dos nós secundários no cluster.
  - a Faça login diretamente ou usando um cliente SSH no sistema operacional da célula primária como **root**.
  - b Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- c Execute o comando para cancelar o registro de uma célula do dispositivo em espera. Para cancelar o registro de um nó em espera que não está em execução, você deve fornecer o ID do nó.

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister --node-id=ID do nó -f /opt/vmware/vpostgres/current/etc/repmgr.conf
```

- d Repita [5.c](#) para cancelar o registro da outra célula do dispositivo em espera.
- 6 No vSphere Client, encerre e exclua todos os dispositivos em espera.
  - a No vSphere Client, navegue até os dispositivos em espera.
  - b Clique com o botão direito do mouse em um dispositivo em espera e clique em **Ligar/Desligar > Encerrar SO Convidado**.
  - c Clique com o botão direito do mouse no dispositivo e clique em **Excluir do Disco**.

- d Repita 6.a por meio de 6.c para a outra célula do dispositivo em espera.
- 7 Verifique se o conjunto de ferramentas `repmgr` e o banco de dados PostgreSQL incorporado da célula primária do dispositivo do vCloud Director estão funcionando corretamente.
  - a Altere o usuário para **postgres**.

```
sudo -i -u postgres
```

- b Execute o comando para verificar o status do cluster.

```
/opt/vmware/vpostgres/current/bin/repmgr cluster show
```

A saída do console mostra informações sobre o único nó no cluster.

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	Nome do nó	primary	*running			default   host=endereço IP do host user=repmgr dbname=repmgr

- 8 Reimplante os dispositivos secundários. Consulte [Implantar o dispositivo do vCloud Director usando o vSphere Client](#).
- 9 Faça login diretamente ou usando um cliente SSH no sistema operacional de cada célula do dispositivo do vCloud Director. Você deve fazer login como usuário **root**.
- 10 Inicie os serviços do vCloud Director.

```
service vmware-vcd start
```

## Fazer upgrade do dispositivo do vCloud Director usando o Repositório de Atualização da VMware

Você pode usar o Repositório de Atualização da VMware para fazer upgrade do dispositivo do vCloud Director da versão 9.7 para a 10.0.

**Observação** Você pode usar o Repositório de atualização do VMware somente para atualizar o vCloud Director para a versão mais recente do vCloud Director. Somente a versão mais recente está disponível no repositório de atualização da VMware. Se você quiser atualizar o vCloud Director para uma versão diferente, consulte [Fazer upgrade do dispositivo do vCloud Director](#).

Durante o upgrade da implantação do dispositivo do vCloud Director, o serviço vCloud Director para de funcionar, e um certo tempo de inatividade pode ser esperado. O tempo de inatividade depende do tempo necessário para fazer upgrade de cada dispositivo do vCloud Director e executar o script de atualização do banco de dados vCloud Director. O número de células de

trabalho no grupo de servidores vCloud Director será reduzido até que você pare o serviço vCloud Director no último dispositivo vCloud Director. Um balanceador de carga configurado adequadamente na frente dos endpoints HTTP do vCloud Director deve parar o roteamento do tráfego para as células que estão paradas.

Depois de aplicar o upgrade a cada dispositivo do vCloud Director e o upgrade do banco de dados estiver concluído, você deverá reinicializar cada dispositivo do vCloud Director.

### Pré-requisitos

Verifique se o dispositivo do vCloud Director tem acesso ao <https://vapp-updates.vmware.com>.

### Procedimentos

- 1 Em um navegador da Web, faça login na interface do usuário de gerenciamento do dispositivo de uma instância de dispositivo vCloud Director para identificar o dispositivo primário, [https://appliance\\_ip\\_address:5480](https://appliance_ip_address:5480).

Anote o nome do dispositivo primário. Você deverá usar o nome do dispositivo primário ao fazer backup do banco de dados.

- 2 Redefina o repositório de atualização para apontar para o Repositório de Atualização da VMware.

```
vamicli update --repo ""
```

- 3 Verifique se há atualizações para verificar se o Repositório de Atualização da VMware tem o upgrade desejado.

Por padrão, o comando `vamicli` aponta para o Repositório de Atualização da VMware.

```
vamicli update --check
```

A versão do upgrade aparece como **Atualização Disponível**.

- 4 Encerre o vCloud Director executando o seguinte comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 5 Aplique o upgrade disponível.

```
vamicli update --install latest
```

- 6 Repita de [Etapa 2](#) a [Etapa 4](#) em cada dispositivo.

- 7 No dispositivo primário, faça backup do banco de dados do dispositivo vCloud Director incorporado.

```
/opt/vmware/appliance/bin/create-db-backup
```

- 8 Em qualquer dispositivo, execute o utilitário upgrade do banco de dados vCloud Director.

```
/opt/vmware/vcloud-director/bin/upgrade
```

- 9 Reinicie cada dispositivo do vCloud Director.

```
shutdown -r now
```

## Realizar uma atualização orquestrada de uma instalação do vCloud Director

Você pode atualizar todas as células no grupo de servidores junto com o banco de dados compartilhado executando o instalador do vCloud Director com a opção `--private-key-path`.

Você pode usar o instalador do vCloud Director para Linux para fazer upgrade de um grupo de servidor do vCloud Director que consiste de instalações do vCloud Director em um SO Linux com suporte. Se o seu grupo de servidores vCloud Director consistir de implantações de dispositivos do vCloud Director 9.5, use o instalador do vCloud Director para Linux para atualizar o ambiente existente somente como parte do fluxo de trabalho de migração. Consulte [Capítulo 13 Migrando para o dispositivo do vCloud Director](#).

O vCloud Director para Linux é distribuído como um arquivo executável assinado digitalmente com um nome do formulário `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, onde `v.v.v` representa a versão do produto e `nnnnnn` o número da compilação. Por exemplo: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. A execução desse executável instala ou atualiza o vCloud Director.

Quando você executa o instalador do vCloud Director com a opção `--private-key-path`, pode adicionar outras opções de comando do utilitário `upgrade`, por exemplo, `--maintenance-cell`. Para obter informações sobre as opções de utilitário do banco de dados `upgrade`, consulte [Referência do utilitário de atualização de banco de dados](#).

### Pré-requisitos

- Verifique se o banco de dados do vCloud Director, os componentes do vSphere e os componentes do NSX são compatíveis com a nova versão do vCloud Director.

---

**Importante** Se a sua instalação existente do vCloud Director usar um banco de dados Oracle ou um banco de dados Microsoft SQL Server, verifique se você migrou para um banco de dados PostgreSQL antes de fazer upgrade para a versão do vCloud Director 10.0. Para os caminhos de upgrade possíveis, consulte [Capítulo 12 Atualizando o vCloud Director](#).

---

- Verifique se você tem as credenciais de superusuário para o servidor de destino.
- Se você quiser que o instalador verifique a assinatura digital do arquivo de instalação, baixe e instale a chave pública da VMware para o servidor de destino. Se você já verificou a assinatura digital do arquivo de instalação, não é necessário verificá-la novamente durante a instalação. Consulte [Baixe e instale a chave pública da VMware](#).

- Verifique se você tem uma chave de licença válida para usar a versão do software vCloud Director para o qual você está atualizando.
- Verifique se todas as células permitem conexões SSH do superusuário sem uma senha. Para realizar uma verificação, você pode executar o seguinte comando Linux:

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

Esse exemplo define a sua identidade como vcloud e, em seguida, faz uma conexão SSH à célula em *cell-ip* como raiz, mas não fornece a senha raiz. Se a chave privada em *private-key-path* na célula local for legível pelo usuário vcloud.vcloud e a chave pública correspondente estiver presente no arquivo *authorized-keys* para o usuário raiz em *cell-ip*, o comando será bem-sucedido.

---

**Observação** O usuário do vcloud, o grupo do vcloud e a conta do vcloud.vcloud são criados pelo instalador do vCloud Director para ser usado como uma identidade com a qual os processos do vCloud Director são executados. O usuário do vcloud não tem nenhuma senha.

---

- Verifique se todos os hosts ESXi estão ativados. Começando com o vCloud Director 9.5, os hosts ESXi desativados não têm suporte.
- Verifique se todos os servidores do grupo de servidores podem acessar o armazenamento do servidor de transferência compartilhado. Consulte [Preparando o armazenamento do servidor de transferência](#).
- Se a instalação do vCloud Director usa um servidor LDAPS, para evitar falhas de login do LDAP após a atualização, verifique se você tem um certificado criado corretamente para o Java 8 atualização 181. Para obter informações, consulte as *Alterações da versão do Java 8* em <https://www.java.com>.

## Procedimentos

- 1 Faça login no servidor de destino como **raiz**.

- 2 Baixe o arquivo de instalação para o servidor de destino.

Se você comprou o software na mídia, copie o arquivo de instalação para um local que seja acessível ao servidor de destino.

- 3 Verifique se a soma de verificação do download corresponde à soma de verificação lançada na página de download.

Os valores para as somas de verificação MD5 e SHA1 são lançados na página de download. Use a ferramenta adequada para verificar se a soma de verificação do arquivo de instalação baixado corresponde à soma de verificação mostrada na página de download. Um comando do Linux da seguinte forma exibe a soma de verificação para o *installation-file*.

```
[root@cell11 /tmp]# md5sum installation-file
```

O comando retorna a soma de verificação do arquivo de instalação que deve corresponder à soma de verificação MD5 da página de download.

**4** Certifique-se de que o arquivo de instalação seja executável.

O arquivo de instalação requer a permissão de execução. Para ter certeza de que ele tem essa permissão, abra uma janela de console, shell ou terminal e execute o seguinte comando do Linux, onde o *arquivo de instalação* é o nome do caminho completo para o arquivo de instalação do vCloud Director.

```
[root@cell1 /tmp]# chmod u+x installation-file
```

**5** Em um console, shell ou janela de terminal, execute o arquivo de instalação com a opção `--private-key-path` e o nome do caminho para a chave particular da célula de destino.

Você pode adicionar outras opções de comando do utilitário `upgrade` de banco de dados.

```
./installation-file --private-key-path /vcloud/.ssh/id_rsa
```

---

**Observação** Você não pode executar o arquivo de instalação de um diretório cujo nome do caminho inclui caracteres de espaço incorporado.

---

O instalador detecta uma versão anterior do vCloud Director e solicita que você confirme o upgrade.

Se o instalador detectar uma versão do vCloud Director igual ou posterior à versão no arquivo de instalação, ele exibirá uma mensagem de erro e será encerrado.

**6** Insira **y** e pressione ENTER para confirmar o upgrade.**Resultados**

O instalador inicia o seguinte fluxo de trabalho de upgrade de várias células.

- 1 Verifica se o host de célula atual atende a todos os requisitos.
- 2 Desempacota o pacote RPM do vCloud Director.
- 3 Atualiza o software do vCloud Director na célula atual.
- 4 Atualiza o banco de dados vCloud Director.
- 5 Atualiza o software vCloud Director em cada uma das células restantes e reinicia os serviços do vCloud Director na célula.
- 6 Reinicia os serviços do vCloud Director na célula atual.

**Próximo passo**

Inicie os serviços do vCloud Director em todas as células do grupo de servidores.

Agora, você pode [Atualizar cada NSX Manager associado a um sistema vCenter Server anexado](#) e depois [Atualizar sistemas vCenter Server, hosts ESXi e NSX Edges](#) .

## Atualizar manualmente uma instalação do vCloud Director

Você pode atualizar uma única célula executando o instalador do vCloud Director sem opções de comando. Antes de reiniciar uma célula atualizada, você deve atualizar o esquema do banco de dados. Você atualiza o esquema do banco de dados depois de atualizar pelo menos uma célula no grupo de servidores.

Você pode usar o instalador do vCloud Director para Linux para fazer upgrade de um grupo de servidor do vCloud Director que consiste de instalações do vCloud Director em um SO Linux com suporte. Se o seu grupo de servidores vCloud Director consistir de implantações de dispositivos do vCloud Director 9.5, use o instalador do vCloud Director para Linux para atualizar o ambiente existente somente como parte do fluxo de trabalho de migração. Consulte [Capítulo 13 Migrando para o dispositivo do vCloud Director](#).

Para uma instalação do vCloud Director de várias células, em vez de fazer upgrade manualmente de cada célula e do banco de dados em uma sequência, você pode realizar um upgrade orquestrado da instalação do vCloud Director. Consulte [Realizar uma atualização orquestrada de uma instalação do vCloud Director](#).

### Pré-requisitos

- Verifique se o banco de dados do vCloud Director, os componentes do vSphere e os componentes do NSX são compatíveis com a nova versão do vCloud Director.

---

**Importante** Se a sua instalação existente do vCloud Director usar um banco de dados Oracle ou um banco de dados Microsoft SQL Server, verifique se você migrou para um banco de dados PostgreSQL antes de fazer upgrade para a versão do vCloud Director 10.0. Para os caminhos de upgrade possíveis, consulte [Capítulo 12 Atualizando o vCloud Director](#).

---

- Verifique se você tem credenciais de superusuário para os servidores no seu grupo de servidores do vCloud Director.
- Se você quiser que o instalador verifique a assinatura digital do arquivo de instalação, baixe e instale a chave pública da VMware para o servidor de destino. Se você já verificou a assinatura digital do arquivo de instalação, não é necessário verificá-la novamente durante a instalação. Consulte [Baixe e instale a chave pública da VMware](#).
- Verifique se você tem uma chave de licença válida para usar a versão do software vCloud Director para o qual você está atualizando.
- Verifique se todos os hosts ESXi estão ativados. Começando com o vCloud Director 9.5, os hosts ESXi desativados não têm suporte.

### Procedimentos

#### 1 [Atualizar uma célula do vCloud Director](#)

O instalador do vCloud Director verifica se o servidor de destino atende a todos os pré-requisitos de atualização e atualiza o software do vCloud Director no servidor.



## 2 Atualizar o banco de dados do vCloud Director

De um servidor vCloud Director atualizado, você executa uma ferramenta que atualiza o banco de dados do vCloud Director. Você não deve reiniciar qualquer servidor vCloud Director atualizado antes de atualizar o banco de dados compartilhado.

### Próximo passo

- Depois de atualizar todos os servidores do vCloud Director no grupo de servidores e no banco de dados, você pode iniciar os serviços do vCloud Director em todas as células.
- [Atualizar cada NSX Manager associado a um sistema vCenter Server anexado](#)
- Depois de atualizar cada NSX Manager, você pode fazer upgrade dos sistemas do vCenter Server, hosts e NSX edges. Consulte [Atualizar sistemas vCenter Server, hosts ESXi e NSX Edges](#).

## Atualizar uma célula do vCloud Director

O instalador do vCloud Director verifica se o servidor de destino atende a todos os pré-requisitos de atualização e atualiza o software do vCloud Director no servidor.

O vCloud Director para Linux é distribuído como um arquivo executável assinado digitalmente com um nome do formulário `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, onde `v.v.v` representa a versão do produto e `nnnnnn` o número da compilação. Por exemplo: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. A execução desse executável instala ou atualiza o vCloud Director.

Para uma instalação do vCloud Director de várias células, você deve executar o instalador do vCloud Director em cada membro do grupo de servidores do vCloud Director.

### Procedimentos

- 1 Faça login no servidor de destino como **raiz**.
- 2 Baixe o arquivo de instalação para o servidor de destino.  
  
Se você comprou o software na mídia, copie o arquivo de instalação para um local que seja acessível ao servidor de destino.
- 3 Verifique se a soma de verificação do download corresponde à soma de verificação lançada na página de download.

Os valores para as somas de verificação MD5 e SHA1 são lançados na página de download. Use a ferramenta adequada para verificar se a soma de verificação do arquivo de instalação baixado corresponde à soma de verificação mostrada na página de download. Um comando do Linux da seguinte forma exibe a soma de verificação para o *installation-file*.

```
[root@cell1 /tmp]# md5sum installation-file
```

O comando retorna a soma de verificação do arquivo de instalação que deve corresponder à soma de verificação MD5 da página de download.

**4** Certifique-se de que o arquivo de instalação seja executável.

O arquivo de instalação requer a permissão de execução. Para ter certeza de que ele tem essa permissão, abra uma janela de console, shell ou terminal e execute o seguinte comando do Linux, onde o *arquivo de instalação* é o nome do caminho completo para o arquivo de instalação do vCloud Director.

```
[root@cell1 /tmp]# chmod u+x installation-file
```

**5** Execute o arquivo de instalação.

Para executar o arquivo de instalação, insira o nome do caminho completo, por exemplo:

```
[root@cell1 /tmp]# ./installation-file
```

O arquivo inclui um script de instalação e um pacote RPM incorporado.

---

**Observação** Você não pode executar o arquivo de instalação de um diretório cujo nome do caminho inclui caracteres de espaço incorporado.

---

Se o instalador detectar uma versão do vCloud Director igual ou posterior à versão no arquivo de instalação, ele exibirá uma mensagem de erro e será encerrado.

Se o instalador detectar uma versão anterior do vCloud Director, ele solicitará que você confirme o upgrade.

**6** Insira **y** e pressione ENTER para confirmar o upgrade.

O instalador inicia o seguinte fluxo de trabalho de upgrade.

- a Verifica se o host atende a todos os requisitos.
- b Desempacota o pacote RPM do vCloud Director.
- c Depois que todos os trabalhos ativos do vCloud Director ativos na célula forem finalizados, ele interrompe os serviços do vCloud Director no servidor e atualiza o software do vCloud Director instalado.

Se você não tiver instalado a chave pública da VMware no servidor de destino, o instalador exibirá um aviso no seguinte formato:

```
warning: installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

Ao alterar o arquivo `global.properties` existente no servidor de destino, o instalador exibirá um aviso no seguinte formato:

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-director/etc/global.properties.rpmnew
```

---

**Observação** Se você tiver atualizado anteriormente o arquivo `global.properties` existente, poderá recuperar as alterações de `global.properties.rpmnew`.

---

## 7 (Opcional) Atualize as propriedades de log.

Após um upgrade, novas propriedades de log são gravadas no arquivo `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew`.

Opção	Ação
<b>Se você não alterou as propriedades de log existentes</b>	Copie este arquivo para <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> .
<b>Se você alterou as propriedades de log</b>	Para preservar suas alterações, mescle <code>/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew</code> com o arquivo <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> existente.

### Resultados

Quando a atualização do vCloud Director for concluída, o instalador exibirá uma mensagem com informações sobre o local dos arquivos de configuração antigos. Em seguida, o instalador solicitará que você execute a ferramenta de atualização de banco de dados.

### Próximo passo

Se ainda não tiver atualizado, você poderá atualizar o banco de dados do vCloud Director.

Repita esse procedimento em cada célula do vCloud Director no grupo de servidores.

**Importante** Não inicie os serviços do vCloud Director até atualizar todas as células no grupo de servidores e no banco de dados.

## Atualizar o banco de dados do vCloud Director

De um servidor vCloud Director atualizado, você executa uma ferramenta que atualiza o banco de dados do vCloud Director. Você não deve reiniciar qualquer servidor vCloud Director atualizado antes de atualizar o banco de dados compartilhado.

Informações sobre todas as tarefas em execução e concluídas recentemente são armazenadas no banco de dados do vCloud Director. Como uma atualização de banco de dados invalida essas informações de tarefa, o utilitário de atualização de banco de dados verifica se nenhuma tarefa está sendo executada quando o processo de atualização começa.

Todas as células em um grupo de servidores do vCloud Director compartilham o mesmo banco de dados. Independentemente de quantas células você está atualizando, o banco de dados é atualizado apenas uma vez. Depois que o banco de dados for atualizado, as células do vCloud Director que não forem atualizadas não poderão se conectar ao banco de dados. Você deve fazer upgrade de todas as células para que elas se conectem ao banco de dados atualizado.

### Pré-requisitos

- Faça backup de seu banco de dados existente. Use os procedimentos que o fornecedor de software de banco de dados recomenda.

- Verifique se todas as células do vCloud Director do grupo de servidores estão interrompidas. As células atualizadas são interrompidas durante o processo de atualização. Se existirem servidores vCloud Director que ainda não foram atualizados, você poderá utilizar a ferramenta de gerenciamento de células para desativar e encerrar os respectivos serviços. Para obter informações sobre como gerenciar uma célula usando a ferramenta de gerenciamento de células, consulte [Capítulo 10 Referência da ferramenta de gerenciamento de células](#).
- Revise o tópico [Referência do utilitário de atualização de banco de dados](#).

## Procedimentos

- 1 Execute o utilitário upgrade de banco de dados com ou sem opções.

```
/opt/vmware/vcloud-director/bin/upgrade
```

Se o utilitário de atualização do banco de dados detectar uma versão incompatível do NSX Manager, ele exibirá uma mensagem de aviso e cancelará a atualização.

- 2 No prompt, insira **y** e pressione ENTER para confirmar a atualização do banco de dados.
- 3 No prompt, insira **y** e pressione ENTER para confirmar que você fez backup do banco de dados.

Se você usou a opção `--backup-completed`, o utilitário ignora esse prompt.

- 4 Se o utilitário detectar uma célula ativa, no prompt para continuar, insira **n** para sair do shell e, em seguida, verifique se não há células em execução e repita a atualização desde a [Etapa 1](#).

## Resultados

A ferramenta de atualização de banco de dados é executada e exibe mensagens de andamento. Quando a atualização for concluída, você será solicitado a iniciar o serviço vCloud Director no servidor atual.

## Próximo passo

Insira **y** e pressione Enter ou inicie o serviço em um momento posterior, executando o comando `service vmware-vcd start`.

Você pode iniciar os serviços dos servidores do vCloud Director atualizados.

Você pode atualizar o restante dos membros do vCloud Director do grupo de servidores e iniciar seus serviços. Consulte [Atualizar uma célula do vCloud Director](#).

# Referência do utilitário de atualização de banco de dados

Quando você executa o utilitário `upgrade`, fornece as informações de configuração na linha de comando como opções e argumentos.

O local do utilitário `upgrade` é `/opt/vmware/vcloud-director/bin/`.

Tabela 12-1. Opções e argumentos do utilitário de atualização de banco de dados

Opção	Argumento	Descrição
<code>--backup-completed</code>	Nenhum	Especifica que você concluiu um backup do vCloud Director. Quando você inclui essa opção, o utilitário de atualização não solicita que você faça backup do banco de dados.
<code>--ceip-user</code>	O nome de usuário da conta do serviço CEIP.	Se um usuário com esse nome de usuário já existir na organização do sistema, o upgrade falhará. Padrão: <code>phone-home-system-account</code> .
<code>--enable-ceip</code>	Escolha um: <ul style="list-style-type: none"> <li>■ <code>true</code></li> <li>■ <code>false</code></li> </ul>	Especifica se essa instalação participa do Programa de aperfeiçoamento da experiência do cliente (CEIP) da VMware. O padrão é <code>true</code> se não for fornecido e não definido como <code>false</code> na configuração atual. O Programa de Aperfeiçoamento da Experiência do Cliente ("CEIP") da VMware fornece informações adicionais sobre os dados coletados por meio do CEIP e as finalidades para as quais eles são usados pela VMware. Essas informações podem ser encontradas no Centro de Confiança e Garantia, em <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> . Você pode usar a ferramenta de gerenciamento de células para participar ou sair do CEIP da VMware para este produto a qualquer momento. Consulte <a href="#">Capítulo 10 Referência da ferramenta de gerenciamento de células</a> .
<code>--installer-path</code>	Nome do caminho completo para o arquivo de instalação do vCloud Director. O arquivo de instalação e o diretório no qual ele está armazenado devem ser legíveis pelo usuário <code>vcloud.vcloud</code> .	Requer a opção <code>--private-key-path</code> .

Tabela 12-1. Opções e argumentos do utilitário de atualização de banco de dados (continuação)

Opção	Argumento	Descrição
<code>--maintenance-cell</code>	Endereço IP	O endereço IP de uma célula para o utilitário de upgrade a ser executado no modo de manutenção durante o upgrade. Essa célula entra no modo de manutenção antes que as outras células sejam desligadas e permanece no modo de manutenção enquanto outras células são atualizadas. Depois que as outras células forem atualizadas e pelo menos uma delas tiver sido iniciada novamente, esta célula será encerrada e atualizada. Requer a opção <code>--private-key-path</code> .
<code>--multisite-user</code>	O nome de usuário para a conta de sistema multisite.	Essa conta é usada pelo recurso Multisite do vCloud Director. Se um usuário com esse nome de usuário já existir na organização do sistema, o upgrade falhará. Padrão: <code>multisite-system-account</code> .
<code>--private-key-path</code>	nome do caminho	O nome do caminho completo para a chave privada da célula. Quando você usar essa opção, todas as células do grupo de servidores serão normalmente encerradas, atualizadas e reiniciadas depois que o banco de dados tiver sido atualizado. Consulte <a href="#">Realizar uma atualização orquestrada de uma instalação do vCloud Director</a> para obter mais informações sobre esse fluxo de trabalho de atualização.
<code>--unattended-upgrade</code>	Nenhum	Especifica a atualização autônoma

Se você usar a opção `--private-key-path`, todas as células deverão ser configuradas para permitir conexões ssh do superusuário sem uma senha. Você pode usar uma linha de comando do Linux como aquela mostrada aqui para verificar isso. Este exemplo define sua identidade para `vcloud` e, em seguida, faz uma conexão ssh com a célula em `cell-ip` como `root`, mas não fornece a senha raiz.

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

Se a chave privada em *private-key-path* na célula local for legível pelo usuário `vcloud.vcloud` e a chave pública correspondente tiver sido adicionada ao arquivo `authorized-keys` para o usuário raiz em *cell-ip*, o comando será bem-sucedido.

---

**Observação** O usuário do `vcloud`, o grupo do `vcloud` e a conta do `vcloud.vcloud` são criados pelo instalador do vCloud Director para ser usado como uma identidade com a qual os processos do vCloud Director são executados. O usuário do `vcloud` não tem nenhuma senha.

---

# Migrando para o dispositivo do vCloud Director

# 13

A partir da versão 9.7, o dispositivo do vCloud Director inclui um banco de dados PostgreSQL incorporado com uma função de alta disponibilidade. Você pode migrar sua versão anterior existente do ambiente do vCloud Director com um banco de dados PostgreSQL externo para um ambiente do vCloud Director que consiste em implantações de dispositivos do vCloud Director 10.0.

Você pode migrar um ambiente vCloud Director que consiste em instalações do vCloud Director no Linux ou em implantações de dispositivos do vCloud Director. A partir da versão 10.0, o banco de dados Microsoft SQL não é mais compatível, e você pode migrar apenas um ambiente do vCloud Director que usa um banco de dados PostgreSQL externo.

Se o seu ambiente vCloud Director usar um banco de dados externo Oracle ou Microsoft SQL externo, você deverá migrar para um banco de dados PostgreSQL antes de fazer upgrade para o vCloud Director 10.0. Para conhecer os caminhos de upgrade, consulte [Capítulo 12 Atualizando o vCloud Director](#).

Este capítulo inclui os seguintes tópicos:

- [Migrando o vCloud Director com um banco de dados externo PostgreSQL para um dispositivo do vCloud Director](#)

## Migrando o vCloud Director com um banco de dados externo PostgreSQL para um dispositivo do vCloud Director

Se o seu ambiente do vCloud Director atual usar um banco de dados PostgreSQL externo, você poderá migrar para um novo ambiente do vCloud Director formado por implantações de dispositivos do vCloud Director. Seu ambiente atual do vCloud Director pode consistir em instalações do vCloud Director no Linux ou em implantações de dispositivos do vCloud Director. O novo ambiente vCloud Director pode usar os bancos de dados PostgreSQL incorporados do dispositivo em um modo de alta disponibilidade.

O fluxo de trabalho de migração inclui quatro estágios principais.

- Atualizando o ambiente vCloud Director existente
- Criando o novo grupo de servidores vCloud Director implantando uma ou mais instâncias do dispositivo do vCloud Director
- Migrando o banco de dados externo para o banco de dados incorporado



- Copiando os dados do serviço de transferência compartilhada e os dados de certificados.

## Procedimento

- 1 Se o seu banco de dados PostgreSQL externo atual for da versão 9.x, faça upgrade do banco de dados PostgreSQL externo para a versão 10 ou posterior.

- 2 Faça upgrade do seu ambiente vCloud Director atual para a versão 10.0.

Consulte [Capítulo 12 Atualizando o vCloud Director](#).

- 3 Verifique se a reinicialização do vCloud Director de origem de migração foi bem-sucedida.

- 4 Em cada célula do ambiente vCloud Director atualizado, execute o comando para interromper o serviço vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <nome de usuário administrador> cell -- shutdown
```

- 5 No banco de dados PostgreSQL externo, faça backup do banco de dados atual.

```
sudo -u postgres path_to_pg_dump -Fc db_name > /tmp/db_dump_name
```

Se não houver espaço livre suficiente na pasta /tmp, use outra localização para armazenar o arquivo de despejo.

- 6 Se o proprietário do banco de dados e o nome do banco de dados forem diferentes de vcloud, anote esses valores.

Você deverá criar esse usuário no novo ambiente e renomear o banco de dados na Etapa 13.

- 7 Se quiser que o novo ambiente vCloud Director use os endereços IP do ambiente existente, deverá copiar as propriedades e os arquivos de certificados para uma localização no banco de dados PostgreSQL externo e desligar as células.

- a Copie os arquivos `global.properties`, `responses.properties`, `certificates`, `proxycertificates` e `truststore`, localizados em `/opt/vmware/vcloud-director/etc/`, para /tmp ou qualquer local preferido no banco de dados PostgreSQL externo.

- b Desligue as células no ambiente existente.

- 8 Se quiser que o novo ambiente vCloud Director use o servidor NFS do ambiente existente, crie e exporte um novo diretório neste servidor NFS como o novo ponto de montagem compartilhado do NFS.

Não é possível reutilizar o ponto de montagem existente, pois os IDs de usuário e de grupo (UID/GID) dos usuários no NFS antigo podem não corresponder aos IDs de usuário e de grupo no novo NFS.

- 9 Crie o novo grupo de servidores implantando uma ou mais instâncias do dispositivo do vCloud Director 10.0.
  - Se quiser usar a função de alta disponibilidade do banco de dados, implante uma célula primária e duas células em espera e, opcionalmente, uma ou mais células de aplicativo vCD.
  - Se você tiver desligado as células no ambiente existente, poderá usar os endereços IP originais para as novas células.
  - Se você tiver exportado um novo caminho no servidor NFS existente, você poderá usar esse novo ponto de montagem compartilhado para o novo ambiente.

Consulte [Capítulo 6 Implantação do vCloud DirectorAppliance](#).

- 10 Em cada nova célula implantada, execute o comando para interromper o serviço vCloud Director.

```
service vmware-vcd stop
```

- 11 Copie o arquivo de despejo da pasta /tmp no banco de dados PostgreSQL externo para a pasta /tmp na célula primária do novo ambiente.

Consulte a Etapa 5.

- 12 Altere as permissões no arquivo de despejo.

```
chmod a+r /tmp/db_dump_name
```

- 13 Faça login como **root** para o console da célula primária recém implantada e transfira o banco de dados vCloud Director do externo para o banco de dados incorporado.

- a Alterne o usuário para postgres, conecte-se ao terminal do banco de dados psql e execute a instrução para descartar o banco de dados vcloud.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

- b Se o proprietário do banco de dados externo existente for diferente de vcloud, crie um usuário com o nome que você anotou na Etapa 6.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'CREATE USER
<db_owner_external_pg>;'
```

- c Execute o comando pg\_restore.

```
sudo -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/db_dump_name
```

- d Se o nome do banco de dados externo existente for diferente de vcloud, altere o nome do banco de dados para vcloud usando o nome que você anotou na Etapa 6.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE
<db_name_external_pg> RENAME TO vcloud;'
```

- e Se o proprietário do banco de dados do ambiente vCloud Director existente for diferente de vcloud, altere o proprietário do banco de dados para vcloud e reatribua as tabelas a vcloud.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE vcloud OWNER TO vcloud;'
```

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -d vcloud -c 'REASSIGN OWNED BY <db_owner_external_pg> TO vcloud;'
```

- 14 Em cada nova célula implantada, faça backup e substitua os dados de configuração e reconfigure e inicie o serviço vCloud Director.

- a Faça backup das propriedades, do truststore e dos arquivos de certificados e copie e substitua esses arquivos do local no banco de dados PostgreSQL externo da origem de migração para o qual você copiou os arquivos na etapa 7a.

Os arquivos `global.properties`, `responses.properties`, `truststore`, `certificates` e `proxycertificates` estão em `/opt/vmware/vcloud-director/etc/`.

- b Faça backup do repositório de chaves localizado em `/opt/vmware/vcloud-director/certificates.ks`.

Não copie e substitua pelo arquivo de armazenamento de chaves da origem de migração.

- c Execute o comando para reconfigurar o serviço vCloud Director.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

Em que:

- O valor `--keystore-password` corresponde à senha **root** inicial desse dispositivo.
- O valor `--database-password` corresponde à senha de banco de dados que você define durante a implantação do dispositivo.
- O valor de `--database-host` corresponde ao endereço IP da rede eth1 do dispositivo primário.
- O valor de `--primary-ip` corresponde ao endereço IP da rede eth0 do dispositivo.
- O valor de `--console-proxy-ip` corresponde ao endereço IP da rede eth0 do dispositivo.
- O valor de `--console-proxy-port` corresponde à porta 8443 do proxy do console do dispositivo.

Para obter informações sobre solução de problemas, consulte [A reconfiguração do serviço do vCloud Director falha ao migrar ou restaurar para o dispositivo vCloud Director](#).

- d Execute o comando para iniciar o serviço vCloud Director.

```
service vmware-vcd start
```

Você pode monitorar o progresso da inicialização da célula em `/opt/vmware/vcloud-director/logs/cell.log`.

- 15 Modifique a configuração do balanceador de carga para incluir todos os novos IPs do eth0 do dispositivo nos pools do balanceador de carga para o tráfego HTTP, HTTPS e TCP e remova os IPs antigos de célula do vCloud Director da Linux desses pools.
- 16 Depois que todas as células do novo grupo de servidores terminarem o processo de inicialização, verifique se a migração do seu ambiente vCloud Director foi bem-sucedida.
  - a Abra o Service Provider Admin Portal usando o endereço IP de rede eth0 de qualquer célula do novo grupo de servidores, `https://eth0_IP_new_cell/provider`.
  - b Faça login no Service Provider Admin Portal com suas credenciais de **administrador de sistema** existentes.
  - c Confirme se os seus recursos do vSphere e de nuvem estão disponíveis no novo ambiente.
- 17 Após a verificação bem-sucedida da migração do vCloud Director, use o Service Provider Admin Portal para excluir as células desconectadas que pertencem ao ambiente vCloud Director antigo.
  - a No menu principal () , selecione **Recursos de Nuvem**.
  - b No painel esquerdo, clique em **Células da Nuvem**.
  - c Selecione uma célula inativa e clique em **Cancelar registro**.

Você pode implantar o dispositivo do vCloud Director para adicionar membros ao grupo de servidores do ambiente migrado.

## O que fazer em seguida

O novo ambiente do dispositivo do vCloud Director migrado usa certificados autoassinados. Para usar os certificados bem assinados do ambiente antigo, em cada célula do novo ambiente, siga estas etapas:

- 1 Copie e substitua o arquivo de armazenamento de chaves da célula antiga para `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.
- 2 Execute o comando da ferramenta de gerenciamento de célula para substituir os certificados.

Certifique-se de que vcloud.vcloud seja o proprietário desse arquivo.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/  
vcloud-director/data/transfer/certificates.ks \  
--keystore-password ks_password_old_vCD
```

3 Reinicie o serviço vCloud Director.

```
service vmware-vcd restart
```

Se você adicionar novos membros a esse grupo de servidores, as novas células do dispositivo serão implantadas com esses certificados bem assinados.

# Depois de atualizar ou migrar o vCloud Director

# 14

Depois de atualizar ou migrar todos os servidores do vCloud Director e o banco de dados compartilhado, você pode atualizar as instâncias do NSX Manager que fornecem serviços de rede para a sua nuvem. Depois disso, você poderá atualizar os hosts do ESXi e as instâncias do vCenter Server que estão registradas em sua instalação do vCloud Director.

---

**Importante** A partir da versão 9.7, o vCloud Director suporta somente edge gateways avançados. Você deve converter qualquer edge gateway não avançado herdado em um gateway avançado. Consulte <https://kb.vmware.com/kb/66767>.

---

Este capítulo inclui os seguintes tópicos:

- [Atualizar cada NSX Manager associado a um sistema vCenter Server anexado](#)
- [Atualizar sistemas vCenter Server, hosts ESXi e NSX Edges](#)

## Atualizar cada NSX Manager associado a um sistema vCenter Server anexado

Antes de atualizar um vCenter Server e hosts ESXi registrados no vCloud Director, você deve atualizar cada NSX Manager associado a esse vCenter Server.

Atualizar o NSX Manager interrompe o acesso às funções administrativas do NSX, mas não interrompe os serviços de rede. Você pode atualizar o NSX Manager antes ou depois de atualizar o vCloud Director, mesmo que as células do vCloud Director estejam em execução.

Para obter informações sobre como atualizar o NSX, consulte o NSX para a documentação do vSphere em <https://docs.vmware.com>.

### Procedimentos

- 1 Atualize o NSXGerenciador associado a cada vCenter Server registrado na sua instalação do vCloud Director.
- 2 Depois de ter atualizado todos os seus NSX Managers, você pode atualizar seus sistemas vCenter Server e hosts registrados do ESXi.

## Atualizar sistemas vCenter Server, hosts ESXi e NSX Edges


Depois de atualizar o vCloud Director e o NSX Manager, você deve atualizar os sistemas vCenter Server e os hosts ESXi que estão registrados no vCloud Director. Depois de atualizar todos os sistemas anexados vCenter Server e hosts ESXi, você poderá atualizar os NSX Edges.

### Pré-requisitos

Verifique se você já atualizou cada NSX Manager que está associado aos sistemas vCenter Server que estão conectados à sua nuvem. Consulte [Atualizar cada NSX Manager associado a um sistema vCenter Server anexado](#).

### Procedimentos


#### 1 Desative a instância do vCenter Server.

- a No menu principal () do vCloud Director Service Provider Admin Portal, selecione **Recursos do vSphere**.
- b No painel esquerdo, clique em **vCenters**.
- c Selecione o botão de opção ao lado do vCenter Server que você deseja desativar e clique em **Desativar**.
- d Clique em **OK**.


#### 2 Atualize o sistema do vCenter Server.

Para obter informações, consulte *Upgrade do vCenter Server*.

#### 3 Verifique todas as URLs públicas e cadeias de certificados do vCloud Director.

- a No menu principal () , selecione **Administração**.
- b No painel esquerdo, em **Configurações**, clique em **Endereços Públicos**.
- c Verifique todos os endereços públicos.

#### 4 Atualize o registro do vCenter Server com o vCloud Director.

- a No menu principal () do vCloud Director Service Provider Admin Portal, selecione **Recursos do vSphere**.
- b No painel esquerdo, clique em **vCenters**.
- c Selecione o botão de opção ao lado do vCenter Server de destino e clique em **Reconectar**.
- d Clique em **OK**.

- 5 Atualize cada host do ESXi para o qual o sistema do vCenter Server atualizado oferece suporte.

Consulte o *Upgrade do VMware ESXi*.

---

**Importante** Para garantir que você tenha capacidade de host atualizada o suficiente para oferecer suporte às máquinas virtuais na sua nuvem, atualize os hosts em pequenos lotes. Quando você faz isso, as atualizações de agentes de host podem ser concluídas em tempo para permitir que as máquinas virtuais migrem de volta para o host atualizado.

---

- a Use o sistema vCenter Server para colocar o host no modo de manutenção e permitir que todas as máquinas virtuais no host migrem para outro host.
  - b Atualize o host.
  - c Use o sistema vCenter Server para reconectar o host.
  - d Use o sistema vCenter Server para tirar o host do modo de manutenção.
- 6 (Opcional) Atualize os NSX Edges gerenciados pelo NSX Manager associado ao sistema vCenter Server atualizado.

NSX Edges atualizados fornecem melhorias no desempenho e na integração. Você pode usar o NSX Manager ou o vCloud Director para atualizar os NSX Edges.

- Para obter informações sobre como usar o NSX Manager para atualizar NSX Edges, consulte a documentação do NSX para vSphere em <https://docs.vmware.com>.
- Para usar o vCloud Director para fazer upgrade do edge gateway do NSX, você deve operar no objeto de rede do vCloud Director ao qual o Edge oferece suporte:
  - Um upgrade apropriado de um Edge Gateway ocorre automaticamente quando você usa o vCloud Director ou a API do vCloud para redefinir uma rede atendida pelo Edge Gateway.
  - A reimplantação de um Edge Gateway atualiza o dispositivo do NSX Edge associado.

---

**Observação** A reimplantação é suportada apenas para os Edge Gateways do NSX Data Center for vSphere.

---

- Redefinir uma rede vApp de dentro do contexto do vApp atualiza o dispositivo do NSX Edge associado a essa rede. Para redefinir uma rede vApp de dentro do contexto de um vApp, navegue até a guia **Redes** para o vApp, exiba os detalhes da rede, clique no botão de opção ao lado do nome da rede do vApp e clique em **Redefinir**.

Para obter mais informações sobre como reimplantar Edge Gateways e redefinir redes de vApp, consulte o *Guia de programação da API do vCloud*.

#### Próximo passo

Repita esse procedimento para os outros sistemas vCenter Server registrados na sua instalação do vCloud Director.



# Exibindo os logs do vCloud Director

# 15

O vCloud Director fornece informações de registro para cada célula de nuvem no sistema. Você pode exibir os logs para monitorar suas células e solucionar problemas.

Você pode encontrar os logs para uma célula em `/opt/vmware/vcloud-director/logs`. [Tabela 15-1. Logs do vCloud Director](#) lista os logs disponíveis.

**Tabela 15-1. Logs do vCloud Director**

Nome do log	Descrição
cell.log	Saída de console da célula do vCloud Director.
cell-management-tool	Mensagens do log de Ferramenta de gerenciamento de célula vindas da célula.
cell-runtime	Mensagens de log de tempo de execução da célula.
cloud-proxy	Mensagens de log de proxy de nuvem da célula.
console-proxy	Mensagens de log de proxy do console remoto da célula.
server-group-communications	Comunicações de grupo de servidor da célula.
statsfeeder	Recuperação de métrica de máquina virtual (do vCenter Server) e informações de armazenamento e mensagens de erro.
vcloud-container-debug.log	Mensagens de log da célula no nível de depuração.
vcloud-container-info.log	Mensagens de log informativas vindas da célula. Esse log também mostra avisos ou erros encontrados pela célula.
vmware-vcd-watchdog.log	Mensagens informativas de log vindas do watchdog da célula. Ele registra quando a célula entra em pane, é restaurada, etc.
diagnostics.log	Log de diagnósticos da célula. Esse arquivo permanece vazio a menos que os registros de diagnósticos estejam habilitados na configuração de registros local.
YYYY_MM_DD.request.log	Os logs de solicitação HTTP no formato de log comum do Apache.

Você pode usar qualquer editor de texto/visualizador ou ferramenta de terceiros para exibir os logs.

# Solucionando problemas com o appliance vCloud Director

# 16

Se a implantação do appliance vCloud Director falhar ou se o appliance não estiver funcionando corretamente, examine os arquivos de log do appliance para determinar a causa do problema.

O suporte técnico da VMware costuma solicitar informações de diagnóstico ao lidar com solicitações de suporte. Você pode usar o script `vmware-vcd-support` para coletar informações de log do host e logs do vCloud Director. Para obter mais informações sobre como coletar informações de diagnóstico para o vCloud Director, consulte <https://kb.vmware.com/s/article/1026312>. Ao executar o script `vmware-vcd-support`, os logs podem incluir informações sobre células descomissionadas ou substituídas com o status FAIL. Consulte <https://kb.vmware.com/s/article/71349>.

Este capítulo inclui os seguintes tópicos:

- [Examinar os arquivos de log no vCloud Director Appliance](#)
- [A célula do vCloud Director não é iniciada após a implantação do appliance](#)
- [A reconfiguração do serviço do vCloud Director falha ao migrar ou restaurar para o dispositivo vCloud Director](#)
- [Usando os arquivos de log para solucionar problemas de atualizações e patches do vCloud Director](#)
- [Falha na verificação de atualizações do vCloud Director](#)
- [Falha na instalação da atualização mais recente do vCloud Director](#)

## Examinar os arquivos de log no vCloud Director Appliance

Depois de implantar o vCloud DirectorAppliance, você poderá examinar os logs do arquivo Firstboot e do banco de dados em busca de erros e avisos.

### Procedimentos

- 1 Faça login diretamente ou conecte-se via SSH no console do dispositivo do vCloud Director como **root**.
- 2 Navegue até `/opt/vmware/var/log`.

### 3 Examine os arquivos de log.

- O arquivo `Firstboot` contém informações de log relacionadas à primeira inicialização do Appliance.
- O diretório `/opt/vmware/var/log/vcd/` contém os log relacionados à configuração e reconfiguração da suíte de ferramentas Replication Manager (repmgr) e à sincronização do dispositivo.
- O diretório `/opt/vmware/var/log/vcd/pg/` contém os logs relacionados ao backup do banco de dados do dispositivo incorporado.
- O arquivo `/opt/vmware/etc/vami/ovfEnv.xml` contém os parâmetros OVF de implantação.

## A célula do vCloud Director não é iniciada após a implantação do appliance

Você implantou o appliance vCloud Director com êxito, mas os serviços vCloud Director podem falhar ao serem iniciados.

### Problema

O serviço `vmware-vcd` fica inativo após a implantação do appliance.

### Causa

Se você tiver implantado uma célula primária, os serviços vCloud Director poderão falhar ao serem iniciados devido a um armazenamento de serviços de transferência compartilhado do NFS previamente preenchido. Antes de implantar o appliance primário, o armazenamento de serviços de transferência compartilhado não deve conter um arquivo `responses.properties` ou um diretório `appliance-nodes`.

Se você tiver implantado uma célula de aplicativo em espera ou vCD, os serviços vCloud Director poderão falhar ao serem iniciados devido a um arquivo `responses.properties` ausente no armazenamento de transferências compartilhado NFS. Antes de implantar um appliance de aplicativo em espera ou vCD, o armazenamento de serviços de transferência compartilhado deve conter o arquivo `responses.properties`.

### Solução

- 1 Faça login diretamente ou conecte-se via SSH no console do dispositivo do vCloud Director como **root**.
- 2 Examine `/opt/vmware/var/log/vcd/setupvcd.log` em busca de mensagens de erro sobre o armazenamento NFS.
- 3 Prepare o armazenamento NFS para o tipo de appliance.
- 4 Reimplante a célula.

## A reconfiguração do serviço do vCloud Director falha ao migrar ou restaurar para o dispositivo vCloud Director

Quando você está migrando ou restaurando para o dispositivo do vCloud Director, a execução do comando `configure` pode falhar.

### Problema

Durante o procedimento para migrar ou restaurar o vCloud Director para um novo ambiente de dispositivo do vCloud Director, execute o comando `configure` para reconfigurar o serviço vCloud Director em cada nova célula. O comando `configure` pode falhar com a mensagem de erro `sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: falha na verificação de assinatura`.

### Solução

- 1 Na célula de destino, execute o comando.

```
sed -i '/vcd_ova.crt/ s/$/ --force /' /opt/vmware/appliance/bin/appliance-sync.sh
```

- 2 Aguarde um minuto e execute novamente o comando `configure`.

## Usando os arquivos de log para solucionar problemas de atualizações e patches do vCloud Director

Você pode examinar os arquivos de log em busca de erros e avisos ao aplicar patches ao dispositivo vCloud Director.

### Problema

Se o comando `vamicli` retornar um erro, você poderá usar os arquivos de log para solucionar o problema.

### Solução

- 1 Faça login diretamente ou conecte-se via SSH no console do dispositivo do vCloud Director como **root**.
- 2 Navegue até o arquivo de log apropriado.
  - Se `vamicli update --check` falhar, navegue até `/opt/VMware/var/log/vami/vami.log`.
  - Se houver falha no `vamicli update --install latest`, navegue até `/opt/VMware/var/log/vami/updatecli.log`.
- 3 Examine o arquivo de log.

## Falha na verificação de atualizações do vCloud Director

Quando você verifica se há atualizações no dispositivo vCloud Director, a execução do comando `vamicli update --check` pode falhar.

### Problema

Durante o procedimento de aplicação de um patch ao dispositivo vCloud Director, você executa o comando `vamicli update --check` para verificar se há atualizações disponíveis. O comando `vamicli update --check` pode falhar com Falha: erro ao baixar o manifesto. Entre em contato com seu fornecedor.

### Causa

O caminho para o diretório do repositório de atualização está incorreto.

### Solução

- 1 Execute o comando `vamicli` com o caminho correto.

```
vamicli update --repo file:/root/local-update-repo
```

- 2 Execute novamente o comando para verificar se há atualizações.

```
vamicli update --check
```

## Falha na instalação da atualização mais recente do vCloud Director

Quando você estiver instalando as atualizações mais recentes do dispositivo vCloud Director, a execução do comando `vamicli update --install latest` poderá falhar.

### Problema

Durante o procedimento de aplicação de um patch ao dispositivo vCloud Director, você executa o comando `vamicli update --install latest` para aplicar o patch mais recente disponível. O comando `vamicli update --install latest` pode falhar com Falha: erro ao executar a instalação do pacote

### Causa

O erro ocorre quando o servidor NFS está inacessível.

### Solução

- 1 Verifique se o servidor NFS montado em `/opt/vmware/vcloud-director/data/transfer` está acessível.

- 2 Execute novamente o comando para aplicar o patch disponível.

```
vamicli update --install latest
```

# Desinstalar o software vCloud Director

# 17

Use o comando Linux `rpm` para desinstalar o software vCloud Director de um servidor individual.

## Procedimentos

- 1 Faça login no servidor de destino como **raiz**.
- 2 Desmonte o armazenamento de serviços de transferência, normalmente montado em `/opt/vmware/vcloud-director/data/transfer`.
- 3 Abra uma janela de console, shell ou terminal e execute o comando Linux `rpm`.

```
rpm -e vmware-phonehome vmware-vcloud-director vmware-vcloud-director-rhel
```

Se outros pacotes instalados dependerem do pacote `vmware-vcloud-director`, o sistema solicitará que você desinstale esses pacotes antes de desinstalar o vCloud Director.