

Guia de instalação, configuração e upgrade do VMware Cloud Director

Modificado em 8 de abril de 2021
VMware Cloud Director 10.2

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

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

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

Copyright © 2010-2021 VMware, Inc. Todos os direitos reservados. [Informações sobre direitos autorais e marca registrada.](#)

Conteúdo

Guia de instalação, configuração e upgrade do VMware Cloud Director™ 7

1 Arquitetura do VMware Cloud Director 8

2 Requisitos de hardware e software do VMware Cloud Director 11

Requisitos de configuração de rede para o VMware Cloud Director 12

Requisitos de segurança de rede 14

3 Implantação, upgrade e administração do dispositivo do VMware Cloud Director 16

Implantações de dispositivo e configuração de alta disponibilidade do banco de dados 16

Failover automático do dispositivo do VMware Cloud Director 20

Isolamento automático de uma célula primária com falha 22

Preparando a implantação do dispositivo do VMware Cloud Director 23

Preparando o armazenamento do servidor de transferência para o dispositivo do VMware Cloud Director 23

Instalar e configurar o NSX Data Center for vSphere para o VMware Cloud Director 25

Instalar e configurar o NSX-T Data Center para o VMware Cloud Director 26

Implantação e configuração inicial do dispositivo do VMware Cloud Director 28

Diretrizes de dimensionamento de dispositivos do VMware Cloud Director 30

Pré-requisitos para a implantação do appliance do VMware Cloud Director 35

Implantar o dispositivo do VMware Cloud Director usando o vSphere Client 36

Implantação do dispositivo VMware Cloud Director usando o VMware OVF Tool 43

Implantar o dispositivo VMware Cloud Director com certificados curinga assinados para comunicação HTTPS e via proxy de console 53

Criar e importar certificados SSL assinados pela autoridade de certificação para o dispositivo do VMware Cloud Director 55

Importar chaves privadas e certificados SSL assinados pela autoridade de certificação para o dispositivo do VMware Cloud Director 59

Depois de implantar o dispositivo do VMware Cloud Director 60

Alterar a senha raiz do dispositivo do VMware Cloud Director 66

Fazendo upgrade e migrando o dispositivo do VMware Cloud Director 68

Fazer upgrade do dispositivo do VMware Cloud Director usando um pacote de atualização 71

Fazer upgrade do dispositivo do VMware Cloud Director usando o Repositório de Atualização da VMware 73

Reverter um dispositivo do VMware Cloud Director quando um upgrade falhar 76

Migrando o VMware Cloud Director com um banco de dados PostgreSQL externo para o dispositivo do VMware Cloud Director 77

Depois de fazer upgrade do VMware Cloud Director 82

Atualizar cada NSX Manager associado a um sistema vCenter Server anexado	83
Atualizar sistemas vCenter Server, hosts ESXi e NSX Edges	83
Administração do dispositivo do VMware Cloud Director	85
Fazer backup e restaurar o banco de dados incorporado do dispositivo do VMware Cloud Director	86
Alterando o modo de failover do dispositivo do VMware Cloud Director	94
Configurar o acesso externo ao banco de dados do VMware Cloud Director	94
Ativar ou desativar o acesso do SSH ao dispositivo do VMware Cloud Director	95
Ativar ou desativar o modo FIPS no dispositivo VMware Cloud Director	96
Configurando o agente SNMP do dispositivo VMware Cloud Director	99
Editando as configurações de DNS do dispositivo do VMware Cloud Director	105
Editar as rotas estáticas para as interfaces de rede do dispositivo do VMware Cloud Director	106
Scripts de configuração no dispositivo do VMware Cloud Director	108
Renovar os certificados do dispositivo VMware Cloud Director	108
Substituir um certificado de interface de usuário de gerenciamento do dispositivo VMware Cloud Director e PostgreSQL incorporado autoassinado	110
Substituir o armazenamento do servidor de transferência para o dispositivo do VMware Cloud Director	111
Aumentar a capacidade do banco de dados PostgreSQL incorporado em um dispositivo do VMware Cloud Director	112
Modificar as configurações do PostgreSQL no dispositivo do VMware Cloud Director	113
Cancelar o registro de uma célula em espera em execução em um cluster de alta disponibilidade de banco de dados	114
Alternar as funções da célula primária e de uma célula em espera em um cluster de alta disponibilidade de banco de dados	115
Assinar eventos, tarefas e métricas usando um cliente MQTT	117
Grupos de Dimensionamento Automático	118
Monitorando a integridade do cluster do banco de dados do dispositivo do VMware Cloud Director	120
Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director	120
Exibir o status do serviço do dispositivo do VMware Cloud Director	123
Verificar o status de conectividade de um cluster de alta disponibilidade de banco de dados	123
Verificar o status de replicação de um nó em um cluster de alta disponibilidade de banco de dados	124
Verificar o status dos serviços do VMware Cloud Director	126
Recuperação de clusters de banco de dados de dispositivo do VMware Cloud Director	126
Recuperar de uma falha de célula primária em um cluster de alta disponibilidade	128
Recuperar de uma falha de célula em espera em um cluster de alta disponibilidade	130
Cancelar o registro de uma célula primária ou em espera com falha em um cluster de alta disponibilidade de banco de dados	131
Solucionando problemas do dispositivo	132
Examinar os arquivos de log no VMware Cloud Director Appliance	132

A célula do VMware Cloud Director não é iniciada após a implantação do dispositivo	132
Recuperando após a validação do NFS falhar durante a configuração inicial do dispositivo	133
A reconfiguração do serviço do VMware Cloud Director falha ao migrar ou restaurar para o dispositivo VMware Cloud Director	138
Um nó em espera de dispositivo do VMware Cloud Director torna-se inacessível	138
Um nó em espera de dispositivo do VMware Cloud Director torna-se desconectado	141
A integridade do cluster indica um problema de SSH	143
Usando os arquivos de log para solucionar problemas de atualizações e patches do VMware Cloud Director	147
Falha na verificação de atualizações do VMware Cloud Director	148
Falha na instalação da atualização mais recente do VMware Cloud Director	148
4 Instalação, upgrade e administração do VMware Cloud Director no Linux	150
Planejamento de configuração	150
Preparando para a instalação do VMware Cloud Director	151
Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux	151
Preparando o armazenamento do servidor de transferência para o VMware Cloud Director no Linux	153
Baixe e instale a chave pública da VMware	155
Instalar e configurar o NSX Data Center for vSphere para o VMware Cloud Director	156
Instalar e configurar o NSX-T Data Center para o VMware Cloud Director	157
Instalar o VMware Cloud Director no Linux	158
Instalar o VMware Cloud Director no primeiro membro de um grupo de servidores	160
Criação e gerenciamento de certificados SSL para o VMware Cloud Director no Linux	162
Configurar as conexões de rede e banco de dados	169
Instalar o VMware Cloud Director em um membro adicional de um grupo de servidores	177
Depois de instalar o VMware Cloud Director	179
Personalizar endereços públicos para o VMware Cloud Director no Linux	180
Instalar e configurar um banco de dados Cassandra para armazenar dados de métricas de históricos	181
Realizar configurações adicionais no banco de dados PostgreSQL externo	183
Instalar e configurar um agente RabbitMQ AMQP	185
Assinar eventos, tarefas e métricas usando um cliente MQTT	186
Grupos de Dimensionamento Automático	187
Fazendo upgrade do VMware Cloud Director no Linux	189
Realizar uma atualização orquestrada de uma instalação do VMware Cloud Director	192
Atualizar manualmente uma instalação do VMware Cloud Director	195
Referência do utilitário de atualização de banco de dados	200
Depois de fazer upgrade do VMware Cloud Director	202
Atualizar cada NSX Manager associado a um sistema vCenter Server anexado	203
Atualizar sistemas vCenter Server, hosts ESXi e NSX Edges	204

5 Referência da ferramenta de gerenciamento de células 206

- Configurar uma instalação do VMware Cloud Director 210
- Desativar o acesso do provedor de serviços ao endpoint da API herdada 212
- Como gerenciar uma célula 213
- Como gerenciar aplicativos de célula 215
- Como atualizar as propriedades de conexão do banco de dados 217
- Detectar e reparar dados corrompidos do agendador 220
- Gerando certificados autoassinados para os endpoints de proxy do console e HTTPS 221
- Substituindo certificados para os endpoints de proxy de console e HTTPS 223
- Importação de certificados SSL de serviços externos 225
- Importar os certificados de endpoints dos recursos do vSphere 226
- Configurar uma lista de negação para conexão de teste 227
- Visualizar o status FIPS de todas as células ativas 228
- Gerenciamento da lista de codificações SSL permitidas 229
- Gerenciar a lista de protocolos SSL permitidos 233
- Configurar a coleção e a publicação de métricas 235
- Configuração de um banco de dados de métricas do Cassandra 238
- Recuperação da senha do administrador do sistema 240
- Atualizar o status de falha de uma tarefa 240
- Configurar o tratamento de mensagens de auditoria 241
- Configurando modelos de e-mail 243
- Encontrar VMs órfãs 247
- Entrar ou sair do Programa de aperfeiçoamento da experiência do cliente da VMware 249
- Atualização das definições de configuração do aplicativo 250
- Como configurar a limitação da sincronização de catálogo 251
- Solucionar problemas de falha no acesso à interface do usuário do VMware Cloud Director 253
- Depuração da detecção de VM do vCenter 254
- Como regenerar endereços MAC para redes estendidas multissite 255
- Atualizar os endereços IP do banco de dados em células do VMware Cloud Director 258

6 Coletar logs do VMware Cloud Director 260

7 Desinstalar o software VMware Cloud Director 262

Guia de instalação, configuração e upgrade do VMware Cloud Director™

O Guia de instalação, configuração e upgrade do VMware Cloud Director fornece informações sobre como instalar e fazer upgrade do software VMware Cloud Director™ e configurá-lo para funcionar com o VMware vSphere®, o VMware NSX® for vSphere® e o VMware NSX-T™ Data Center.

Público-alvo

O Guia de instalação, configuração e upgrade do VMware Cloud Director foi concebido para qualquer pessoa que queira instalar ou atualizar o software VMware Cloud 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.

Arquitetura do VMware Cloud Director

1

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

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

Para garantir a alta disponibilidade do VMware Cloud Director, você deve instalar pelo menos duas células do VMware Cloud 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 VMware Cloud Director a vários sistemas do VMware vCenter Server[®] e aos hosts VMware ESXi[™] que eles gerenciam. Para serviços de rede, o VMware Cloud Director pode usar o NSX Data Center for vSphere associado ao vCenter Server ou você pode registrar o NSX-T Data Center no VMware Cloud Director. NSX Data Center for vSphere e NSX-T Data Center mistos também são compatíveis.

Figura 1-1. Diagrama da arquitetura para instalação em Linux do VMware Cloud Director

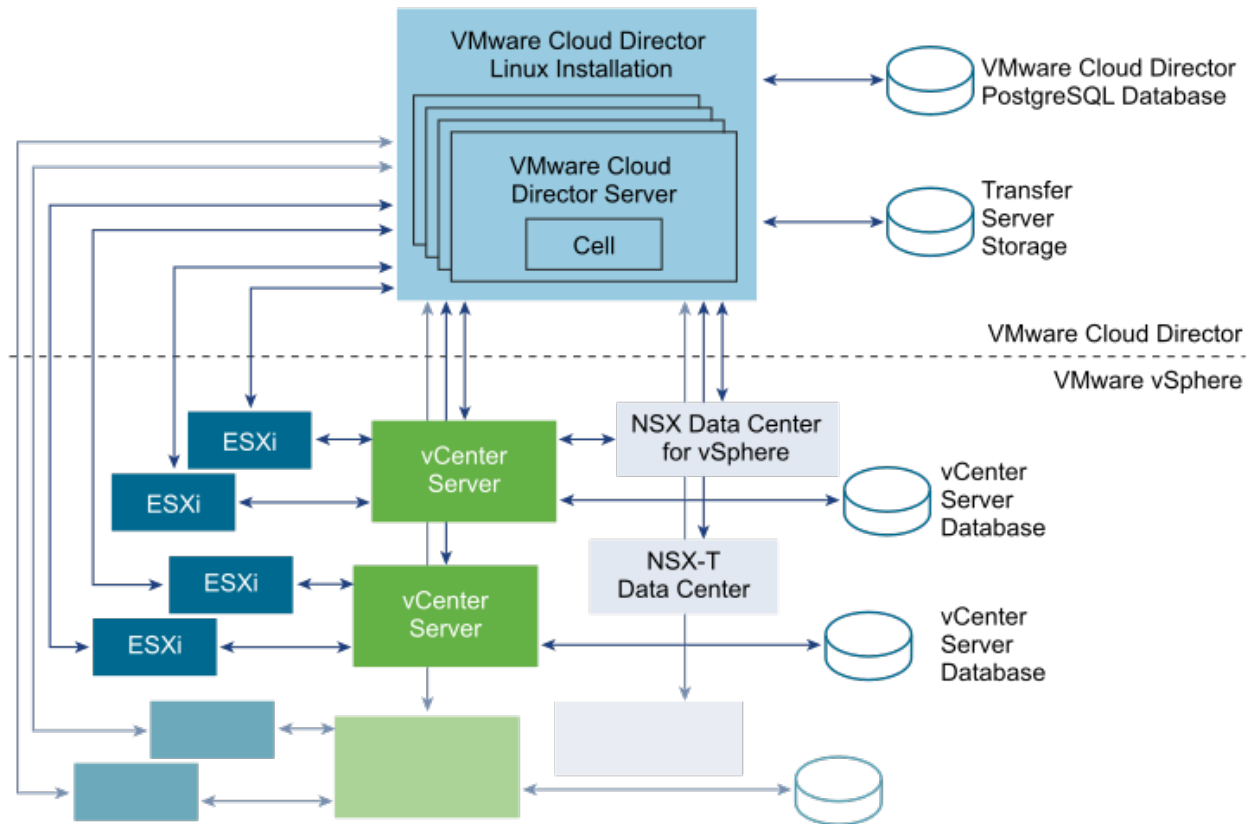
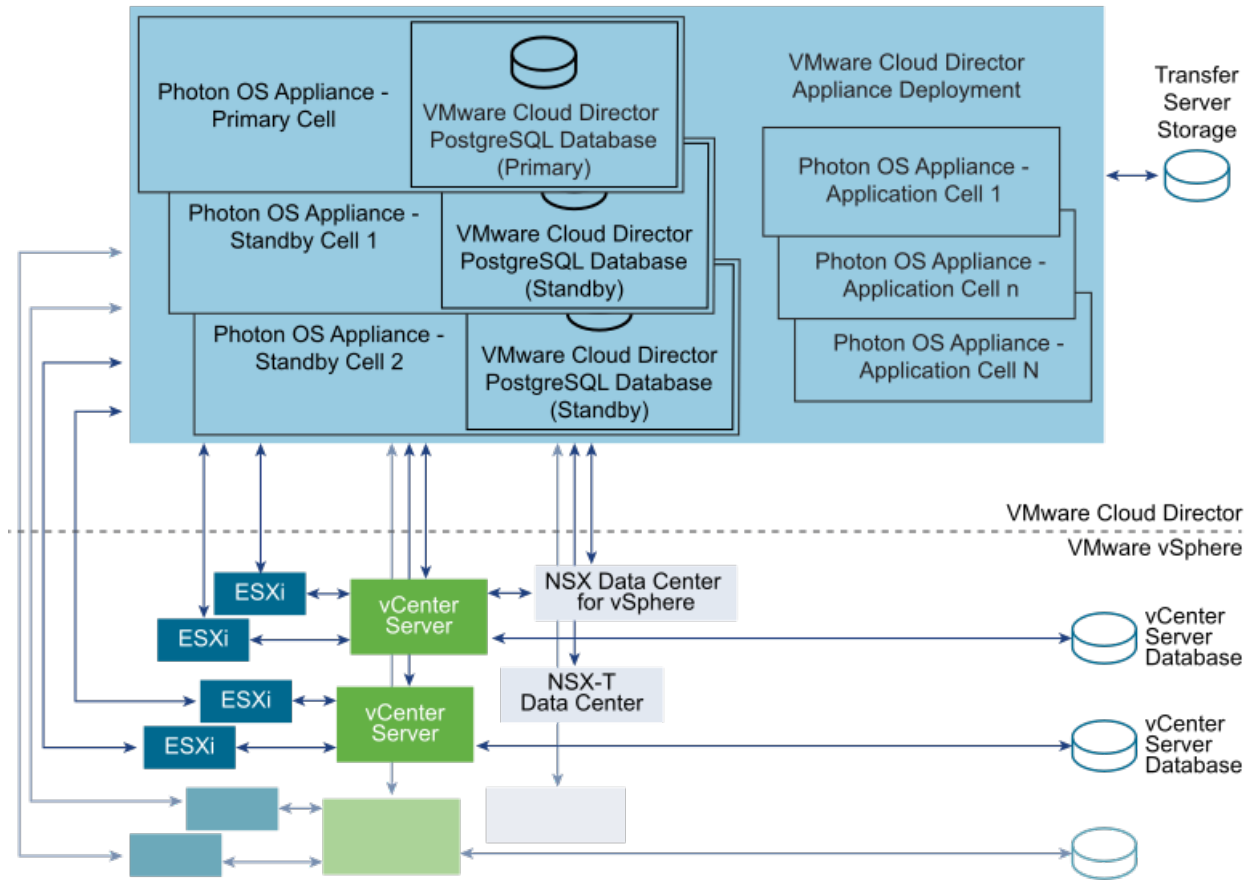


Figura 1-2. Diagrama da arquitetura do dispositivo do VMware Cloud Director



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

Um grupo de servidores VMware Cloud 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 VMware Cloud 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 1-3. Dispositivos do VMware Cloud Director que compõem um cluster de alta disponibilidade de banco de dados incorporado

O processo de instalação e configuração do VMware Cloud 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 VMware Cloud Director*.

Requisitos de hardware e software do VMware Cloud Director

2

Cada servidor em um grupo de servidores do VMware Cloud 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 VMware Cloud Director e outros produtos VMware, consulte as *Matrizes de interoperabilidade de produtos VMware* em 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 VMware Cloud Director devem atender a requisitos de configuração específicos.

- Redes do vCenter Server destinadas para uso como redes externas ou pools de rede do VMware Cloud Director devem estar disponíveis para todos os hosts em qualquer cluster destinado ao uso pelo VMware Cloud Director. Tornar essas redes disponíveis para todos os hosts em um datacenter simplifica a tarefa de adicionar novas instâncias vCenter Server a VMware Cloud 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 VMware Cloud 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 VMware Cloud 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*.

Plataformas, bancos de dados e navegadores com suporte

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

Requisitos de espaço em disco, memória e CPU

Para obter mais informações sobre espaço em disco, memória e requisitos de CPU, consulte [Diretrizes de dimensionamento de dispositivos do VMware Cloud Director](#).

Armazenamento compartilhado

O NFS ou outro volume de armazenamento compartilhado para o serviço de transferência do VMware Cloud 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 VMware Cloud Director](#)
- [Requisitos de segurança de rede](#)

Requisitos de configuração de rede para o VMware Cloud Director

A operação segura e confiável do VMware Cloud 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 VMware Cloud Director.

A rede que conecta os servidores do VMware Cloud 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 VMware Cloud Director deve oferecer suporte a dois endpoints SSL diferentes. Um endpoint é para o serviço HTTPS. 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director, incluindo o servidor de banco de dados. O desvio máximo permitido entre os relógios dos servidores sincronizados é de 2 segundos.

Para as implantações do dispositivo do VMware Cloud Director, o servidor NFS usado para o compartilhamento de transferência deve usar um serviço de tempo de rede, como o NTP, para sincronizar seu relógio com o dos dispositivos do VMware Cloud Director. O desvio máximo permitido entre os relógios dos servidores sincronizados é de 2 segundos.

Fusos horários do servidor

Todos os servidores do VMware Cloud Director, incluindo o servidor NFS usado para o compartilhamento de transferência e o servidor de banco de dados, devem estar configurados para ficar 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 VMware Cloud 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 VMware Cloud Director requer um ambiente de rede seguro. Configure e teste esse ambiente de rede antes de começar a instalação do VMware Cloud Director.

Conecte todos os servidores do VMware Cloud Director a uma rede que é protegida e monitorada.

Para obter informações sobre as portas de rede e os protocolos usados pelo VMware Cloud Director, consulte [Portas e protocolos da VMware](#).

As conexões de rede do VMware Cloud Director têm vários requisitos adicionais:

- Não conecte o VMware Cloud Director diretamente à Internet pública. Proteja sempre as conexões de rede do VMware Cloud 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.

Para obter informações sobre as portas que devem permitir pacotes de entrada de hosts do VMware Cloud Director, consulte [Portas e protocolos da VMware](#).

- Não conecte as portas usadas para conexões de saída à rede pública.
Para obter informações sobre as portas que devem permitir pacotes de saída de hosts do VMware Cloud Director, consulte [Portas e protocolos da VMware](#).
- A partir da versão 10.1, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger as conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos inacessíveis aos tenants que estejam usando a API do VMware Cloud Director para teste de conexão. Configure a lista de negação após a instalação ou o upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação de conexões de teste](#).
- Rotear o tráfego entre os servidores do VMware Cloud Director e os seguintes servidores em uma rede privada dedicada.
 - Servidor do banco de dados do VMware Cloud Director
 - RabbitMQ
 - Cassandra
- Se possível, rotear o tráfego entre os servidores do VMware Cloud 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 VMware Cloud Director estão disponíveis no artigo da Base de Conhecimento VMware [2086127](#).

Implantação, upgrade e administração do dispositivo do VMware Cloud Director

3

A partir da versão 9.7, o dispositivo do VMware Cloud Director inclui um banco de dados PostgreSQL incorporado com uma função de alta disponibilidade. Ao implantar, fazer upgrade ou migrar o dispositivo do VMware Cloud Director, você pode realizar operações de administração, monitoramento, correção ou solução de problemas.

Este capítulo inclui os seguintes tópicos:

- Implantações de dispositivo e configuração de alta disponibilidade do banco de dados
- Preparando a implantação do dispositivo do VMware Cloud Director
- Implantação e configuração inicial do dispositivo do VMware Cloud Director
- Fazendo upgrade e migrando o dispositivo do VMware Cloud Director
- Depois de fazer upgrade do VMware Cloud Director
- Administração do dispositivo do VMware Cloud Director
- Monitorando a integridade do cluster do banco de dados do dispositivo do VMware Cloud Director
- Recuperação de clusters de banco de dados de dispositivo do VMware Cloud Director
- Solucionando problemas do dispositivo

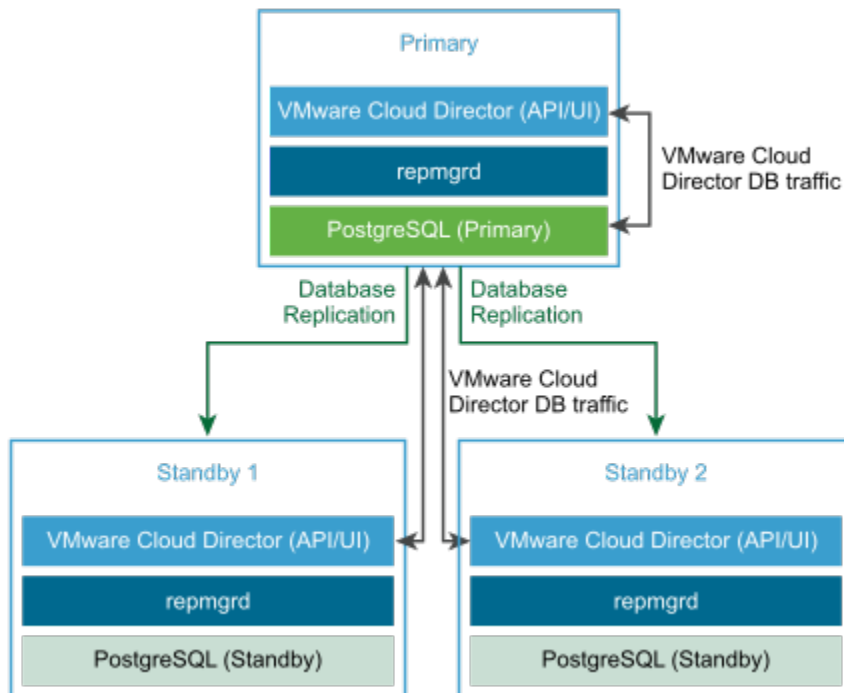
Implantações de dispositivo e configuração de alta disponibilidade do banco de dados

O dispositivo do VMware Cloud 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 VMware Cloud Director.

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

Para configurar o HA para o seu banco de dados do VMware Cloud 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 VMware Cloud Director. Você pode dimensionar horizontalmente o seu grupo de servidores implantando adicionalmente as células do aplicativo. Consulte a figura [Figura 3-1. Cluster de HA do banco de dados do dispositivo do VMware Cloud Director](#).

Figura 3-1. Cluster de HA do banco de dados do dispositivo do VMware Cloud Director



Criar uma implantação do dispositivo do VMware Cloud Director com o banco de dados de HA

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

1. Implante o dispositivo do VMware Cloud Director como uma célula primária.

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

- 2 Verifique se a célula primária está funcionando.
 - a Para verificar a integridade do serviço VMware Cloud Director, faça login com as credenciais do **administrador do sistema** para o VMware Cloud 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 VMware Cloud Director como células em espera.

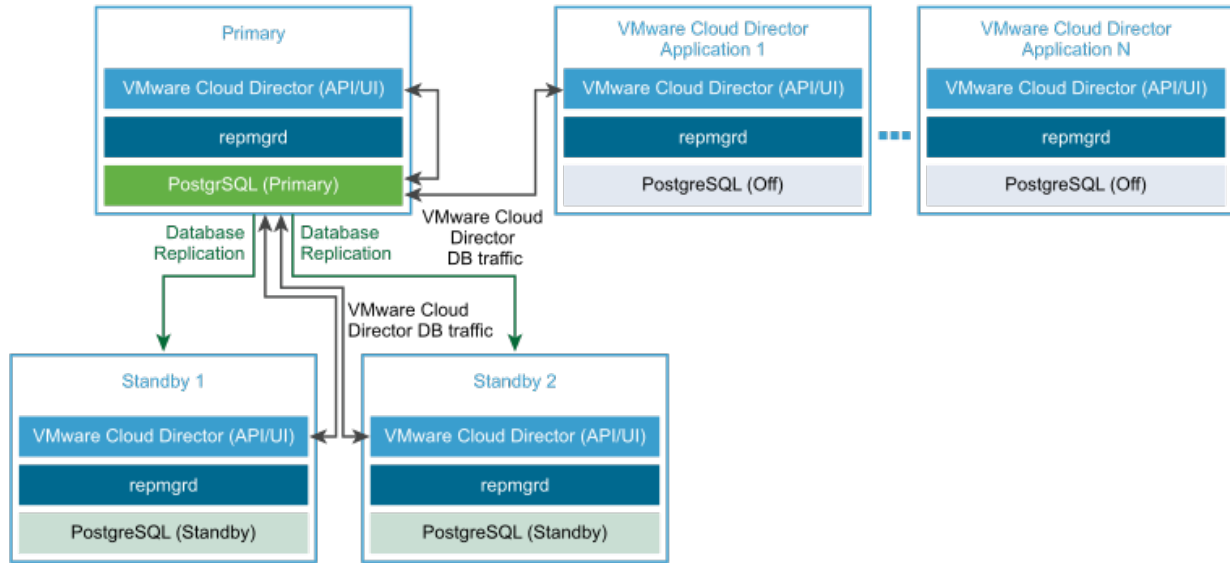
Os bancos de dados incorporados são configurados em modo de replicação com o banco de dados primário.

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 VMware Cloud Director e, portanto, a interface de usuário do VMware Cloud Director não estarão disponíveis.

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

Consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).
- 5 (Opcional) Implante uma ou mais instâncias do dispositivo do VMware Cloud Director como células do aplicativo VMware Cloud Director.

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



Observação Se o cluster estiver configurado para failover automático, depois de implantar uma ou mais células adicionais, você deverá usar a API do Dispositivo para redefinir o modo de failover do cluster para o *Automatic*. Consulte a [API do dispositivo do VMware Cloud Director](#). O modo de failover padrão para novas células é *Manual*. Se o modo de failover estiver inconsistente em todos os nós do cluster, o modo de failover do cluster será *Indeterminate*. O modo de *Indeterminate* pode levar a estados de clusters inconsistentes entre os nós e os nós seguindo uma célula primária antiga. Para exibir o modo de failover do cluster, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

Criar uma implantação de dispositivo do VMware Cloud Director sem o banco de dados de HA

Observação Você pode implantar um cluster VMware Cloud 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 VMware Cloud Director sem uma configuração de HA do banco de dados, siga este fluxo de trabalho:

1. Implante o dispositivo do VMware Cloud Director como uma célula primária.

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

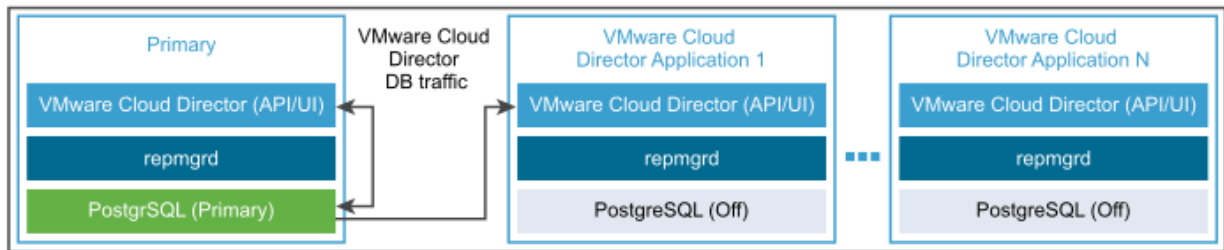
2 Verifique se a célula primária está funcionando.

- a Para verificar a integridade do serviço VMware Cloud Director, faça login com as credenciais do **administrador do sistema** para o VMware Cloud 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 VMware Cloud Director como células do aplicativo VMware Cloud Director.

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



Failover automático do dispositivo do VMware Cloud Director

A partir do VMware Cloud Director 10.1, se o serviço de banco de dados primário falhar, você poderá ativar o VMware Cloud Director para realizar um failover automático para um novo primário.

O failover automático elimina a necessidade de um administrador iniciar a ação de failover se o serviço de banco de dados primário falhar em executar suas funções por qualquer motivo. Por padrão, o modo de failover é definido como manual. Você pode definir o modo de failover como automático ou manual usando a API do dispositivo do VMware Cloud Director. Consulte o *Referência de esquemas de API do dispositivo do VMware Cloud Director*.

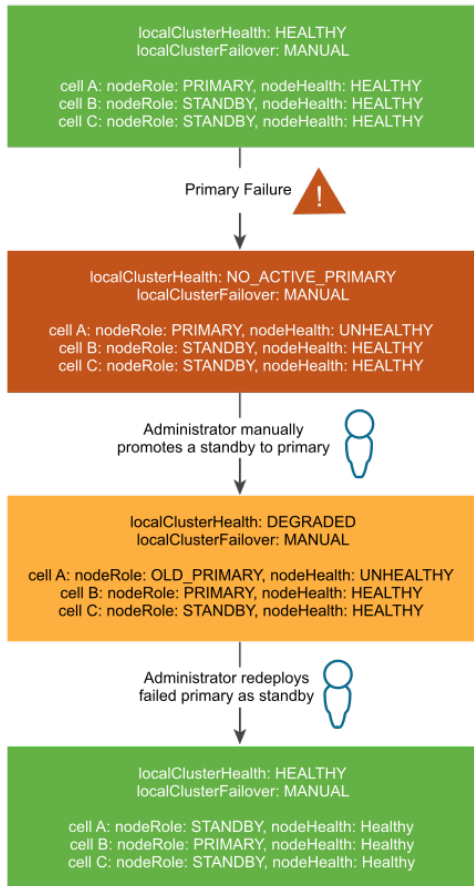
Observação Se o cluster estiver configurado para failover automático, depois de implantar uma ou mais células adicionais, você deverá usar a API do Dispositivo para redefinir o modo de failover do cluster para o `Automatic`. Consulte a [API do dispositivo do VMware Cloud Director](#). O modo de failover padrão para novas células é `Manual`. Se o modo de failover estiver inconsistente em todos os nós do cluster, o modo de failover do cluster será `Indeterminate`. O modo de `Indeterminate` pode levar a estados de clusters inconsistentes entre os nós e os nós seguindo uma célula primária antiga. Para exibir o modo de failover do cluster, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

Se o seu ambiente tiver pelo menos duas células em espera ativas, no caso de uma falha no banco de dados primário, um failover do banco de dados será iniciado automaticamente. Após o failover, deve haver pelo menos uma espera ativa para que o novo banco de dados primário seja atualizável. Em circunstâncias normais, sua implantação do dispositivo do VMware Cloud Director deve ter pelo menos duas esperas ativas em todos os momentos. Se houver apenas uma espera ativa por um curto período, por exemplo, devido à falha do primário e à promoção de uma das esperas, o primário com falha antigo deverá ser substituído por uma nova espera o mais rápido possível.

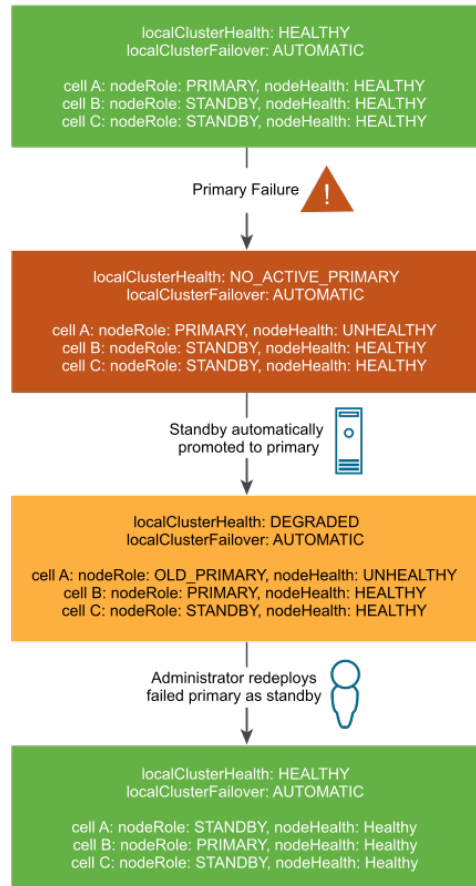
Quando há um primário ativo e pelo menos duas células em espera ativas, o cluster é considerado estar em um estado de `Healthy`. Se houver um primário ativo e apenas uma espera ativa, o cluster estará em um estado de `Degraded`. Se houver outra falha de banco de dados enquanto o cluster estiver em um estado de `Degraded`, o primário não será atualizável até que outra espera seja colocada online. Quando o banco de dados primário não é atualizável, o VMware Cloud Director não está disponível porque as células do VMware Cloud Director não conseguem atualizar o banco de dados até que haja pelo menos uma espera ativa para processar uma replicação de streaming do banco de dados primário. O conceito de um cluster de `Healthy` e `Degraded` é o mesmo que você ativa o failover manual ou automático.

Figura 3-2. Failover de dispositivo do VMware Cloud Director manual e automático

Manual VMware Cloud Director Appliance Failover



Automatic VMware Cloud Director Appliance Failover



Isolamento automático de uma célula primária com falha

Se uma nova célula primária for promovida após uma falha de célula primária, o VMware Cloud Director isola automaticamente a primária antiga para impedir que ela reinicie.

No caso de um failover, se um banco de dados primário com falha reiniciar após a promoção de uma nova célula primária, o VMware Cloud Director isola automaticamente a primária antiga. Essa automação evita a síndrome do cérebro dividido, em que dois bancos de dados ativos podem divergir um do outro. A automação de isolamento para e desativa o serviço vpostgres no antigo nó primário. Depois disso, você pode reimplantar o primário com falha como uma célula em espera para restaurar a integridade do cluster para `Healthy`.

Para obter mais informações sobre como exibir o status de integridade do cluster e o modo de failover, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

Preparando a implantação do dispositivo do VMware Cloud Director

Antes de implantar o dispositivo do VMware Cloud Director, você deve preparar o ambiente.

Preparando o armazenamento do servidor de transferência para o dispositivo do VMware Cloud Director

Você deve tornar um NFS ou outro volume de armazenamento compartilhado acessível para todos os servidores em um grupo de servidores do VMware Cloud Director. O VMware Cloud Director usa o armazenamento do servidor de transferência para o gerenciamento de cluster do dispositivo e o fornecimento de armazenamento temporário para carregamentos, downloads e itens de catálogo que são publicados ou assinados externamente.

Importante O dispositivo do VMware Cloud 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. O dispositivo do VMware Cloud Director também valida a maioria dos detalhes do compartilhamento NFS durante a implantação, incluindo permissões de diretório e propriedade. Você deve verificar se um ponto de montagem do NFS válido existe e se é acessível às instâncias do dispositivo do VMware Cloud Director.

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

- Durante transferências, uploads e downloads ocupam esse armazenamento. Quando a transferência termina, os uploads e downloads são removidos do armazenamento. As transferências que não fizeram 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.
- O VMware Cloud Director armazena os backups de banco de dados do dispositivo no diretório `pgdb-backup` no compartilhamento de transferência. Esses pacotes de backup podem consumir um espaço significativo.
- O coletor de pacotes de log de várias células ocupa esse espaço.

- Os dados dos nós do dispositivo e o arquivo `response.properties` ocupam esse espaço.

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

Observação O tempo de inatividade do NFS pode causar o funcionamento incorreto do cluster do dispositivo do VMware Cloud Director. A interface do usuário de gerenciamento do dispositivo não responde enquanto o NFS está desligado ou não pode ser acessado. Outras funcionalidades que podem ser afetadas são a exclusão de uma célula primária com falha, a alternância, a promoção de uma célula em espera e assim por diante.

Observação Quando você usa distribuições do Linux baseadas em Ubuntu ou Debian para o NFS, pode ocorrer uma falha na criação de backups de banco de dados.

Opções de armazenamento compartilhado

Um servidor NFS tradicional baseado em Linux ou outras soluções como o Microsoft Windows Server, o recurso NFS do VMware vSAN File Service e assim por diante podem fornecer o armazenamento compartilhado. A partir do vSAN 7.0, você pode usar a funcionalidade vSAN File Service para exportar compartilhamentos NFS usando os protocolos NFS 3.0 e NFS 4.1. Para obter mais informações sobre o vSAN File Service, consulte o guia *Administrando o VMware vSAN* na [Documentação do produto VMware vSphere](#).

Requisitos para a configuração do servidor NFS

Há requisitos específicos para a configuração do servidor NFS, para que o VMware Cloud 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 **raiz** pode realizar uma 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 VMware Cloud 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 VMware Cloud 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.

Exemplo de servidor NFS do Linux

Se o servidor NFS do Linux tiver um diretório chamado vCDspace como o espaço de transferência para o grupo de servidores do VMware Cloud Director com a localização `/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 três células denominadas vCD-Cell1-IP, vCD-Cell2-IP e vCD-Cell3-IP é `no_root_squash`. Você deve adicionar as seguintes linhas ao arquivo `/etc/exports`.

```
/nfs/vCDspace vCD_Cell1_IP_Address(rw, sync, no_subtree_check, no_root_squash)
/nfs/vCDspace vCD_Cell2_IP_Address(rw, sync, no_subtree_check, no_root_squash)
/nfs/vCDspace vCD_Cell3_IP_Address(rw, sync, no_subtree_check, no_root_squash)
```

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.

Para cada servidor no grupo de servidores do VMware Cloud Director, você deve ter uma entrada correspondente no arquivo `/etc/exports` do servidor NFS para que eles possam montar esse compartilhamento NFS. Depois de alterar o arquivo `/etc/exports` no servidor NFS, execute `exportfs -a` para exportar novamente todos os compartilhamentos NFS.

Instalar e configurar o NSX Data Center for vSphere para o VMware Cloud Director

Se você planeja a instalação do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director e outros produtos VMware, consulte as *Matrizes de interoperabilidade de produtos VMware* em 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 VMware Cloud Director](#).

Importante Esse procedimento é utilizado somente quando você está realizando uma nova instalação do VMware Cloud Director. Se você estiver atualizando uma instalação existente do VMware Cloud Director, consulte [Fazendo upgrade do VMware Cloud Director no Linux](#).

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 VMware Cloud Director na instalação do VMware Cloud Director planejada.
- 4 Configure o suporte VXLAN nas instâncias do NSX Manager associadas.

O VMware Cloud 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 VMware Cloud Director

Se você planeja que a instalação do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director](#).

Esse procedimento é utilizado somente quando você está realizando uma nova instalação do VMware Cloud Director. Se você estiver atualizando uma instalação existente do VMware Cloud Director, consulte [Fazendo upgrade do VMware Cloud Director no Linux](#).

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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director*.

Implantação e configuração inicial do dispositivo do VMware Cloud Director

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

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

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

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-9.7.0.0-9229800_OVA10.ova`.

O pacote do VMware Cloud DirectorAppliance contém os seguintes softwares:

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

Os tamanhos de dispositivo do VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud DirectorAppliance como uma célula primária e duas instâncias como células em espera. Você pode implantar instâncias adicionais do VMware Cloud DirectorAppliance no grupo de servidores como células do aplicativo vCD, que executam apenas o grupo de serviços do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director e PostgreSQL incorporado autoassinado](#).

Observação O VMware Cloud DirectorAppliance não é compatível com bancos de dados externos.

Configuração da rede do Appliance

A partir da versão 9.7, o VMware Cloud 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 <code>eth0</code>	Porta em <code>eth1</code>
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 VMware Cloud 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 VMware Cloud 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`.

A partir da versão 10.1, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos que não são acessíveis aos tenants que estão

usando a API do VMware Cloud Director para testes de conexão. Configure a lista de negação após a instalação ou o upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação para conexão de teste](#).

Diretrizes de dimensionamento de dispositivos do VMware Cloud Director

Dependendo das suas necessidades, você pode ter configurações diferentes do seu grupo de servidores com base no dispositivo do VMware Cloud Director e tamanhos diferentes das instâncias do dispositivo virtual do VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director	Não	Não	Sim
Ativação de métricas de VM do Cassandra no VMware Cloud 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 VMware Cloud 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 VMware Cloud 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

	Médio	Grande	Extragrande (VVD)
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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director para uma das configurações com suporte, depois de executar o implantador de dispositivo do VMware Cloud 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 VMware Cloud Director para uma configuração personalizada, depois de executar o implantador de dispositivo do VMware Cloud 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.

$$\text{shared_buffers} = 0,25 * (\text{total de RAM} - 4 \text{ GB})$$
- 5 Calcule o valor de `effective_cache_size` para ser três quartos da RAM total menos 4 GB.

$$\text{effective_cache_size} = 0,75 * (\text{total de RAM} - 4 \text{ GB})$$
- 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
```

Pré-requisitos para a implantação do appliance do VMware Cloud Director

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

- Verifique se você tem acesso ao arquivo `.ova` do VMware Cloud Director.
- Antes de implantar o appliance primário, prepare um armazenamento do serviço de transferência compartilhada NFS. Consulte [Preparando o armazenamento do servidor de transferência para o VMware Cloud Director no Linux](#).

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 VMware Cloud Director

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

Implantar o dispositivo do VMware Cloud Director usando o vSphere Client

Você pode implantar o dispositivo do VMware Cloud Director como um modelo OVF usando o vSphere Client (HTML5). Depois de implantar o modelo OVF, você deverá concluir a configuração na interface de usuário de gerenciamento de dispositivos.

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

Importante As instalações mistas do VMware Cloud Director no Linux e as implantações de appliance VMware Cloud 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 VMware OVF Tool. Consulte [Implantação do dispositivo VMware Cloud Director usando o VMware OVF Tool](#).

Observação Não há suporte para a implantação do VMware Cloud Director Appliance em VMware Cloud Director.

Pré-requisitos

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

Procedimentos

1 Iniciar a implantação do dispositivo do VMware Cloud Director

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

2 Configurar o dispositivo primário do VMware Cloud Director

Depois de implantar o Modelo OVF para o dispositivo primário, você deve continuar para a fase de configuração na interface de usuário de gerenciamento de dispositivos da instância primária do dispositivo do VMware Cloud Director.

3 Configurar as células de aplicativo e em espera do VMware Cloud Director

Depois de implantar o modelo OVF para uma célula de aplicativo ou em espera, você deve continuar para a fase de configuração na interface de usuário de gerenciamento de dispositivos da instância que deseja implantar.

Próximo passo

- Configure o endereço de proxy do console público, pois o VMware Cloud DirectorAppliance usa o NIC do seu `eth0` com a porta personalizada 8443 para o serviço de proxy do console. Consulte [Personalizar endereços públicos para o VMware Cloud Director no Linux](#).
- Para adicionar membros ao grupo de servidores do VMware Cloud Director, repita o procedimento.
- Para inserir a chave de licença, faça login no VMware Cloud 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 VMware Cloud Director no Linux](#).

Iniciar a implantação do dispositivo do VMware Cloud Director

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

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 VMware Cloud 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 VMware Cloud 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
Primária-pequena	<p>Implanta o dispositivo com 12 GB de RAM e 2 vCPUs como o primeiro membro em um grupo de servidores do VMware Cloud Director.</p> <p>O banco de dados incorporado na célula primária é configurado como o banco de dados do VMware Cloud Director. O nome do banco de dados é <code>vcloud</code> e o usuário do banco de dados é <code>vcloud</code>.</p>
Primária-grande	<ul style="list-style-type: none"> ■ O VMware Cloud Director 10.2.1 e versões posteriores implantam o dispositivo com 24 GB de RAM e 8 vCPUs como o primeiro membro de um grupo de servidores do VMware Cloud Director. ■ O VMware Cloud Director 10.2 implanta o dispositivo com 24 GB de RAM e 4 vCPUs como o primeiro membro de um grupo de servidores do VMware Cloud Director. <p>O banco de dados incorporado na célula primária é configurado como o banco de dados do VMware Cloud Director. O nome do banco de dados é <code>vcloud</code> e o usuário do banco de dados é <code>vcloud</code>.</p>
Em espera-pequena	<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 VMware Cloud 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>

Opção	Descrição
Em espera-grande	<p>Usado para ingressar em uma célula primária-grande em um cluster de alta disponibilidade do banco de dados.</p> <ul style="list-style-type: none"> ■ O VMware Cloud Director 10.2.1 e versões posteriores implantam o dispositivo com 24 GB de RAM e 8 vCPUs como o segundo ou o terceiro membro de um grupo de servidores do VMware Cloud Director com uma configuração de alta disponibilidade de banco de dados. ■ O VMware Cloud Director 10.2 implanta o dispositivo com 24 GB de RAM e 4 vCPUs como o segundo ou o terceiro membro de um grupo de servidores do VMware Cloud Director com uma configuração de alta disponibilidade de banco de dados. <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>
Aplicativo de célula do Cloud Director	<ul style="list-style-type: none"> ■ O VMware Cloud Director 10.2.1 e versões posteriores implantam o dispositivo com 8 GB de RAM e 4 vCPUs como um membro subsequente em um grupo de servidores do VMware Cloud Director. ■ O VMware Cloud Director 10.2 implanta o dispositivo com 8 GB de RAM e 2 vCPUs como um membro subsequente em um grupo de servidores do VMware Cloud Director. <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 VMware Cloud 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.

A lista de redes de origem pode estar em ordem inversa. Verifique se você está selecionando a rede de destino correta para cada rede de origem.

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 um protocolo **IPv4**.

- 11 Clique em **Avançar**.

Você será redirecionado para a página **Personalizar modelo** do assistente para configurar os detalhes do VMware Cloud Director.

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

Configuração	Descrição
Servidor NTP	O nome do host ou o endereço IP do servidor NTP a ser usado.
Senha raiz inicial	<p>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.</p> <p>Importante 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.</p> <p>Se quiser usar o modo FIPS, a senha raiz para o dispositivo deverá conter pelo menos 14 caracteres.</p> <p>Observação O assistente de implantação do OVF não valida a senha raiz inicial em relação aos critérios de senha.</p>
Expirar a senha raiz após o primeiro login	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.
Ativar login de raiz SSH	Desativado por padrão.

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

13 (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`.

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

Configuração	Descrição
Gateway Padrão	O endereço IP do gateway padrão para o dispositivo.
Nome de Domínio	O domínio de pesquisa DNS, por exemplo, <i>mydomain.com</i> .

Configuração	Descrição
Caminho de Pesquisa de Domínio	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> . Observação 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.
Servidores de Nome de Domínio	O endereço IP do servidor do nome de domínio para o dispositivo.
Endereço IP de rede eth0	O endereço IP para a interface <code>eth0</code> .
Máscara de rede eth0	A máscara de rede ou o prefixo da interface <code>eth0</code> .
Endereço IP de rede eth1	O endereço IP para a interface <code>eth1</code> .
Máscara de rede eth1	A máscara de rede ou o prefixo da interface <code>eth1</code> .

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

Próximo passo

- Ligue a máquina virtual recém-criada.
- [Configurar o dispositivo primário do VMware Cloud Director](#) ou [Configurar as células de aplicativo e em espera do VMware Cloud Director](#).

Configurar o dispositivo primário do VMware Cloud Director

Depois de implantar o Modelo OVF para o dispositivo primário, você deve continuar para a fase de configuração na interface de usuário de gerenciamento de dispositivos da instância primária do dispositivo do VMware Cloud Director.

Pré-requisitos

- [Iniciar a implantação do dispositivo do VMware Cloud Director](#).
- Ligue a máquina virtual recém-criada.
- Familiarize-se com o tópico [Preparando o armazenamento do servidor de transferência para o dispositivo do VMware Cloud Director](#).

Procedimentos

- Abra um navegador da Web e navegue até `https://Primary-Appliance-eth1-IP-Address:5480`.
- Faça login na interface de usuário de gerenciamento de dispositivos da instância primária do dispositivo.

A página **Configuração do Sistema do Dispositivo Primário** é exibida.

- 3 Na seção **Configurações do Dispositivo**, configure os detalhes do dispositivo e clique em **Avançar**.

Configuração	Descrição
Montagem do NFS para a localização do arquivo de transferência	A localização do armazenamento do servidor de transferência compartilhado NFS. O VMware Cloud Director valida a localização e exibirá uma marca de seleção verde se a montagem NFS for validada.
Senha de banco de dados para o usuário 'vcloud'	A senha para o usuário vcloud do banco de dados PostgreSQL.
Confirmar senha do banco de dados	Confirmação da senha para o usuário vcloud do banco de dados PostgreSQL.
Participar do Programa de Aperfeiçoamento da Experiência do Cliente	Ativa ou desativa a participação no Programa de aperfeiçoamento da experiência do cliente da VMware.

- 4 Na seção **Conta do Administrador**, configure os detalhes do administrador do sistema e clique em **Avançar**.

Configuração	Descrição
Nome de usuário	O nome de usuário para a conta do administrador do sistema . O padrão é <code>administrator</code> .
Senha	A senha para a conta do administrador do sistema . A senha deve ter entre 6 e 128 caracteres.
Confirmar Senha	Confirme a senha para a conta do administrador do sistema .
Nome completo	O nome completo do administrador do sistema . O padrão é <code>vCD Admin</code> .
Endereço de e-mail	O endereço de e-mail do administrador do sistema .

- 5 Na seção **Configurações do VMware Cloud Director**, configure a instalação dessa instância.

Configuração	Descrição
Nome do sistema	O nome da pasta do vCenter Server a criar para esta instalação do VMware Cloud Director.
ID de Instalação	A ID para esta instalação do VMware Cloud 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 VMware Cloud Director em implantações em vários sites, considere definir um ID exclusivo de instalação para cada instalação do VMware Cloud Director.

- 6 Clique em **Enviar** e, quando a configuração do sistema for concluída, clique em **OK**.

Resultados

Se a implantação for bem-sucedida, as guias **Disponibilidade do Banco de Dados Incorporado** e **Serviços** serão exibidas.

Próximo passo

- [Alterar o fuso horário do dispositivo do VMware Cloud Director](#)
- Implante uma célula de aplicativo ou em espera. Consulte [Iniciar a implantação do dispositivo do VMware Cloud Director](#).
- [Configurar as células de aplicativo e em espera do VMware Cloud Director](#)

Configurar as células de aplicativo e em espera do VMware Cloud Director

Depois de implantar o modelo OVF para uma célula de aplicativo ou em espera, você deve continuar para a fase de configuração na interface de usuário de gerenciamento de dispositivos da instância que deseja implantar.

Pré-requisitos

- 1 Implante uma célula de aplicativo ou em espera. Consulte [Iniciar a implantação do dispositivo do VMware Cloud Director](#).
- 2 Consulte [Preparando o armazenamento do servidor de transferência para o dispositivo do VMware Cloud Director](#).
- 3 Ligue a máquina virtual recém-criada.

Procedimentos

- 1 Abra um navegador da Web e navegue até `https://Cell-eth1-IP-Address:5480`.
- 2 Faça login na interface de usuário de gerenciamento de dispositivos da célula de aplicativo ou em espera.

A página **Configuração do Sistema** é exibida.
- 3 Insira a montagem NFS para a localização do arquivo de transferência.
- 4 Clique em **Enviar** e, quando a configuração do sistema for concluída, clique em **OK**.

Próximo passo

[Alterar o fuso horário do dispositivo do VMware Cloud Director](#)

Implantação do dispositivo VMware Cloud Director usando o VMware OVF Tool

Você pode implantar o VMware Cloud Director Appliance como um modelo OVF usando o VMware OVF Tool.

Você deve implantar o primeiro membro de um grupo de servidores do VMware Cloud Director como uma célula principal. É possível implantar um membro subsequente de um grupo de servidores do VMware Cloud Director como uma célula de aplicativo do VMware Cloud Director ou em espera. 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 VMware Cloud Director no Linux e as implantações de appliance VMware Cloud 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 VMware Cloud Director usando o vSphere Client](#).

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

A partir do VMware Cloud Director 10.2, você deve incluir o parâmetro `--X:enableHiddenProperties` para implantar o dispositivo do VMware Cloud Director.

Observação Você pode escolher se deseja especificar as opções de configuração do OVF opcionais durante a implantação do dispositivo primário ou se prefere executar a interface de usuário de gerenciamento de dispositivos para concluir a configuração após a implantação.

Opções de comando e propriedades do `ovftool` para implantar o VMware Cloud Director Appliance

Opção	Valor	Descrição
<code>--noSSLVerify</code>	N/A	Ignora a verificação de SSL para conexões vSphere.
<code>--acceptAllEulas</code>	N/A	Aceita todos os contratos de licença de usuário final (EULAs).
<code>--X:enableHiddenProperties</code>	N/A	Torna visíveis todas as propriedades para a configuração do dispositivo.
<code>--datastore</code>	<code>target_vc_datastore</code>	O nome do datastore de destino no qual os arquivos de configuração da máquina virtual e os discos virtuais são armazenados.

Opção	Valor	Descrição
<code>--allowAllExtraConfig</code>	N/A	Converte todas as opções de configuração extras no formato VMX.
<code>--net:"eth0 Network"</code>	<code>portgroup_on_vc_for_eth0</code>	A rede de destino para a rede <code>eth0</code> do Appliance. Importante Deve ser diferente da rede de destino do <code>eth1</code> .
<code>--net:"eth1 Network"</code>	<code>portgroup_on_vc_for_eth1</code>	A rede de destino para a rede <code>eth1</code> do Appliance. Importante Deve ser diferente da rede de destino do <code>eth0</code> .
<code>--name</code>	<code>vm_name_on_vc</code>	O nome da máquina virtual para o Appliance.
<code>--diskMode</code>	<code>thin</code> OU <code>thick</code>	O formato do disco para os arquivos de configuração da máquina virtual e os discos virtuais.
<code>--prop:"vami.ip0.VMware_vCloud_Director"</code>	<code>eth0_ip_address</code>	Endereço IP do <code>eth0</code> . 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.
<code>--prop:"vami.ip1.VMware_vCloud_Director"</code>	<code>eth1_ip_address</code>	Endereço IP do <code>eth1</code> . Usado para acessar serviços internos, incluindo o serviço de banco de dados PostgreSQL incorporado.
<code>--prop:"vami.DNS.VMware_vCloud_Director"</code>	<code>dns_ip_address</code>	O endereço IP do servidor do nome de domínio para o dispositivo.
<code>--prop:"vami.domain.VMware_vCloud_Director"</code>	<code>domain_name</code>	O domínio de pesquisa DNS. Aparece como o primeiro elemento no caminho de pesquisa.
<code>--prop:"vami.gateway.VMware_vCloud_Director"</code>	<code>gateway_ip_address</code>	O endereço IP do gateway padrão para o dispositivo.
<code>--prop:"vami.netmask0.VMware_vCloud_Director"</code>	<code>netmask0</code>	A máscara de rede ou o prefixo da interface <code>eth0</code> .
<code>--prop:"vami.netmask1.VMware_vCloud_Director"</code>	<code>netmask1</code>	A máscara de rede ou o prefixo da interface <code>eth1</code> .
<code>--prop:"vami.searchpath.VMware_vCloud_Director"</code>	<code>searchpath</code>	O caminho de pesquisa do domínio do dispositivo. Uma lista de nomes de domínio separados por vírgulas ou espaços.

Opção	Valor	Descrição
<code>--prop:"vcloudconf.ceip_enabled.VMware_vCloudDirector"</code>	<code>true</code> ou <code>false</code>	<p>Ativa ou desativa a participação no Programa de aperfeiçoamento da experiência do cliente da VMware. O padrão é verdadeiro.</p> <p>Opcional se você planeja executar a interface de usuário de gerenciamento de dispositivos para concluir a configuração do dispositivo primário após a implantação.</p>
<code>--prop:"vcloudapp.enable_ssh.VMware_vCloudDirector"</code>	<code>true</code> ou <code>false</code>	Ativa ou desativa o acesso raiz do SSH ao dispositivo.
<code>--prop:"vcloudapp.expire_root_password.VMware_vCloudDirector"</code>	<code>true</code> ou <code>false</code>	Determina se deve-se continuar ou não o uso da senha inicial após o primeiro login.
<code>--prop:"vcloudapp.nfs_mount.VMware_vCloudDirector":nfs_mount_path</code>	<code>host_ip_address:nfs_mount_path</code>	<p>O endereço IP e o caminho de exportação do servidor NFS externo. Usado somente para uma célula primária.</p>
<code>--prop:"vcloudapp.ntp-server.VMware_vCloudDirector":ntp_server_address</code>	<code>ntp_server_address</code>	O endereço IP do servidor de horário.
<code>--prop:"vcloudapp.varoot-password.VMware_vCloudDirector"</code>	<code>varoot_password</code>	<p>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.</p> <p>Importante 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.</p>
<code>--prop:"vcloudconf.db_pwd.VMware_vCloudDirector":db_password</code>	<code>db_password</code>	<p>A senha do banco de dados do usuário do vcloud.</p> <p>Usado somente para uma célula primária.</p> <p>Opcional se você planeja executar a interface de usuário de gerenciamento de dispositivos para concluir a configuração do dispositivo primário após a implantação.</p>

Opção	Valor	Descrição
<code>--prop:"vcloudconf.admin_email.VMware_vCloud_Director"address</code>	<code>vcl_admin_email</code>	<p>O endereço de email da conta do administrador do sistema.</p> <p>Usado somente para uma célula primária.</p> <p>Opcional se você planeja executar a interface de usuário de gerenciamento de dispositivos para concluir a configuração do dispositivo primário após a implantação.</p>
<code>--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"</code>	<code>vcl_admin_fname</code>	<p>O nome da conta do administrador do sistema.</p> <p>Usado somente para uma célula primária.</p> <p>Opcional se você planeja executar a interface de usuário de gerenciamento de dispositivos para concluir a configuração do dispositivo primário após a implantação.</p>
<code>--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"password</code>	<code>vcl_admin_pwd</code>	<p>A senha para a conta do administrador do sistema.</p> <p>Usado somente para uma célula primária.</p> <p>Opcional se você planeja executar a interface de usuário de gerenciamento de dispositivos para concluir a configuração do dispositivo primário após a implantação.</p>
<code>--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"username</code>	<code>vcl_admin_uname</code>	<p>O nome de usuário para a conta do administrador do sistema.</p> <p>Usado somente para uma célula primária.</p> <p>Opcional se você planeja executar a interface de usuário de gerenciamento de dispositivos para concluir a configuração do dispositivo primário após a implantação.</p>
<code>--prop:"vcloudconf.inst_id.VMware_vCloud_Director"ID</code>	<code>vcl_inst_id</code>	<p>A ID de instalação do VMware Cloud Director.</p> <p>Usado somente para uma célula primária.</p> <p>Opcional se você planeja executar a interface de usuário de gerenciamento de dispositivos para concluir a configuração do dispositivo primário após a implantação.</p>

Opção	Valor	Descrição
<code>--prop:"vcloudconf.sys_name.VMware_vCloudSystemName"</code>	<code>ip_address1</code>	O nome da pasta do vCenter Server a criar para esta instalação do VMware Cloud Director. Opcional se você planeja executar a interface de usuário de gerenciamento de dispositivos para concluir a configuração do dispositivo primário após a implantação.
<code>--prop:"vcloudnet.routes0.VMware_vCloudNetwork" cidr, ip_address2, ...</code>	<code>ip_address1</code>	Opcional. Rotas estáticas para a interface do <code>eth0</code> . 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, 172.16.100.253 172.16.100/19, 172.16.200.253.
<code>--prop:"vcloudnet.routes1.VMware_vCloudNetwork" cidr, ip_address2, ...</code>	<code>ip_address1</code>	Opcional. Rotas estáticas para a interface do <code>eth1</code> . 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, 172.16.100.253 172.16.100/19, 172.16.200.253.

Opção	Valor	Descrição
<code>--deploymentOption</code>	<code>primary-small,primary-large,standby-small, standby-large</code> ou <code>cell</code>	<p>O tipo e o tamanho do dispositivo que você deseja implantar.</p> <p>Os tamanhos de dispositivo do VMware Cloud 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.</p> <ul style="list-style-type: none"> ■ O <code>primary-small</code> implanta o dispositivo com 12 GB de RAM e 2 vCPUs como o primeiro membro de um grupo de servidores do VMware Cloud Director. O banco de dados incorporado na célula primária é configurado como o banco de dados do VMware Cloud Director. O nome do banco de dados é <code>vcloud</code> e o usuário do banco de dados é <code>vcloud</code>. ■ <code>primary-large</code>: <ul style="list-style-type: none"> ■ O VMware Cloud Director 10.2.1 e versões posteriores implantam o dispositivo com 24 GB de RAM e 8 vCPUs como o primeiro membro de um grupo de servidores do VMware Cloud Director. ■ O VMware Cloud Director 10.2 implanta o dispositivo com 24 GB de RAM e 4 vCPUs como o primeiro membro de um grupo de servidores do VMware Cloud Director. <p>O banco de dados incorporado na célula primária é configurado como o banco de dados do VMware Cloud Director. O nome do banco de dados é <code>vcloud</code> e o usuário do banco de dados é <code>vcloud</code>.</p> ■ O <code>standby-small</code> implanta o dispositivo com 12 GB de RAM e 2 vCPUs como o segundo ou o terceiro membro de um grupo de servidores do VMware Cloud Director com uma configuração de alta disponibilidade de banco

Opção	Valor	Descrição
		<p>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"> ■ <code>standby-large:</code> <ul style="list-style-type: none"> ■ O VMware Cloud Director 10.2.1 e versões posteriores implantam o dispositivo com 24 GB de RAM e 8 vCPUs como o segundo ou o terceiro membro de um grupo de servidores do VMware Cloud Director com uma configuração de alta disponibilidade de banco de dados. ■ O VMware Cloud Director 10.2 implanta o dispositivo com 24 GB de RAM e 4 vCPUs como o segundo ou o terceiro membro de um grupo de servidores do VMware Cloud Director com uma configuração de alta disponibilidade de banco de dados. <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> <ul style="list-style-type: none"> ■ <code>cell:</code> <ul style="list-style-type: none"> ■ O VMware Cloud Director 10.2.1 e versões posteriores implantam o dispositivo com 8 GB de RAM e 4 vCPUs como um membro subsequente em um grupo de servidores do VMware Cloud Director. ■ O VMware Cloud Director 10.2 implanta o dispositivo com 8 GB de RAM e 2 vCPUs como um membro subsequente em um grupo de servidores do VMware Cloud Director.

Opção	Valor	Descrição
		<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> <hr/> <p>Importante As células primária e em espera em um grupo de servidores do VMware Cloud 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>
--powerOn	<i>path_to_ova</i>	Liga a máquina virtual após a implantação.

Exemplo de comando para a implantação de um dispositivo primário de produção do VMware Cloud Director

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 \
--X:enableHiddenProperties \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thick \
--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-large" \
--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
```

Exemplo de comando para a implantação de um dispositivo em espera de produção do VMware Cloud Director

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 \
--X:enableHiddenProperties \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thick \
--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-large" \
--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
```

Depois de implantar o dispositivo VMware Cloud Director

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

Use a interface de usuário de gerenciamento de dispositivos para configurar o dispositivo primário. Consulte [Configurar o dispositivo primário do VMware Cloud Director](#).

Use a interface de usuário de gerenciamento de dispositivos para configurar as células do aplicativo e em espera. Consulte [Configurar as células de aplicativo e em espera do VMware Cloud Director](#).

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

Você pode implantar o dispositivo VMware Cloud 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 VMware Cloud Director, o VMware Cloud Director gera certificados autoassinados e os utiliza para configurar a célula do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director](#).

Se os certificados assinados que você usar no dispositivo primário VMware Cloud Director forem certificados curinga assinados, eles poderão ser aplicados a todos os outros dispositivos no grupo de servidores do VMware Cloud Director, ou seja, células em espera e células de aplicativo do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director](#).
- Se o tipo do armazenamento de chaves que contém os certificados SSL curinga assinados for JCEKS, verifique se a senha privada das chaves nesse 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.

```
/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 VMware Cloud 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.

- 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
```

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

No dispositivo do VMware Cloud 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 VMware Cloud Director](#).

Importante Na implantação, o dispositivo do VMware Cloud 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_password*.

Pré-requisitos

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

Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH no console do dispositivo do VMware Cloud Director como **root**.

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

Quando você implanta o dispositivo do VMware Cloud Director, o VMware Cloud 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 5](#).
- Se você quiser gerar novos certificados com opções personalizadas, como um tamanho de chave maior, vá para a [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 VMware Cloud 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 VMware Cloud 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 PKCS12 -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 PKCS12 -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 VMware Cloud Director.
- 8 Execute os comandos para importar os certificados assinados para o armazenamento de chaves PKCS12.

- 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 PKCS12 -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 PKCS12 -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 PKCS12 -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 PKCS12 -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 PKCS12 -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -list
```

- 10 Execute o comando para importar os certificados para a instância do VMware Cloud 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 VMware Cloud Director no dispositivo do `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
```

Próximo passo

- Se você estiver usando certificados curinga, consulte [Implantar o dispositivo VMware Cloud 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 VMware Cloud 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 VMware Cloud Director, consulte [Substituir um certificado de interface de usuário de gerenciamento do dispositivo VMware Cloud Director e PostgreSQL incorporado autoassinado](#).

Importar chaves privadas e certificados SSL assinados pela autoridade de certificação para o dispositivo do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. O VMware Cloud 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 usando um cliente SSH no console do dispositivo do VMware Cloud 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 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.p12 -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.p12 -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 `certificates.ks`.

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

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/vcloud-director/certificates.ks -deststoretype PKCS12 -srckeystore http.p12 -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 PKCS12 -srckeystore consoleproxy.p12 -srcstoretype PKCS12 -srcstorepass keystore_password
```

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

```
keytool -storetype PKCS12 -storepass keystore_password -keystore /opt/vmware/vcloud-director/certificates.ks -list
```

- 7 Execute o comando para importar os certificados assinados para a instância do VMware Cloud 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 VMware Cloud Director no dispositivo do `vmware-vcd`.

```
service vmware-vcd restart
```

Próximo passo

- Se você estiver usando certificados curinga, consulte [Implantar o dispositivo VMware Cloud 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 VMware Cloud 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 VMware Cloud Director, consulte [Substituir um certificado de interface de usuário de gerenciamento do dispositivo VMware Cloud Director e PostgreSQL incorporado autoassinado](#).

Depois de implantar o dispositivo do VMware Cloud Director

Depois de criar o grupo de servidores do VMware Cloud Director, você poderá instalar os arquivos de Sysprep da Microsoft e o banco de dados Cassandra. Se estiver usando um banco de dados do PostgreSQL, você poderá configurar o SSL e ajustar alguns parâmetros no banco de dados.

Após a criação do dispositivo do VMware Cloud 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*.

Observação Se o cluster estiver configurado para failover automático, depois de implantar uma ou mais células adicionais, você deverá usar a API do Dispositivo para redefinir o modo de failover do cluster para o `Automatic`. Consulte a [API do dispositivo do VMware Cloud Director](#). O modo de failover padrão para novas células é `Manual`. Se o modo de failover estiver inconsistente em todos os nós do cluster, o modo de failover do cluster será `Indeterminate`. O modo de `Indeterminate` pode levar a estados de clusters inconsistentes entre os nós e os nós seguindo uma célula primária antiga. Para exibir o modo de failover do cluster, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

A partir da versão 10.1, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos que não são acessíveis aos tenants que estão usando a API do VMware Cloud Director para testes de conexão. Configure a lista de negação após a instalação ou o upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação para conexão de teste](#).

Alterar o fuso horário do dispositivo do VMware Cloud Director

Depois de implantar com êxito o dispositivo do VMware Cloud Director, você pode alterar o fuso horário do sistema do dispositivo. Todas as instâncias do dispositivo do VMware Cloud Director no grupo de servidores e o armazenamento do servidor de transferência devem usar as mesmas configurações.

Pré-requisitos

- Implante o dispositivo do VMware Cloud Director. Consulte [Implantação e configuração inicial do dispositivo do VMware Cloud Director](#).
- Altere o fuso horário de armazenamento do servidor de transferência para o novo fuso horário do dispositivo primário do VMware Cloud 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 VMware Cloud Director como **raiz**.

- 4 Para garantir que o dispositivo do VMware Cloud 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 VMware Cloud Director.

Personalizar endereços públicos para o dispositivo do VMware Cloud Director

Para atender aos requisitos de balanceador de carga ou de proxy, você pode alterar os endereços da Web do endpoint padrão para o Portal da Web do VMware Cloud Director, a API do VMware Cloud Director e o proxy do console.

Você deve configurar o endereço de proxy do console público do VMware Cloud Director porque o dispositivo usa um único endereço IP com porta personalizada 8443 para o serviço de proxy do console. Consulte [6](#).

Pré-requisitos

Verifique se você está conectado como **administrador do sistema**. Somente um **administrador do sistema** pode personalizar os endpoints públicos.

Procedimentos

- 1 Na barra de navegação superior do Service Provider Admin Portal, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, clique em **Endereços Públicos**.
- 3 Para personalizar os endpoints públicos, clique em **Editar**.
- 4 Para personalizar as URLs do VMware Cloud Director, edite os endpoints do **Portal da Web**.
 - a Insira a URL pública personalizada do VMware Cloud Director para conexões HTTPS (seguras) e clique em **Carregar** para carregar os certificados que estabelecem a cadeia de confiança para esse endpoint.

A cadeia de certificados deve corresponder ao certificado usado pelo endpoint de serviço, que é o certificado carregado para cada armazenamento de chaves de célula do VMware Cloud Director com o alias `consoleproxy`. Não há suporte para a terminação SSL das conexões de proxy do console em um balanceador de carga. A cadeia de certificados deve incluir um certificado de endpoint, certificados intermediários e um certificado raiz no formato PEM sem uma chave privada.

5 (Opcional) Para personalizar as URLs da REST API e do OpenAPI do Cloud Director, desative a opção **Usar Configurações do Portal da Web**.

- a Insira uma URL base HTTP personalizada.

Por exemplo, se você definir a URL base HTTP como **http://vcloud.example.com**, poderá acessar a API do VMware Cloud Director em **http://vcloud.example.com/api** e poderá acessar o OpenAPI do VMware Cloud Director em **http://vcloud.example.com/cloudapi**.

- b Insira uma URL de base da REST API de HTTPS e clique em **Carregar** para carregar os certificados que estabelecem a cadeia de confiança para esse endpoint.

Por exemplo, se você definir a URL base da API REST HTTPS como **https://vcloud.example.com**, poderá acessar a API do VMware Cloud Director em **https://vcloud.example.com/api** e o OpenAPI do VMware Cloud Director em **https://vcloud.example.com/cloudapi**.

A cadeia de certificados deverá corresponder ao certificado usado pelo endpoint de serviço, que é o certificado carregado para cada armazenamento de chaves de célula do VMware Cloud Director com o alias **http**, ou ao certificado VIP do balanceador de carga se for usada uma terminação SSL. A cadeia de certificados deve incluir um certificado de endpoint, certificados intermediários e um certificado raiz no formato **PEM** sem uma chave privada.

6 Insira um endereço de proxy personalizado do console público do VMware Cloud Director.

Esse endereço é o nome de domínio completo (FQDN) do dispositivo do VMware Cloud Director **eth0** NIC, especificado por FQDN ou por endereço IP, com a porta personalizada **8443** para o serviço de proxy do console.

Por exemplo, para uma instância do VMware Cloud Director Appliance com FQDN **vcloud.example.com**, insira **vcloud.exemplo.com:8443**.

O VMware Cloud Director usa o endereço de proxy do console ao abrir uma janela de console remoto em uma VM.

7 Para salvar as alterações, clique em **Salvar**.

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

O VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. A recuperação das métricas atuais não exige o software de banco de dados opcional.

Pré-requisitos

- Verifique se o VMware Cloud 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 VMware Cloud 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 VMware Cloud 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@cell11 /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 5 Referência da ferramenta de gerenciamento de células](#).

- 2 (Opcional) Se você está atualizando o VMware Cloud 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@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --add-
rollup \ --username admin --password 'P@55w0rd'
```

- 3 Reinicie cada célula do VMware Cloud Director.

Instalar e configurar um agente RabbitMQ AMQP

Se quiser usar tarefas de bloqueio, notificações ou extensões de API do VMware Cloud Director, como Container Service Extension (CSE) e VMware Cloud Director App Launchpad, deverá instalar e configurar um Agente RabbitMQ AMQP.

O protocolo AMQP (Advanced Message Queuing Protocol) é um padrão aberto para enfileiramento de mensagens que oferece suporte a mensagens flexíveis para sistemas empresariais. O VMware Cloud Director usa o agente RabbitMQ AMQP para fornecer o barramento de mensagem usado por serviços de extensão, extensões de objeto e notificações.

Para o VMware Cloud Director, o uso de um cliente MQTT pode ser uma alternativa para o Agente RabbitMQ AMQP durante a configuração de notificações. Consulte [Assinar eventos, tarefas e métricas usando um cliente MQTT](#).

Procedimentos

- 1 Baixe o Servidor do RabbitMQ do <https://www.rabbitmq.com/download.html>.

Consulte *Notas da Versão do VMware Cloud 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 VMware Cloud Director.

3 Durante a instalação do RabbitMQ, anote os valores necessários para configurar o VMware Cloud 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 para não SSL. A porta padrão para SSL/TLS é 5671.
- O protocolo de comunicação é TCP.
- O host virtual do RabbitMQ. O padrão é "/"

Próximo passo

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

Para ativar o SSL com o serviço AMQP do VMware Cloud Director, consulte as informações em [configurar um agente deAMQP](#) no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

Alterar a senha raiz do dispositivo do VMware Cloud Director

Ao alterar a senha raiz de um dispositivo do VMware Cloud Director, você também deve atualizar o armazenamento de chaves do certificado do dispositivo para usar a nova senha.

Pré-requisitos

- Familiarize-se com o comando do `keytool`. O VMware Cloud Director insere uma cópia de `keytool` em `/opt/vmware/vcloud-director/jre/bin/keytool`.
- Se você estiver usando certificados curinga e estiver os armazenando no armazenamento de transferência compartilhado do NFS, para garantir que eles sejam atualizados, siga o procedimento descrito em [Implantar o dispositivo VMware Cloud Director com certificados curinga assinados para comunicação HTTPS e via proxy de console](#).

Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH no console do dispositivo do VMware Cloud Director como **root**.

- 2 Execute o comando `passwd` e altere a senha do usuário **root**.

```
passwd root
```

Observação Se o modo FIPS estiver habilitado, a senha **raiz** do dispositivo deverá conter pelo menos 14 caracteres.

Observação Se a senha root já tiver expirado, o VMware Cloud Director solicitará que você a defina pela primeira vez ao fazer login no console do dispositivo do VMware Cloud Director como **root**.

- 3 Execute o comando para fazer backup do arquivo de armazenamento de chaves de certificados existente.

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

- 4 Para gerar um novo armazenamento de chaves de certificados, execute o comando `keytool`.

```
keytool -importkeystore -srckeystore /opt/vmware/vcloud-director/certificates.ks
-srcstoretype PKCS12 -srcstorepass old_root_password -destkeystore /opt/vmware/vcloud-
director/certificates-new.ks -deststoretype PKCS12 -deststorepass new_root_password
-destkeypass new_root_password
```

Observação A partir do VMware Cloud Director 10.2, o tipo de armazenamento de chaves de certificados padrão para o dispositivo do VMware Cloud Director é PKCS12. Se estiver usando uma versão do dispositivo que tenha sido atualizada para a versão 10.2, use JCEKS como `-srcstoretype` e `-deststoretype`.

```
keytool -importkeystore -srckeystore /opt/vmware/vcloud-director/certificates.ks
-srcstoretype JCEKS -srcstorepass old_root_password -destkeystore /opt/vmware/vcloud-
director/certificates-new.ks -deststoretype JCEKS -deststorepass new_root_password
-destkeypass new_root_password
```

- 5 Execute o comando para substituir o arquivo de armazenamento de chaves de certificados antigo pelo novo.

```
mv /opt/vmware/vcloud-director/certificates-new.ks /opt/vmware/vcloud-director/
certificates.ks
```

- 6 Para verificar a propriedade de grupo e usuário do arquivo de armazenamento de chaves, execute o comando `chown`.

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

- 7 Para usar a nova senha do armazenamento de chaves, atualize a configuração do servidor do VMware Cloud Director:

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

Próximo passo

Repita este procedimento em cada dispositivo do cluster.

Importante Todos os dispositivos devem compartilhar a mesma senha root. Qualquer dispositivo recém-implantado deverá usar a nova senha root.

Fazendo upgrade e migrando o dispositivo do VMware Cloud Director

A partir da versão 9.7, o dispositivo do VMware Cloud Director inclui um banco de dados PostgreSQL incorporado com uma função de alta disponibilidade. Você pode fazer upgrade do dispositivo do VMware Cloud Director para uma versão posterior. Você pode migrar sua versão anterior existente do VMware Cloud Director com um banco de dados PostgreSQL externo para um ambiente do VMware Cloud Director que consiste em implantações de dispositivo do VMware Cloud Director de versão 10.0 ou posterior.

Fazendo upgrade do dispositivo do VMware Cloud Director

Para o upgrade da versão 9.7 para a versão 10.2 do dispositivo do VMware Cloud Director, consulte [Fazer upgrade do dispositivo do VMware Cloud Director usando um pacote de atualização](#).

A partir do VMware Cloud Director 10.0, os bancos de dados Microsoft SQL Server não têm suporte.

Quando você atualiza o VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Para obter informações sobre a compatibilidade do VMware Cloud 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. Se você planeja fazer upgrade dos componentes do vSphere ou do NSX como parte do upgrade do VMware Cloud Director, deverá fazer o upgrade deles após o upgrade do VMware Cloud Director. Consulte [Depois de fazer upgrade do VMware Cloud Director](#).

Depois de atualizar pelo menos um servidor VMware Cloud Director, você pode atualizar o banco de dados VMware Cloud Director. O banco de dados armazena informações sobre o estado de tempo de execução do servidor, incluindo o estado de todas as tarefas VMware Cloud 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 VMware Cloud 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 VMware Cloud 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`.

A partir da versão 10.1, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos que não são acessíveis aos tenants que estão usando a API do VMware Cloud Director para testes de conexão. Configure a lista de negação após a instalação ou o upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação para conexão de teste](#).

Importante Após o upgrade para a versão 10.1 e posterior, o VMware Cloud Director sempre verificará certificados para todos os endpoints de infraestrutura conectados a ele. Isso ocorre devido a uma alteração na maneira como o VMware Cloud Director gerencia certificados SSL. Se você não importar seus certificados para o VMware Cloud Director antes do upgrade, as conexões do vCenter Server e do NSX poderão apresentar erros de conexão devido a problemas de verificação de SSL. Nesse caso, após o upgrade, você tem duas opções:

- 1 Execute o comando `trust-infra-certs` da ferramenta de gerenciamento de células para importar automaticamente todos os certificados para o armazenamento centralizado de certificados. Consulte [importar os certificados de Endpoints dos recursos do vSphere](#).
 - 2 Na interface do usuário do Service Provider Admin Portal, selecione cada instância do vCenter Server e do NSX e insira novamente as credenciais ao aceitar o certificado.
-

Migrando o dispositivo do VMware Cloud Director

Se o seu grupo de servidores VMware Cloud Director existente consistir em uma implantação de dispositivo do VMware Cloud Director 9.5, você só poderá migrar seu ambiente para uma versão mais recente do dispositivo do VMware Cloud Director. Use o instalador do VMware Cloud 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](#).

Se o seu ambiente VMware Cloud 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 VMware Cloud Director 10.2. Para conhecer os caminhos de upgrade, consulte [Fazendo upgrade do VMware Cloud Director no Linux](#).

Fluxos de trabalho e caminhos de upgrade e migração

Ambiente de origem	Ambiente de destino
	Dispositivo do VMware Cloud Director 10.2 com um banco de dados PostgreSQL incorporado
VMware Cloud Director 9.7 no Linux com um banco de dados Microsoft SQL Server externo	<ol style="list-style-type: none"> 1 Migre para o dispositivo do VMware Cloud Director 9.7. Consulte Migrando o vCloud Director com um banco de dados Microsoft SQL externo para um dispositivo do vCloud Director. 2 Faça upgrade do seu ambiente para o dispositivo do VMware Cloud Director 10.2. Consulte Fazer upgrade do dispositivo do VMware Cloud Director usando um pacote de atualização.
VMware Cloud Director 9.7 no Linux com um banco de dados PostgreSQL externo	<ol style="list-style-type: none"> 1 Migre para o dispositivo do VMware Cloud Director 9.7. Consulte Migrando o vCloud Director com um banco de dados PostgreSQL externo para um dispositivo do vCloud Director. 2 Faça upgrade do seu ambiente para o dispositivo do VMware Cloud Director 10.2. Consulte Fazer upgrade do dispositivo do VMware Cloud Director usando um pacote de atualização.
VMware Cloud Director 10.0 no Linux com um banco de dados PostgreSQL externo	<ol style="list-style-type: none"> 1 Migre para o dispositivo do VMware Cloud Director 10.0. Consulte Migrando o vCloud Director com um banco de dados PostgreSQL externo para um dispositivo do vCloud Director. 2 Faça upgrade do seu ambiente para o dispositivo do VMware Cloud Director 10.2. Consulte Fazer upgrade do dispositivo do VMware Cloud Director usando um pacote de atualização.

Ambiente de origem	Ambiente de destino
	Dispositivo do VMware Cloud Director 10.2 com um banco de dados PostgreSQL incorporado
VMware Cloud Director 10.1 no Linux com um banco de dados PostgreSQL externo	<ol style="list-style-type: none"> 1 Migre para o dispositivo do VMware Cloud Director 10.1. Consulte Migrando o VMware Cloud Director com um banco de dados PostgreSQL externo para um dispositivo do VMware Cloud Director. 2 Faça upgrade do seu ambiente para o dispositivo do VMware Cloud Director 10.2. Consulte Fazer upgrade do dispositivo do VMware Cloud Director usando um pacote de atualização.
Dispositivo do VMware Cloud Director 9.7, 10.0 e 10.1 com um banco de dados PostgreSQL incorporado	Faça upgrade do seu ambiente para o dispositivo do VMware Cloud Director 10.2. Consulte Fazer upgrade do dispositivo do VMware Cloud Director usando um pacote de atualização .

Fazer upgrade do dispositivo do VMware Cloud Director usando um pacote de atualização

Você pode fazer upgrade do dispositivo do VMware Cloud Director para a versão mais recente ou aplicar patches ao dispositivo do VMware Cloud Director usando um pacote de atualização.

Durante o upgrade da implantação do dispositivo do VMware Cloud Director, o serviço VMware Cloud 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 VMware Cloud Director e executar o script de atualização do banco de dados VMware Cloud Director. O número de células de trabalho no grupo de servidores VMware Cloud Director será reduzido até que você pare o serviço VMware Cloud Director no último dispositivo VMware Cloud Director. Um balanceador de carga configurado adequadamente na frente dos endpoints HTTP do VMware Cloud Director deve parar o roteamento do tráfego para as células que estão paradas.

Depois de aplicar o upgrade a cada dispositivo do VMware Cloud Director e o upgrade do banco de dados estiver concluído, você deverá reinicializar cada dispositivo do VMware Cloud Director.

Pré-requisitos

Tire um instantâneo do dispositivo primário do VMware Cloud Director.

- 1 Ao fazer upgrade da versão 10.1 ou posterior ou ao aplicar patches, se o failover automático no caso de uma falha no serviço de banco de dados primário estiver ativado, altere o modo de failover para `Manual` durante o upgrade. Após o upgrade, você pode definir o modo de failover como `Automatic`. Consulte [Failover automático do dispositivo do VMware Cloud Director](#).
- 2 Faça login na instância do vCenter Server na qual reside o dispositivo primário do VMware Cloud Director do seu cluster de alta disponibilidade do banco de dados.
- 3 Navegue até o dispositivo primário do VMware Cloud Director, clique com o botão direito do mouse nele e clique em **Ligar/Desligar > Encerrar SO Convidado**.

- 4 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**.
- 5 Clique com o botão direito do mouse no dispositivo do VMware Cloud Director e clique em **Ligar/Desligar > Ligar**.
- 6 Verifique se todos os nós na configuração de alta disponibilidade do banco de dados estão em bom estado. Consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

Procedimentos

- 1 Em um navegador da Web, faça login na interface do usuário de gerenciamento do dispositivo de uma instância de dispositivo VMware Cloud 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 VMware Cloud Director é distribuído como um arquivo executável com um nome no formato `VMware_Cloud_Director_v.v.v.v-xxxxxxxxx_update.tar.gz`, em que `v.v.v.v` representa a versão do produto e `xxxxxxxxx`, o número da compilação. Por exemplo, `VMware_Cloud_Director_10.1.0.4424-14420378_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 -xzf VMware_Cloud_Director_v.v.v.v-xxxxxxxxx_update.tar.gz \
-C /tmp/local-update-package
```

- 5 Defina o diretório `local-update-package` como o repositório de atualização.

```
vam_cli update --repo file:///tmp/local-update-package
```

- 6 Verifique se há atualizações para conferir se você estabeleceu corretamente o repositório.

```
vam_cli update --check
```

A versão do upgrade aparece como `Atualização Disponível`.

- 7 Encerre o VMware Cloud 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 VMware Cloud Director incorporado.

```
/opt/vmware/appliance/bin/create-db-backup
```

- 11 Em qualquer dispositivo, execute o utilitário `upgrade` do banco de dados VMware Cloud Director.

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

- 12 Reinicie cada dispositivo do VMware Cloud Director.

```
shutdown -r now
```

Próximo passo

- Se o upgrade for bem-sucedido, você poderá excluir o instantâneo do dispositivo do VMware Cloud Director.
- Se o upgrade não for bem-sucedido, você poderá reverter o dispositivo do VMware Cloud Director para o instantâneo que tirou antes do upgrade. Consulte [Reverter um dispositivo do VMware Cloud Director quando um upgrade falhar](#).

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

Você pode usar o Repositório de Atualização da VMware para fazer upgrade do dispositivo do VMware Cloud Director da versão 9.7 para a 10.0 e posteriores e aplicar patches.

Observação Você pode usar o Repositório de atualização do VMware somente para atualizar o VMware Cloud Director para a versão mais recente do VMware Cloud Director. Somente a versão mais recente está disponível no repositório de atualização da VMware. Se você quiser atualizar o VMware Cloud Director para uma versão diferente, consulte [Fazer upgrade do dispositivo do VMware Cloud Director usando um pacote de atualização](#).

Durante o upgrade da implantação do dispositivo do VMware Cloud Director, o serviço VMware Cloud 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 VMware Cloud Director e executar o script de atualização do banco de dados VMware Cloud Director. O

número de células de trabalho no grupo de servidores VMware Cloud Director será reduzido até que você pare o serviço VMware Cloud Director no último dispositivo VMware Cloud Director. Um balanceador de carga configurado adequadamente na frente dos endpoints HTTP do VMware Cloud Director deve parar o roteamento do tráfego para as células que estão paradas.

Depois de aplicar o upgrade a cada dispositivo do VMware Cloud Director e o upgrade do banco de dados estiver concluído, você deverá reinicializar cada dispositivo do VMware Cloud Director.

Pré-requisitos

- Tire um instantâneo do dispositivo primário do VMware Cloud Director.
 - a Ao fazer upgrade da versão 10.1 ou posterior ou quando aplicar patches, se o failover automático no caso de uma falha no serviço de banco de dados primário estiver ativado, altere o modo de failover para o `Manual` para a duração do upgrade. Após o upgrade, você pode definir o modo de failover como `Automatic`. Consulte [Failover automático do dispositivo do VMware Cloud Director](#).
 - b Faça login na instância do vCenter Server na qual reside o dispositivo primário do VMware Cloud Director do seu cluster de alta disponibilidade do banco de dados.
 - c Navegue até o dispositivo primário do VMware Cloud Director, clique com o botão direito do mouse nele e clique em **Ligar/Desligar > Encerrar SO Convidado**.
 - d 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**.
 - e Clique com o botão direito do mouse no dispositivo do VMware Cloud Director e clique em **Ligar/Desligar > Ligar**.
 - f Verifique se todos os nós na configuração de alta disponibilidade do banco de dados estão em bom estado. Consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).
- Verifique se o dispositivo do VMware Cloud 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 VMware Cloud Director para identificar o dispositivo primário, `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 Faça login diretamente ou usando um cliente SSH no console do dispositivo primário como **raiz**.

- 3 Redefina o repositório de atualização para apontar para o Repositório de Atualização da VMware.

```
vamicli update --repo ""
```

- 4 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`.

- 5 Encerre o VMware Cloud Director executando o seguinte comando:

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

- 6 Continuando no dispositivo primário, faça backup do banco de dados do dispositivo VMware Cloud Director incorporado.

```
/opt/vmware/appliance/bin/create-db-backup
```

Observação Você deve fazer backup do dispositivo somente uma vez. Não faça backup do dispositivo depois de aplicar o upgrade disponível.

- 7 Aplique o upgrade disponível.

```
vamicli update --install latest
```

- 8 Faça login nas células de aplicativo e em espera restantes e repita as etapas 3, 4, 5 e 7 em cada dispositivo.
- 9 Em qualquer dispositivo, execute o utilitário `upgrade` do banco de dados VMware Cloud Director.

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

- 10 Reinicie cada dispositivo do VMware Cloud Director.

```
shutdown -r now
```

Próximo passo

- Se o upgrade for bem-sucedido, você poderá excluir o snapshot do dispositivo do VMware Cloud Director.
- Se o upgrade não for bem-sucedido, você poderá reverter o dispositivo do VMware Cloud Director para o snapshot que tirou antes do upgrade. Consulte [Reverter um dispositivo do VMware Cloud Director quando um upgrade falhar](#).

- Se houver uma falha no comando `vamicli update --install latest`, consulte [Falha na instalação da atualização mais recente do VMware Cloud Director](#).

Reverter um dispositivo do VMware Cloud Director quando um upgrade falhar

Se o upgrade de um dispositivo do VMware Cloud Director falhar, você poderá usar o instantâneo do dispositivo que tirou antes do upgrade e reverter o dispositivo do VMware Cloud Director.

Antes de iniciar a reversão, use a API do dispositivo do VMware Cloud Director para anotar as IDs dos nós em espera no cluster. Consulte *Referência de esquemas de API do dispositivo do VMware Cloud Director* em <http://code.vmware.com>.

- 1 Reverta o dispositivo primário do VMware Cloud 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 VMware Cloud Director.
- 3 Faça login diretamente ou usando um cliente SSH no sistema operacional de cada célula do dispositivo do VMware Cloud Director. Você deve fazer login como usuário **root**.
- 4 Pare os serviços do VMware Cloud Director em todas as células do dispositivo.

```
service vmware-vcd stop
```

- 5 Use a célula primária do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director usando o vSphere Client](#).
- 9 Faça login diretamente ou usando um cliente SSH no sistema operacional de cada célula do dispositivo do VMware Cloud Director. Você deve fazer login como usuário **root**.
- 10 Inicie os serviços do VMware Cloud Director.

```
service vmware-vcd start
```

Migrando o VMware Cloud Director com um banco de dados PostgreSQL externo para o dispositivo do VMware Cloud Director

Se o seu ambiente do VMware Cloud Director atual usar um banco de dados PostgreSQL externo, você poderá migrar para um novo ambiente do VMware Cloud Director formado por implantações de dispositivos do VMware Cloud Director. Seu ambiente atual do VMware Cloud Director pode consistir em instalações do VMware Cloud Director no Linux ou em implantações de dispositivos do VMware Cloud Director. O novo ambiente VMware Cloud 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 VMware Cloud Director existente

- Criando o novo grupo de servidores VMware Cloud Director implantando uma ou mais instâncias do dispositivo do VMware Cloud 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 VMware Cloud Director atual para a versão 10.2.

Consulte [Fazendo upgrade do VMware Cloud Director no Linux](#).

- 3 Verifique se a reinicialização do VMware Cloud Director de origem de migração foi bem-sucedida.
- 4 Em cada célula do ambiente VMware Cloud Director atualizado, execute o comando para interromper o serviço VMware Cloud 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 deve criar esse usuário no novo ambiente e renomear o banco de dados na [Etapa 13](#).

- 7 Se quiser que o novo ambiente VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.
 - 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 [Implantação e configuração inicial do dispositivo do VMware Cloud Director](#).

- 10 Em cada nova célula implantada, execute o comando para interromper o serviço VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 7 a](#).

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 VMware Cloud 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 VMware Cloud Director falha ao migrar ou restaurar para o dispositivo VMware Cloud Director](#).

- d Execute o comando para iniciar o serviço VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 da origem de migração.
 - 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 VMware Cloud Director, use o Service Provider Admin Portal para excluir as células desconectadas que pertencem ao ambiente VMware Cloud Director antigo.
 - a Na barra de navegação superior, em **Recursos**, 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 VMware Cloud Director para adicionar membros ao grupo de servidores do ambiente migrado.

O que fazer em seguida

O novo ambiente do dispositivo do VMware Cloud 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 VMware Cloud 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 fazer upgrade do VMware Cloud Director

Depois que fazer upgrade de todos os servidores do VMware Cloud Director e o banco de dados compartilhado, poderá fazer upgrade das instâncias do NSX Manager que fornecem serviços de rede à nuvem. Depois disso, você poderá atualizar os hosts do ESXi e as instâncias do vCenter Server que estão registradas em sua instalação do VMware Cloud Director.

Importante O VMware Cloud Director oferece suporte somente a edge gateways avançados. Você deve converter qualquer edge gateway não avançado herdado em um gateway avançado. Consulte <https://kb.vmware.com/kb/66767>.

A partir da versão 10.1, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos que não são acessíveis aos tenants que estão

usando a API do VMware Cloud Director para testes de conexão. Configure a lista de negação após a instalação ou o upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação para conexão de teste](#).

Importante Após o upgrade para a versão 10.1 e posterior, o VMware Cloud Director sempre verificará certificados para todos os endpoints de infraestrutura conectados a ele. Isso ocorre devido a uma alteração na maneira como o VMware Cloud Director gerencia certificados SSL. Se você não importar seus certificados para o VMware Cloud Director antes do upgrade, as conexões do vCenter Server e do NSX poderão apresentar erros de conexão devido a problemas de verificação de SSL. Nesse caso, após o upgrade, você tem duas opções:

- 1 Execute o comando `trust-infra-certs` da ferramenta de gerenciamento de células para importar automaticamente todos os certificados para o armazenamento centralizado de certificados. Consulte [importar os certificados de Endpoints dos recursos do vSphere](#).
 - 2 Na interface do usuário do Service Provider Admin Portal, selecione cada instância do vCenter Server e do NSX e insira novamente as credenciais ao aceitar o certificado.
-

Atualizar cada NSX Manager associado a um sistema vCenter Server anexado

Antes de atualizar um vCenter Server e hosts ESXi registrados no VMware Cloud 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 VMware Cloud Director, mesmo que as células do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director e o NSX Manager, você deve atualizar os sistemas vCenter Server e os hosts ESXi que estão registrados no VMware Cloud 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 Na barra de navegação superior do VMware Cloud Director Service Provider Admin Portal, em **Recursos**, selecione **Recursos do vSphere**.
- b No painel esquerdo, clique em **Instâncias do vCenter Server**.
- c Selecione o botão de opção ao lado da instância 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 VMware Cloud Director.

- a Na barra de navegação superior, 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 VMware Cloud Director.

- a Na barra de navegação superior do VMware Cloud Director Service Provider Admin Portal, em **Recursos**, selecione **Recursos do vSphere**.
- b No painel esquerdo, clique em **Instâncias do vCenter Server**.
- 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 VMware Cloud 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/br/>.
- Para usar o VMware Cloud Director para fazer upgrade do edge gateway do NSX, você deve operar no objeto de rede do VMware Cloud Director ao qual o Edge oferece suporte:
 - Um upgrade apropriado de um Edge Gateway ocorre automaticamente quando você usa o VMware Cloud Director ou a API do VMware Cloud Director 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 VMware Cloud Director*.

Próximo passo

Repita esse procedimento para os outros sistemas vCenter Server registrados na sua instalação do VMware Cloud Director.

Administração do dispositivo do VMware Cloud Director

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 VMware Cloud 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 VMware Cloud 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.

Observação Se o cluster estiver configurado para failover automático, depois de implantar uma ou mais células adicionais, você deverá usar a API do Dispositivo para redefinir o modo de failover do cluster para o `Automatic`. Consulte a [API do dispositivo do VMware Cloud Director](#). O modo de failover padrão para novas células é `Manual`. Se o modo de failover estiver inconsistente em todos os nós do cluster, o modo de failover do cluster será `Indeterminate`. O modo de `Indeterminate` pode levar a estados de clusters inconsistentes entre os nós e os nós seguindo uma célula primária antiga. Para exibir o modo de failover do cluster, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

Fazer backup e restaurar o banco de dados incorporado do dispositivo do VMware Cloud Director

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

Fazer backup do banco de dados incorporado do dispositivo VMware Cloud Director

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

Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH da célula primária como **raiz**.
- 2 Faça backup do banco de dados incorporado do dispositivo VMware Cloud Director executando o seguinte comando.

```
/opt/vmware/appliance/bin/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.

Restaurar um ambiente de dispositivo VMware Cloud Director 10.2.1 e anterior com uma configuração de banco de dados de alta disponibilidade

Se você tiver feito backup do banco de dados PostgreSQL de um ambiente de dispositivo VMware Cloud Director 10.2.1 e anterior 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 VMware Cloud Director](#).
- Implante uma célula de banco de dados primária e duas células de banco de dados em espera. Consulte [Implantação e configuração inicial do dispositivo do VMware Cloud Director](#).
- 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 VMware Cloud 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 VMware Cloud Director da versão 9.7.0.1 até a versão 10.2.1.

- 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 VMware Cloud 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 VMware Cloud Director da versão 9.7.0.1 até a versão 10.2.1.

```
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 VMware Cloud Director da versão 9.7.0.1 até a versão 10.2.1.

- 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 os seguintes comandos para reconfigurar o serviço VMware Cloud 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 --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

/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-
ssl true
```

Em que:

- A opção `--keystore-password` corresponde à senha do armazenamento de chaves para os certificados no dispositivo. A senha do armazenamento de chaves pode ser a senha **root** utilizada durante a implantação do dispositivo.
- A opção `--database-password` corresponde à senha de banco de dados que você definiu durante a configuração do dispositivo na UI de gerenciamento do dispositivo do VMware Cloud Director em `https://appliance_eth0_ip:5480`.
- 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 VMware Cloud Director falha ao migrar ou restaurar para o dispositivo VMware Cloud Director](#).

- e Execute o comando para iniciar o serviço VMware Cloud 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 [Implantação e configuração inicial do dispositivo do VMware Cloud Director](#).
- 7 Se os novos dispositivos usarem IPs diferentes dos dispositivos originais que você está substituindo, será necessário atualizar a configuração do balanceador de carga que faz frente ao grupo de servidores VMware Cloud Director para incluir os IPs dos novos dispositivos.

- 8 Depois que todas as células do grupo de servidores terminarem o processo de inicialização, verifique se a restauração do seu ambiente VMware Cloud Director foi bem-sucedida.
 - a Abra o VMware Cloud 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`.

Se você tiver atualizado a configuração do balanceador de carga de acordo com a etapa 7, deverá usar o endereço público do grupo de servidores para acessar o Service Provider Admin Portal.
 - 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.
- 9 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 VMware Cloud Director.
 - a Na barra de navegação superior, em **Recursos**, selecione **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Células da Nuvem**.
 - c Selecione uma célula inativa e clique em **Cancelar registro**.
- 10 Se o modo de failover antes da restauração era `Automatic`, você deverá defini-lo novamente como `Automatic` usando a API do dispositivo do VMware Cloud Director.

Restaurar um ambiente de dispositivo VMware Cloud Director 10.2.2 e posterior com uma configuração de banco de dados de alta disponibilidade

Se você tiver feito backup do banco de dados PostgreSQL de um ambiente de dispositivo VMware Cloud Director 10.2.2 e posterior 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 VMware Cloud Director](#).

- Implante uma célula de banco de dados primária e duas células de banco de dados em espera. Consulte [Implantação e configuração inicial do dispositivo do VMware Cloud Director](#).
- 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 VMware Cloud 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 os arquivos extraídos

global.properties, responses.properties, certificates.pem, certificates.key, proxycertificates.pem, proxycertificates.key, truststore.pem e o arquivo de despejo de banco de dados denominado vcloud_date_time_format.

Observação O arquivo truststore.pem está disponível somente para o VMware Cloud Director 10.2.2 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 VMware Cloud Director.

- a Faça backup das propriedades, dos certificados e dos arquivos truststore.

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

Observação O arquivo `truststore.pem` está disponível somente para o VMware Cloud Director 10.2.2 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.pem` está disponível somente para o VMware Cloud Director 10.2.2 e versões posteriores.

- 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 os seguintes comandos para reconfigurar o serviço VMware Cloud 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 --uid --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
```

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-
ssl true
```

Em que:

- A opção `--keystore-password` corresponde à senha do armazenamento de chaves para os certificados no dispositivo. A senha do armazenamento de chaves pode ser a senha **root** utilizada durante a implantação do dispositivo.

- A opção `--database-password` corresponde à senha de banco de dados que você definiu durante a configuração do dispositivo na UI de gerenciamento do dispositivo do VMware Cloud Director em `https://appliance_eth0_ip:5480`.
- 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 VMware Cloud Director falha ao migrar ou restaurar para o dispositivo VMware Cloud Director](#).

- e Execute o comando para iniciar o serviço VMware Cloud 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 [Implantação e configuração inicial do dispositivo do VMware Cloud Director](#).
- 7 Se os novos dispositivos usarem IPs diferentes dos dispositivos originais que você está substituindo, será necessário atualizar a configuração do balanceador de carga que faz frente ao grupo de servidores VMware Cloud Director para incluir os IPs dos novos dispositivos.
- 8 Depois que todas as células do grupo de servidores terminarem o processo de inicialização, verifique se a restauração do seu ambiente VMware Cloud Director foi bem-sucedida.
 - a Abra o VMware Cloud Director Service Provider Admin Portal usando o endereço IP de rede `eth0` de qualquer célula do novo grupo de servidores, `https://et0_IP_new_cell/provider`.

Se você tiver atualizado a configuração do balanceador de carga de acordo com a etapa 7, deverá usar o endereço público do grupo de servidores para acessar o Service Provider Admin Portal.
 - 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.

- 9 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 VMware Cloud Director.
 - a Na barra de navegação superior, em **Recursos**, selecione **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Células da Nuvem**.
 - c Selecione uma célula inativa e clique em **Cancelar registro**.
- 10 Se o modo de failover antes da restauração era *Automatic*, você deverá defini-lo novamente como *Automatic* usando a API do dispositivo do VMware Cloud Director.
- 11 Se o modo FIPS do dispositivo VMware Cloud Director estava ativo antes da restauração, você deve defini-lo novamente usando a API do dispositivo VMware Cloud Director.

O modo FIPS da célula é restaurado automaticamente.

Alterando o modo de failover do dispositivo do VMware Cloud Director

Por padrão, o dispositivo do VMware Cloud Director está no modo de failover manual e, se o serviço de banco de dados primário falhar, você deverá iniciar a ação de failover. Você pode definir o modo de failover como automático usando a API do dispositivo.

Do VMware Cloud Director 10.1 em diante, se o serviço do banco de dados primário falhar, você poderá ativar o VMware Cloud Director para realizar um failover automático para um novo primário. Consulte [Failover automático do dispositivo do VMware Cloud Director](#).

O modo de failover é definido como *automatic* ou *manual* usando a API do dispositivo do VMware Cloud Director. Consulte a seção *Failovermode* da [Referência do esquema de API do dispositivo do VMware Cloud Director](#).

No caso de clusters configurados com failover automático, após implantar uma ou mais células adicionais, você deverá usar a API do dispositivo para redefinir o modo de failover do cluster como *automatic*. Se você não redefinir o modo de failover do cluster, os modos de failover serão inconsistentes entre os nós.

Configurar o acesso externo ao banco de dados do VMware Cloud Director

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

Durante uma migração para o dispositivo do VMware Cloud 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 VMware Cloud Director incorporado.

Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH da célula primária como **raiz**.

- 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  CIDR_notation    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 VMware Cloud Director

Durante a implantação do dispositivo, você pode deixar desativado o acesso SSH ou ativá-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 desativar o acesso ao SSH para o usuário **raiz**. O acesso ao SSH para a função de HA do banco de dados permanece inalterado.

Pré-requisitos

Para fazer com que as alterações nas propriedades OVF sejam permanentes, você deve usar a interface de usuário do vSphere para alterar os valores da propriedade OVF. Consulte o tópico *Configurar propriedades do vApp no guia Administração da máquina virtual do vSphere*.

Procedimentos

- 1 Se você quiser fazer alterações temporárias na propriedade OVF, por exemplo, para fins de teste, altere a propriedade no VMware Cloud Director.
 - a Faça login diretamente ou usando um cliente SSH no console do dispositivo do VMware Cloud Director como **root**.
 - b Execute o script para ativar ou desativar o acesso **raiz** ao SSH.
 - Para ativar o acesso **raiz** ao SSH, execute o script `/opt/vmware/appliance/bin/enable_root_login.sh`.
 - Para desativar 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**.

Ativar ou desativar o modo FIPS no dispositivo VMware Cloud Director

Na versão 10.2.2, você pode configurar o dispositivo VMware Cloud Director para usar módulos criptográficos validados para FIPS 140-2 e executar no modo compatível com FIPS.

O Federal Information Processing Standard (FIPS) 140-2 é um padrão federal dos EUA e do Canadá que especifica requisitos de segurança para módulos criptográficos. O Programa de Validação de Módulos Criptográficos (CMVP) do NIST valida os módulos criptográficos em conformidade com os padrões FIPS 140-2.

O objetivo do suporte ao FIPS do VMware Cloud Director é facilitar as atividades de conformidade e a segurança em vários ambientes regulamentados. Para saber mais sobre o suporte para FIPS 140-2 em produtos da VMware, consulte <https://www.vmware.com/security/certifications/fips.html>.

A criptografia validada por FIPS do VMware Cloud Director está desativada por padrão. Ao ativar o modo FIPS, você configura o VMware Cloud Director para usar módulos criptográficos validados para FIPS 140-2 e executados no modo compatível com FIPS.

Observação Ativar o modo FIPS também permite a pesquisa inversa de nomes de host.

Importante Quando você ativa o modo FIPS, a integração ao vRealize Orchestrator não funciona.

No VMware Cloud Director 10.2.2, quando você ativa o modo FIPS, não é possível criptografar asserções SAML. Quando não está no modo FIPS, não há restrição quanto à criptografia de asserções.

O VMware Cloud Director usa os seguintes módulos criptográficos validados para FIPS 140-2:

- BC-FJA (Bouncy Castle FIPS Java API) da VMware, versão 1.0.2.1: [Certificado #3673](#)
- Módulo de objeto OpenSSL FIPS da VMware, versão 2.0.20-vmw: [Certificado #3857](#)

O VMware Cloud Director está em um pacote com a ferramenta de gerenciamento de células (CMT). No entanto, a ferramenta de gerenciamento de células não é compatível com FIPS.

Ao usar o dispositivo VMware Cloud Director para configurar o dispositivo para ser executado no modo compatível com FIPS, você deve gerenciar tanto o modo FIPS do dispositivo quanto o modo FIPS da célula.

- O modo FIPS do dispositivo é o modo do SO do dispositivo subjacente, do banco de dados incorporado e de várias bibliotecas de sistema.
- O modo FIPS da célula é o modo da célula do VMware Cloud Director em execução em cada dispositivo.

Para ativar e desativar o modo FIPS no VMware Cloud Director no Linux, consulte [Ativar o modo FIPS nas células do grupo de servidores](#).

Pré-requisitos

- Se a coleta de métricas estiver ativada, verifique se os certificados Cassandra seguem o padrão de certificado X.509 v3 e incluem todas as extensões necessárias. Você deve configurar o Cassandra com os mesmos conjunto de codificações usados pelo VMware Cloud Director. Para obter informações sobre as codificações SSL permitidas, consulte [Gerenciando a lista de codificações SSL permitidas](#).
- Cancele o registro do VMware Cloud Director no vCenter Lookup Service. Consulte [Configurar o vSphere Services](#) no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

Procedimentos

- 1 Na barra de navegação superior do Service Provider Admin Portal, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, selecione **SSL**.
- 3 Clique em **Ativar**.
- 4 Para confirmar que você deseja iniciar o processo, clique em **Ativar**.

Quando a configuração terminar, o VMware Cloud Director exibirá uma mensagem *Ativação em andamento (Aguardando reinicialização das células)*, e você poderá continuar na etapa 5. Quando você executar o comando de API na etapa 5, o dispositivo VMware Cloud Director reiniciará as células automaticamente.

- 5 Para ativar ou desativar o modo FIPS do dispositivo, use a API do dispositivo VMware Cloud Director para fazer uma solicitação PUT à URL `fips/{node_name}`. Consulte a [API do dispositivo VMware Cloud Director](#).

Observação Você deve usar o `{node_name}` da máquina que está processando a solicitação PUT.

Exemplo: ativando o modo FIPS

Solicitação:

```
PUT https://vcloud.example.com:5480/api/1.0.0/fips/{node_name}
Content-Type: application/json
```

```
...
{
  "applianceFips": "ON"
}
```

6 Repita a etapa 5 para cada dispositivo, por exemplo, tipos primário, em espera e de aplicativo.

Próximo passo

Para confirmar o estado das células, você pode usar a UI de gerenciamento do dispositivo do VMware Cloud Director. Consulte [Visualizar o modo FIPS do dispositivo VMware Cloud Director](#).




Visualizar o modo FIPS do dispositivo VMware Cloud Director

Na versão 10.2.2, o dispositivo VMware Cloud Director pode ser executado no modo compatível com FIPS. Você pode exibir o modo FIPS do dispositivo e da célula.

Ao usar o dispositivo VMware Cloud Director, para configurar o dispositivo VMware Cloud Director para ser executado no modo compatível com FIPS, você deve gerenciar tanto o modo FIPS do dispositivo quanto o modo FIPS da célula.

- O modo FIPS do dispositivo é o modo do SO do dispositivo subjacente, do banco de dados incorporado e de várias bibliotecas de sistema.
- O modo FIPS da célula é o modo da célula do VMware Cloud Director em execução em cada dispositivo.

Tabela 3-1. Estado do modo FIPS

Integridade	Descrição
	Os modos FIPS da célula e do dispositivo do são diferentes. Ambos os modos estão ativos ou desligados.
	O modo FIPS da célula está em estado de Reinicialização pendente . Use a API do dispositivo para ativar ou desativar o modo FIPS do dispositivo. Alterar o modo FIPS do dispositivo reinicia automaticamente o serviço de célula do VMware Cloud Director.
	O dispositivo VMware Cloud Director não pode determinar o modo FIPS da célula. Falhas no serviço do VMware Cloud Director no dispositivo do podem fazer com que o modo FIPS da célula seja indeterminado.

Pré-requisitos

[Ativar ou desativar o modo FIPS no dispositivo VMware Cloud Director](#)

Procedimentos

- 1 Faça login como **root** na interface do usuário de gerenciamento do dispositivo em `https://primary_eth1_ip_address:5480`.

- 2 No painel esquerdo, selecione **Configuração do Sistema**.
- 3 Visualize o status do modo FIPS da célula e do dispositivo em cada nó.

Configurando o agente SNMP do dispositivo VMware Cloud Director

No VMware Cloud Director 10.2.2, você pode configurar o agente SNMP do dispositivo VMware Cloud Director para escutar solicitações de sondagem.

O SNMP (Protocolo de Gerenciamento de Rede Simples) é um protocolo de camada de aplicativo para o gerenciamento e o monitoramento de elementos de rede. O dispositivo VMware Cloud Director inclui um agente SNMP que pode receber e responder às solicitações `GET`, `GETBULK` e `GETNEXT`. O agente SNMP do dispositivo VMware Cloud Director é compatível com todos os serviços de gerenciamento SNMP que aceitam os padrões SNMP. É possível configurar o agente para SNMP v1, v2c ou v3. No entanto, somente o SNMP v3 oferece segurança reforçada, incluindo autenticação criptográfica e criptografia.

Se houver um agente Net-SNMP existente, antes de iniciar a configuração, considere o seguinte:

- Durante o upgrade para a versão 10.2.2 ou posterior, o VMware Cloud Director exclui e substitui Net-SNMP por VMware-SNMP.
- Você deve remover todas as regras de firewall existentes que funcionam com Net-SNMP, pois VMware-SNMP ativa e desativa a porta de sondagem ao iniciar e interromper o serviço `snmpd`.

O VMware-SNMP para o dispositivo VMware Cloud Director oferece suporte a bases de informações de gerenciamento (MIBs) do sistema operacional Linux padrão disponíveis por meio das seguintes MIBs padrão do setor.

- SNMPv2-MIB
- RFC 3418IF-MIB
- RFC 2863IP-MIB
- RFC 4293IP-FORWARD-MIB
- RFC 4292UDP-MIB
- RFC 4113TCP-MIB
- RFC 4022ENTITY-MIB
- RFC 4133HOST-RESOURCES-MIB
- RFC 2790VMWARE-SYSTEM-MIB, REVISION 201008020000Z

Configurar uma porta personalizada para o agente SNMP

No VMware Cloud Director 10.2.2, se você configurar o agente SNMP do VMware Cloud Director para sondagem, ele poderá escutar e responder a solicitações de sistemas cliente de gerenciamento SNMP, como solicitações `GET`, `GETNEXT` e `GETBULK`.

Por padrão, o agente SNMP incorporado escuta na porta UDP 161 em busca de solicitações de sondagem de sistemas de gerenciamento. É possível usar o comando `vicfg-snmp --port` para configurar uma porta alternativa. Para evitar conflitos entre a porta do agente SNMP e as portas de outros serviços, consulte <https://ports.vmware.com/home/VMware-Cloud-Director>.

Pré-requisitos

Você deve remover todas as regras de firewall existentes que funcionam com Net-SNMP, pois VMware-SNMP ativa e desativa a porta de sondagem ao iniciar e interromper o serviço `snmpd`.

Procedimentos

- 1 Faça login no shell do dispositivo como um usuário com privilégios administrativos.
- 2 Desative o SNMP executando o seguinte comando.

```
vicfg-snmp --disable
```

- 3 Para alterar a porta usada pelo agente SNMP para ouvir solicitações de sondagem, execute o seguinte comando.

```
vicfg-snmp --port port_number
```

Configurar o dispositivo VMware Cloud Director para SNMP v1 e v2c

No VMware Cloud Director 10.2.2, é possível configurar um dispositivo VMware Cloud Director para SNMP definindo pelo menos uma comunidade para o agente SNMP. Quando você configura o agente SNMP do VMware Cloud Director para SNMP v1 e v2c, o agente oferece suporte para sondagem.

No SNMP v1 e v2c, as cadeias da comunidade são namespaces que contêm um ou mais objetos gerenciados. Namespaces podem atuar como uma forma de autenticação, mas isso não protege a comunicação. Para proteger a comunicação, use SNMP v3.

Para permitir que o agente SNMP do dispositivo VMware Cloud Director envie e receba mensagens SNMP v1 e v2c, você deve configurar pelo menos uma comunidade para o agente. Uma comunidade SNMP define um grupo de dispositivos e sistemas de gerenciamento. Somente dispositivos e sistemas de gerenciamento que forem membros da mesma comunidade poderão trocar mensagens SNMP. Um dispositivo ou sistema de gerenciamento pode ser membro de várias comunidades.

Procedimentos

- 1 Faça login no shell do dispositivo como um usuário com privilégios administrativos.
- 2 Para configurar uma comunidade SNMP, execute o comando `vicfg-snmp -c`.

Por exemplo, para configurar comunidades nos centros de operações de rede pública leste e oeste, execute o seguinte comando:

```
vicfg-snmp --communities public,eastnoc,westnoc
```

Todas as vezes que você especificar uma comunidade com esse comando, as configurações especificadas substituirão a configuração anterior. Para inserir várias comunidades, use vírgulas como separadores.

3 Ative o SNMP executando o seguinte comando.

```
vicfg-snmp --enable
```

Configurar o dispositivo VMware Cloud Director para SNMP v3

No VMware Cloud Director 10.2.2, é possível configurar o dispositivo VMware Cloud Director para SNMP v3. Quando você configura o agente SNMP para SNMP v3, o agente oferece suporte para sondagem e fornece uma segurança mais reforçada, incluindo autenticação criptográfica e criptografia.

A configuração do dispositivo VMware Cloud Director para SNMP v3 consiste em três partes.

- 1 Configurando o ID do mecanismo SNMP
- 2 Configurando protocolos de autenticação e privacidade SNMP
- 3 Configurando usuários SNMP

Cada agente SNMP v3 tem um ID de mecanismo, que serve como um identificador exclusivo do agente. O ID de mecanismo é usado com uma função de hash para gerar chaves localizadas para a autenticação e a criptografia de mensagens SNMP v3. Se você não especificar um ID de mecanismo antes de ativar o agente SNMP, ao ativar o agente SNMP autônomo, o VMware Cloud Director gerará um ID de mecanismo.

Para garantir a identidade dos usuários, você pode usar autenticação. A privacidade permite a criptografia de mensagens SNMP v3 para garantir a confidencialidade dos dados. Os protocolos de privacidade oferecem um nível de segurança maior que o disponível no SNMP v1 e v2c, que usam cadeias de caracteres da comunidade para segurança. A autenticação e a privacidade são opcionais. No entanto, se você planeja ativar a privacidade, precisa ativar a autenticação.

O valor padrão para os protocolos de autenticação e privacidade é Nenhum.

Você pode configurar até cinco usuários que podem acessar as informações do SNMP v3. Nomes de usuário não devem ter mais de 32 caracteres. Ao configurar um usuário, você gera os valores de hash de autenticação e privacidade com base nas senhas de autenticação e privacidade do usuário e no ID de mecanismo do agente SNMP. Depois de configurar os usuários, se o ID de mecanismo for alterado, o protocolo de autenticação ou o protocolo de privacidade invalidará os usuários e será necessário reconfigurá-los.

Pré-requisitos

Se quiser configurar protocolos de privacidade e autenticação SNMP, verifique se você conhece as senhas de autenticação e privacidade para cada usuário que você planeja configurar. As senhas devem ter pelo menos oito caracteres.

Procedimentos

- 1 Faça login no shell do dispositivo como um usuário com privilégios administrativos.
- 2 Execute o comando `vicfg-snmp --engineid` para configurar o destino.

Por exemplo, execute o seguinte comando:

```
vicfg-snmp --engineid 80001f8880167b18238d613d6000000000
```

Em que `80001f8880167b18238d613d6000000000` é o ID, uma cadeia hexadecimal com 5 a 32 caracteres de comprimento.

- 3 (Opcional) Para configurar o protocolo de autenticação, execute o comando `vicfg-snmp --authentication`

Por exemplo, execute o seguinte comando:

```
vicfg-snmp --authentication protocol
```

Em que *protocol* deve ser **none** para nenhuma autenticação, **SHA1**, **SHA256**, **SHA384** ou **SHA512**. Por exemplo, se você quiser definir o protocolo de autenticação como SHA512, deverá executar o seguinte comando.

```
vicfg-snmp --authentication SHA512
```

- 4 (Opcional) Para configurar o protocolo de privacidade, execute o comando `vicfg-snmp --privacy`.

Por exemplo, execute o seguinte comando:

```
vicfg-snmp --privacy protocol
```

Em que *protocol* deve ser **none** para nenhuma privacidade ou **AES128**, **AES192** ou **AES256**. Por exemplo, se você quiser definir o protocolo de privacidade como **AES128**, deverá executar o seguinte comando.

```
vicfg-snmp --privacy AES128
```

- 5 Se estiver usando autenticação, privacidade ou ambas, para gerar os valores de hash de autenticação e privacidade de um usuário, execute o seguinte comando.

```
vicfg-snmp --hashkey authentication-password privacy-password
```

É necessário inserir senhas para *authentication-password* e/ou *privacy-password*, dependendo das suas configurações de autenticação e privacidade. As senhas devem ter pelo menos oito caracteres. Anote as senhas para *authentication-password* e *privacy-password*, pois você precisará delas para configurar um cliente SNMP. A saída do comando inclui as informações de Chave localizada de autenticação e Chave localizada de privacidade.

6 Configure um ou mais usuários executando o seguinte comando.

É possível especificar vários usuários adicionando-os como uma lista separada por vírgulas. Até cinco usuários podem ser configurados.

```
vicfg-snmp --users userid/authhash/privhash/security
```

Os parâmetros no comando são os seguintes.

Parâmetro	Descrição
<i>userid</i>	Substitua pelo nome de usuário.
<i>authhash</i>	Substitua pela chave localizada de autenticação.
<i>privhash</i>	Substitua pela chave localizada de privacidade.
<i>model</i>	Substitua pelo nível de segurança ativado para esse usuário, que pode ser auth , para autenticação somente, priv , para autenticação e privacidade, ou none , para nenhuma autenticação ou privacidade.

Por exemplo, se quiser configurar um usuário sem segurança, execute:

```
vicfg-snmp --users vcd-snmp-user/-/-/none
```

Se quiser configurar um usuário com hash de autorização, execute:

```
vicfg-snmp --users vcd-snmp-user/225e07958d3c6af615588db17d61986e69fb7a71/-/auth
```

Se quiser configurar um usuário com hash de autorização e hash de privacidade, execute:

```
vicfg-snmp --users vcd-snmp-user/225e07958d3c6af615588db17d61986e69fb7a71/da1057af05f67a25a09265a9a2bedb53/priv
```

7 (Opcional) Se quiser excluir um ou mais usuários, repita a etapa 6 com os detalhes do novo usuário.

Uma nova execução de `vicfg-snmp --users` substitui as configurações anteriores.

8 Ative o SNMP executando o seguinte comando.

```
vicfg-snmp --enable
```

Usar `snmpwalk` com o SNMP do VMware Cloud Director

Começando com o VMware Cloud Director 10.2.2, para encadear solicitações do `GETNEXT` sem inserir comandos exclusivos para cada OID ou nó em uma subárvore, você pode executar o comando `snmpwalk`.

Pré-requisitos

- Configure o dispositivo VMware Cloud Director para [Configurar o dispositivo VMware Cloud Director para SNMP v1 e v2c](#) ou [Configurar o dispositivo VMware Cloud Director para SNMP v3](#).

Procedimentos

- 1 Em uma máquina local, verifique se o comando `snmpwalk` está instalado. Se necessário, instale-o.
- 2 Execute o comando `snmpwalk`.

```
snmpwalk -v SNMP_version -l security_level -a authorization_protocol -A
authorization_password -x privacy_protocol -X privacy_password -u username host_IP:port
queried_MIB_OID
```

Em que `-l` é o nível de segurança que você pode definir como `noAuthNoPriv`, `authNoPriv` ou `authPriv`. Para obter ajuda com o comando `snmpwalk`, você pode executar `-h`.

Exemplo: Consulta `snmpwalk`

Uma consulta de amostra do `sysDescr.0` MIB OID pode ter a seguinte aparência:

```
snmpwalk -v 3 -l authPriv -a SHA512 -A myauthpassword -x AES128 -X myprivpassword -u vcd-snmp-
user 192.168.100.187:10161 sysDescr.0
```

Esse comando retorna a seguinte saída.

```
SNMPv2-MIB::sysDescr.0 = STRING: VMware-Cloud-Director-Appliance 10.2.2.5553 generic build
17709283 VMware, Inc x86_64
```

Redefinir as configurações SNMP do dispositivo VMware Cloud Director

No VMware Cloud Director 10.2.2, é possível configurar o agente SNMP do dispositivo VMware Cloud Director. Para limpar todas as configurações SNMP e desativar o agente, redefina as configurações de SNMP do dispositivo.

Pré-requisitos

Configure o dispositivo VMware Cloud Director para [Configurar o dispositivo VMware Cloud Director para SNMP v1 e v2c](#) ou [Configurar o dispositivo VMware Cloud Director para SNMP v3](#).

Procedimentos

- 1 Faça login no shell do dispositivo como um usuário com privilégios administrativos.
- 2 Para retornar todas as configurações SNMP aos seus valores padrão e desativar o agente SNMP, execute o seguinte comando.

```
vicfg-snmp --reset
```

Exibir as configurações SNMP do dispositivo VMware Cloud Director

Começando com o VMware Cloud Director 10.2.2, é possível exibir as configurações de SNMP, por exemplo, porta UDP, comunidades, usuários V3, ID do mecanismo, protocolos de autorização e privacidade e assim por diante.

Pré-requisitos

Configure o dispositivo VMware Cloud Director para [Configurar o dispositivo VMware Cloud Director para SNMP v1 e v2c](#) ou [Configurar o dispositivo VMware Cloud Director para SNMP v3](#).

Procedimentos

- 1 Faça login no shell do dispositivo como um usuário com privilégios administrativos.
- 2 Para exibir as configurações SNMP, execute o seguinte comando.

```
vicfg-snmp --show
```

Exemplo: Amostra da saída de `vicfg-snmp --show`

A amostra de saída mostra que o agente SNMP está ativado para um usuário V3 com um hash de autorização e um hash de privacidade.

```
Current SNMP agent setting
Enabled : true
UDP port : 161
V1/V2c Communities :
V1 Notification targets :
Notification filter oids:
V3 Notification targets :
V3 Users : vcd-snmp-user 225e07958d3c6af615588db17d61986e69fb7a71
da1057af05f67a25a09265a9a2bedb53 authPriv
Contact :
Location :
Engine ID : 80001f8880efbab0540a653e6000000000
Auth Protocol : usmHMACSHAAuthProtocol
Priv Protocol : usmAESCfb128PrivProtocol
Log level : warning
Process ID : 15828
Large Storage Support : False
Simple Application Names: False
INFO: listing complete.
```

Editando as configurações de DNS do dispositivo do VMware Cloud Director

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

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

Pré-requisitos

Para fazer com que as alterações nas propriedades OVF sejam permanentes, você deve usar a interface de usuário do vSphere para alterar os valores da propriedade OVF. Consulte o tópico [Configurar propriedades do vApp no guia *Administração da máquina virtual do vSphere*](#).

Procedimentos

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

- a Faça login diretamente ou usando um cliente SSH no console do dispositivo do VMware Cloud 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 VMware Cloud Director

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

Pré-requisitos

Para fazer com que as alterações nas propriedades OVF sejam permanentes, você deve usar a interface de usuário do vSphere para alterar os valores da propriedade OVF. Consulte o tópico *Configurar propriedades do vApp* no guia *Administração da máquina virtual do vSphere*.

Procedimentos

- 1 Se você quiser alterar o valor da rota estática temporariamente, por exemplo, para fins de teste, edite as rotas estáticas no VMware Cloud Director.
 - a Faça login diretamente ou usando um cliente SSH no console do dispositivo do VMware Cloud 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 VMware Cloud 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 dispositivo do VMware Cloud Director

O appliance VMware Cloud 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 <code>pg_hba.conf</code> . Consulte Configurar o acesso externo ao banco de dados do VMware Cloud Director .

Renovar os certificados do dispositivo VMware Cloud Director

Quando você implanta o dispositivo VMware Cloud 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 VMware Cloud Director individualmente.

O dispositivo VMware Cloud Director usa dois conjuntos de certificados SSL. O serviço VMware Cloud 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 VMware Cloud 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 VMware Cloud 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](#).
- Se o modo FIPS estiver habilitado, a senha **raiz** do dispositivo deverá conter pelo menos 14 caracteres. Consulte [Alterar a senha raiz do dispositivo do VMware Cloud Director](#).

Procedimentos

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

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

- 3 Gere novos certificados autoassinados para a interface de usuário de gerenciamento de banco de dados e dispositivo ou para a comunicação HTTPS e do proxy do console, o banco de dados e a interface de usuário de gerenciamento do dispositivo.

- Gere certificados autoassinados somente para o banco de dados PostgreSQL incorporado e a interface de usuário de gerenciamento do dispositivo do VMware Cloud Director, execute:

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

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.

- Gere novos certificados autoassinados para comunicação HTTPS e do proxy de console do VMware Cloud Director, além de certificados para o banco de dados PostgreSQL incorporado e a interface de usuário de gerenciamento do dispositivo.

- a Execute o seguinte comando:

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

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

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

- c Reinicie o serviço VMware Cloud Director.

```
service vmware-vcd start
```

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 VMware Cloud Director, que são usados no 4.

Resultados

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

O novo certificado PostgreSQL será importado para o truststore do VMware Cloud Director em outras células do VMware Cloud 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.

Substituir um certificado de interface de usuário de gerenciamento do dispositivo VMware Cloud Director e PostgreSQL incorporado autoassinado

Por padrão, o banco de dados PostgreSQL incorporado e a interface do usuário de gerenciamento do dispositivo VMware Cloud 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 VMware Cloud Director, ele gera certificados autoassinados com um período de validade de 365 dias. O dispositivo VMware Cloud Director usa dois conjuntos de certificados SSL. O serviço VMware Cloud 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 VMware Cloud 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 VMware Cloud Director em outras células do VMware Cloud Director da próxima vez em que a função `appliance-sync` for executada. A operação pode demorar até 60 segundos.

Substituir o armazenamento do servidor de transferência para o dispositivo do VMware Cloud Director

Você pode alterar o compartilhamento NFS para o dispositivo do VMware Cloud Director após a implantação.

Procedimentos

- 1 Desative e interrompa o serviço do `vmware-vcd` em todos os dispositivos no grupo de servidores do VMware Cloud Director.

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

- 2 Interrompa o serviço do `appliance-sync.timer` em todos os dispositivos no grupo de servidores.

```
systemctl stop appliance-sync.timer
```

- 3 No dispositivo primário, copie os dados do compartilhamento NFS antigo para o novo.

- a Crie um novo ponto de montagem de compartilhamento NFS.

```
mkdir /opt/vmware/vcloud-director/data/transfer-new/
```

- b Monte o novo compartilhamento do servidor NFS no novo ponto de montagem.

```
mount -t nfs Primary_appliance_IP_address:/data/transfer /opt/vmware/vcloud-director/data/transfer-new
```

- c Copie os arquivos do compartilhamento de transferência antigo para o novo compartilhamento de transferência.

Observação O tempo que leva para copiar os arquivos depende do número de itens de catálogo em cache no compartilhamento de pasta de transferência.

```
cp -R /opt/vmware/vcloud-director/data/transfer/* /opt/vmware/vcloud-director/data/transfer-new/
```

- d Quando você copiar os arquivos com êxito, confirme se o conteúdo do compartilhamento NFS antigo está no novo compartilhamento NFS verificando o conteúdo de `/opt/vmware/vcloud-director/data/transfer-new` ou executando o seguinte comando.

```
diff -r --brief /opt/vmware/vcloud-director/data/transfer/ /opt/vmware/vcloud-director/data/transfer-new/
```

- e Desmonte o novo compartilhamento NFS do ponto de montagem temporário.

```
umount /opt/vmware/vcloud-director/data/transfer-new/
```

- f Exclua o ponto de montagem temporário.

```
rmdir /opt/vmware/vcloud-director/data/transfer-new/
```

- 4 Atualize o arquivo `/etc/fstab`, substituindo a linha NFS pelo caminho para o novo servidor NFS.

```
Primary_appliance_IP_address:/data/transfer_appliance /opt/vmware/vcloud-director/data/transfer/ nfs defaults 0 0
```

- 5 Desmonte o compartilhamento do NFS antigo.

```
umount /opt/vmware/vcloud-director/data/transfer/
```

- 6 Monte o novo compartilhamento NFS.

```
mount -a
```

- 7 Confirme se você montou o compartilhamento NFS com êxito, verificando se a saída do comando `mount` lista o compartilhamento NFS montado.

- 8 Altere a propriedade do diretório de transferência de `root` a `vcloud` usando o seguinte comando.

```
chown -R vcloud:vcloud /opt/vmware/vcloud-director/data/transfer
```

- 9 Reinicie o serviço `appliance-sync.timer`.

```
systemctl start appliance-sync.timer
```

- 10 Repita as etapas de 4 a 9 em todos os nós no grupo de servidores.

- 11 Um nó de cada vez, reinicie o serviço do `vmware-vcd`.

```
systemctl start vmware-vcd
```

- 12 Verifique se o `vmware-vcd` funciona corretamente em todos os nós do grupo de servidores.

Aumentar a capacidade do banco de dados PostgreSQL incorporado em um dispositivo do VMware Cloud Director

Se você não tiver espaço suficiente no disco do banco de dados PostgreSQL de um dispositivo do VMware Cloud 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.

O tamanho do disco do banco de dados PostgreSQL em cada dispositivo em espera deve ser o mesmo que o disco do banco de dados PostgreSQL no dispositivo primário.

Pré-requisitos

- Se o seu ambiente do VMware Cloud 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 [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).
- Se o seu ambiente do VMware Cloud 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 Aplique as alterações ao sistema operacional do nó do dispositivo.

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

```
/opt/vmware/appliance/bin/db_diskresize.sh
```

- 3 Se o seu ambiente não consistir em apenas um dispositivo primário, repita o procedimento para cada um dos nós que tenham um banco de dados.

Modificar as configurações do PostgreSQL no dispositivo do VMware Cloud Director

Você pode alterar as configurações de PostgreSQL do dispositivo do VMware Cloud 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 a operação do cluster requer a substituição periódica do arquivo e as alterações não são persistentes.

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.

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.

Para obter mais informações sobre a API de dispositivo do VMware Cloud Director, consulte a [documentação da API de dispositivo do VMware Cloud Director](#).

Você pode cancelar o registro da célula 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.

Procedimentos

- 1 Para encontrar o nome do nó em espera cujo registro você deseja cancelar, execute o método `NODES` da API de dispositivo do VMware Cloud Director.
- 2 A partir de um dos outros nós, execute o método `UNREGISTER` da API do dispositivo do VMware Cloud Director.

Em que `node-name` é o nome do dispositivo em espera que você deseja remover.

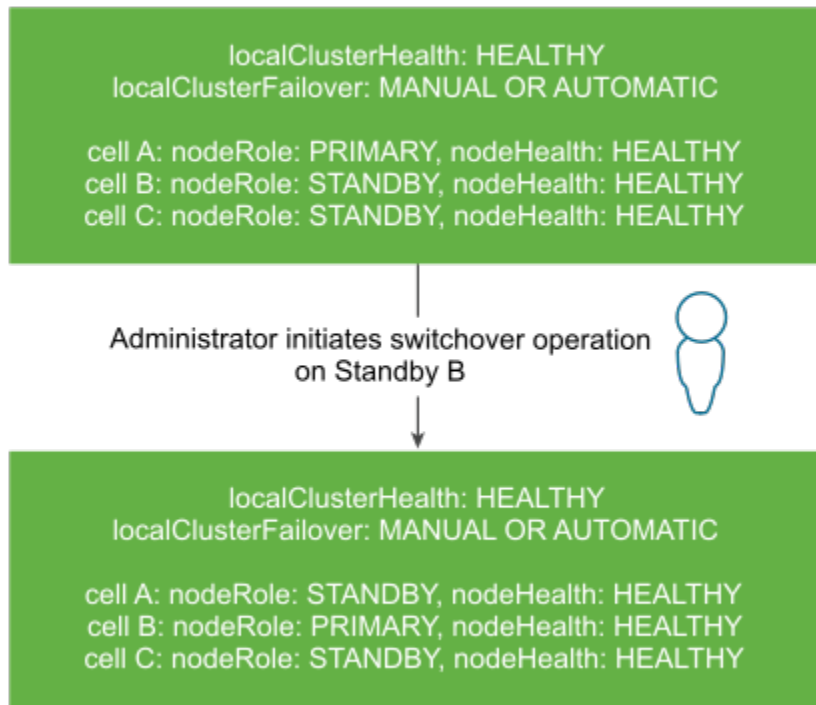
- 3 Para verificar se o nó de espera não registrado não aparece mais no cluster de alta disponibilidade do banco de dados, execute o método de API `NODES`.

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 a interface do usuário de gerenciamento do dispositivo do VMware Cloud Director para alternar as funções das células em um cluster de alta disponibilidade de banco de dados e promover uma célula diferente como a primária.

Você pode alternar as funções da célula primária e de espera usando a interface do usuário de gerenciamento do dispositivo do VMware Cloud Director ou a API do dispositivo do VMware Cloud Director. Este procedimento descreve as etapas para fazer essa alternância, usando a interface do usuário de gerenciamento.

Figura 3-3. Alternância entre uma célula primária e uma célula de espera



Pré-requisitos

- Verifique se todos os nós no cluster estão íntegros e online. Consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

Procedimentos

- 1 Desative as atividades em todas as células do VMware Cloud Director que fazem parte do grupo de servidores ou coloque as células no modo de manutenção.

A alternância faz com que o banco de dados do VMware Cloud Director fique indisponível por 30 a 60 segundos. Para evitar falhas de tarefas inesperadas, você deve desativar a atividade em todas as células no cluster.
- 2 Faça login como **root** na interface do usuário de gerenciamento do dispositivo em `https://primary_eth1_ip_address:5480`.
- 3 No painel esquerdo, selecione **Disponibilidade do Banco de Dados Incorporado**.

Você pode visualizar os nomes das células, suas funções, seu status e o nome da célula que as células de espera estão seguindo.
- 4 Verifique se a integridade do cluster está *Healthy*.
- 5 Clique no botão **Alternância** da célula que você deseja promover como primária e confirme a alternância.
- 6 Quando a tarefa de alternância for concluída, reinicie o agendador ou desative o modo de manutenção para as células no cluster.

Assinar eventos, tarefas e métricas usando um cliente MQTT

Você pode usar um cliente MQTT para assinar mensagens sobre eventos e tarefas do VMware Cloud Director.

O MQTT é um protocolo de transporte de mensagens leve e binário. O VMware Cloud Director usa MQTT para publicar informações sobre eventos e tarefas nos quais você pode assinar usando um cliente MQTT. As mensagens do MQTT passam por um agente do MQTT que também pode armazenar mensagens caso os clientes não estejam online.

Começando com o VMware Cloud Director 10.2.2, é possível usar um cliente MQTT para assinar métricas.

Pré-requisitos

- Verifique se você tem um cliente MQTT que oferece suporte ao WebSocket.
- Verifique se você pode adicionar cabeçalhos a uma solicitação do WebSocket atualizada.
- Se quiser assinar métricas, configure a coleção de métricas e habilite a publicação de métricas. Consulte [Configurar a coleção e a publicação de métricas](#).

Procedimentos

- 1 Faça login no VMware Cloud Director usando o endpoint do OpenAPI.
- 2 Para estabelecer uma conexão WebSocket, defina a propriedade Sec-WebSocket-Protocol como `mqtt`, defina o cliente para se conectar ao caminho `/messaging/mqtt`, adicione um cabeçalho de autorização e siga o fluxo de conexão padrão do MQTT.

Você recebe o token JWT da solicitação de login padrão para o VMware Cloud Director. Você pode deixar o nome de usuário e a senha vazios.

```
Sec-WebSocket-Protocol: mqtt
```

```
Authorization: Bearer {JWT_token}
```

- 3 Quando a conexão for estabelecida com êxito, assine os tópicos por meio do cliente MQTT.

```
publish/{user_org_id}/{user_id}
```

```
publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
```

Os administradores da organização podem usar curingas para acessar todos os tópicos da organização.

```
publish/{user_org_id}/+
```

Os administradores do sistema podem usar curingas para acessar todos os tópicos.

```
publish/#
```

- 4 (Opcional) Para o VMware Cloud Director 10.2.2 ou versões posteriores, assine métricas.

```
metrics/{org_id}/{vApp_id}
```

Somente **administradores do sistema** podem acessar o tópico de métricas.

Grupos de Dimensionamento Automático

Começando com o VMware Cloud Director 10.2.2, você pode permitir que os usuários do tenant dimensionem aplicativos automaticamente, dependendo do uso atual de CPU e memória.

Dependendo de critérios predefinidos para o uso de CPU e memória, os tenants podem usar o VMware Cloud Director para ampliar ou reduzir automaticamente o número de VMs em um grupo de dimensionamento selecionado. Para permitir que os tenants dimensionem aplicativos automaticamente, você deve configurar, publicar e conceder acesso à solução de dimensionamento automático.

Para balancear a carga dos servidores configurados para executar o mesmo aplicativo, você pode usar o VMware NSX Advanced Load Balancer (Avi Networks).

Configurar e publicar o plug-in de dimensionamento automático

Antes de conceder acesso aos tenants, você deve configurar a solução de grupos de dimensionamento automático. O dimensionamento automático pode ser usado a partir do VMware Cloud Director 10.2.2.

- 1 Faça login diretamente ou usando um cliente SSH no sistema operacional de qualquer uma das células no cluster como **root**.
- 2 Ative a coleta de dados de métricas configurando a coleta de métricas em um banco de dados Cassandra ou colete métricas sem persistência de dados de métricas.
 - [Instalar e configurar um banco de dados Cassandra para armazenar dados de métricas de históricos](#)
 - Para coletar dados de métricas sem persistência de dados, execute os seguintes comandos:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.collect.only -v true
```

- 3 Ative a publicação de métricas.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

- 4 Crie um arquivo `metrics.groovy` na pasta `/tmp` com o seguinte conteúdo.

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
    }
}
```

```

        historicInterval=20
        entity="VM"
        instance=""
        minReportingInterval=300
        aggregator="AVERAGE"
    }
}

```

5 Importe o arquivo.

```

$VCLLOUD_HOME/bin/cell-management-tool configure-metrics --metrics-config /tmp/
metrics.groovy

```

6 Se você tiver configurado o Cassandra anteriormente, atualize o esquema Cassandra fornecendo os endereços de nós corretos, os detalhes de autenticação do banco de dados, a porta e o tempo de vida de métricas em dias.

```

$VCLLOUD_HOME/bin/cell-management-tool cassandra -configure -cluster-nodes
nodes_IP_addresses -username cassandra -password cassandra_password -port port_number -ttl
TTL_days -update-schema

```

7 Se você executar a célula com um certificado assinado por CA, para ativar o dimensionamento automático, execute o seguinte comando.

```

$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set enabled=true
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set username=<username>
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --encrypt --set
password=<password>

```

Ao executar o comando no terminal, faça o escape de qualquer caractere especial usando o sinal de barra invertida (\).

8 Reinicie a célula.

```

service vmware-vcd restart

```

9 [Publicar o pacote de direitos de dimensionamento automático.](#)

Publicar o pacote de direitos de dimensionamento automático

Se quiser que os tenants dimensionem aplicativos automaticamente, você deverá publicar o pacote de direitos em uma ou mais organizações do seu sistema. O dimensionamento automático pode ser usado a partir do VMware Cloud Director 10.2.2.

Pré-requisitos

[Configurar e publicar o plug-in de dimensionamento automático](#)

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Pacotes de Direitos**.

- 3 Verifique se não há **Pacotes de Direitos Legados** para as organizações de tenants às quais você deseja conceder acesso para dimensionamento automático.
- 4 Selecione o pacote **vmware:scalegroup Entitlement** e clique em **Publicar**.
- 5 Para publicar o pacote:
 - a Selecione **Publicar em Tenants**.
 - b Selecione as organizações para a qual você deseja publicar a função.
 - Se você quiser publicar o pacote para todas as organizações existentes e recém-criadas no seu sistema, selecione **Publicar para Todos os Tenants**.
 - Se você deseja publicar o pacote para organizações específicas no seu sistema, selecione essas organizações individualmente.
- 6 Clique em **Salvar**.

Próximo passo

Adicione os direitos **VMWARE:SCALEGROUP** necessários para as funções de tenant que você deseja usar para grupos de dimensionamento. Consulte [Exibir e editar uma função de tenant global](#) no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

Monitorando a integridade do cluster do banco de dados do dispositivo do VMware Cloud Director

Você pode monitorar o cluster do dispositivo do VMware Cloud Director usando a interface do usuário de gerenciamento de dispositivo do VMware Cloud Director, a API do dispositivo ou o conjunto de ferramentas de código fonte aberto do repmgr.

Você também pode usar a interface do usuário de gerenciamento do dispositivo do VMware Cloud Director para exibir o modo de failover do dispositivo. O modo de failover indica se o VMware Cloud Director acionará automaticamente um failover de banco de dados se o banco de dados primário falhar, ou se o **administrador do sistema** deve iniciar o failover manualmente.

Se o modo de failover estiver inconsistente entre os nós, o modo de failover será *Indeterminate*. O modo de *Indeterminate* pode levar a estados de clusters inconsistentes entre os nós e os nós seguindo uma célula primária antiga. Você deve diagnosticar o problema e corrigir a situação manualmente.

Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director

Você pode monitorar o status do cluster usando a interface do usuário de gerenciamento do dispositivo do VMware Cloud Director.

Você pode visualizar os nomes das células em um cluster, as funções das células, o status da célula, o nome da célula que as células em espera estão seguindo e o modo de failover do cluster usando a interface de usuário de gerenciamento de dispositivo do VMware Cloud Director ou a API do dispositivo do VMware Cloud Director. Este procedimento descreve as etapas para monitorar a integridade do cluster do dispositivo na interface do usuário de gerenciamento.

Procedimentos

- 1 Faça login como **root** na interface do usuário de gerenciamento do dispositivo em `https://primary_eth1_ip_address:5480`.

- 2 No painel esquerdo, selecione **Disponibilidade do Banco de Dados Incorporado**.

Você pode exibir os nomes DNS curtos dos nós, suas funções, seu status, o nome do respectivo nó upstream, ou seja, o nó primário atual, bem como as ações disponíveis nos nós.

Na coluna **Seguintes**, um ponto de interrogação (?) na frente do nome do host indica que o nó primário atual está inacessível. Um sinal de exclamação (!) na frente do nome do host indica que os metadados do nó primário atual não estão atualizados e podem estar incorretos ou que o nó não está conectado ao nó primário atual. O problema poderá ocorrer se você reiniciar o nó após um tempo de inatividade prolongado. Se o nó não puder se conectar ao nó principal, você deverá cancelar o registro dele e substituí-lo por um novo em espera.

- 3 Visualize a integridade do cluster.

Status de Integridade do Cluster	Descrição
Healthy	O cluster está em um estado íntegro. A célula primária e ambas as células de espera estão online e operacionais. A interface do usuário e a API do VMware Cloud Director estão funcionais.
Degraded	O cluster está em um estado degradado. As células primária e uma das células de espera estão online e operacionais, mas a outra célula de espera não está funcional. O banco de dados primário está funcionando nesse estado, mas, se houver outra falha de banco de dados de qualquer uma das células operacionais, o primário não se tornará não funcional. A célula de espera não funcional deve ser substituída por uma nova célula de espera em funcionamento o mais rápido possível para restaurar o cluster para um estado Healthy . A interface do usuário e a API do VMware Cloud Director estão funcionais.

Status de Integridade do Cluster	Descrição
No_Active_Primary	<p>Não há banco de dados primário operacional. Se houver duas células de espera operacionais, uma delas deverá ser promovida para se tornar a nova célula primária. Se o ambiente não tiver duas células de espera operacionais, você deverá diagnosticar o problema e corrigir a situação manualmente.</p> <p>A interface do usuário e a API do VMware Cloud Director estão não estão disponíveis.</p>
Read_Only_Primary	<p>Existe um banco de dados primário online, mas ele é <code>Read_Only</code> porque o ambiente não tem uma célula de espera operacional. Duas novas células de espera devem ser implantadas.</p> <p>A interface do usuário e a API do VMware Cloud Director estão não estão disponíveis.</p>
Critical_Problem	<p>O cluster está em um estado inconsistente. Por exemplo, mais de uma célula primária está online ou uma célula de espera está seguindo a célula primária errada. Você deve diagnosticar o problema e corrigir a situação manualmente.</p> <p>Esse estado pode afetar a disponibilidade da interface do usuário e da API do VMware Cloud Director.</p>
SSH_Problem	<p>O problema do SSH indica que o usuário postgres não pode se conectar aos seus nós de banco de dados peer via SSH. Você deve corrigir esse problema crítico o mais rápido possível. Consulte A integridade do cluster indica um problema de SSH.</p> <p>A UI e a API do VMware Cloud Director podem não estar totalmente funcionais.</p>

4 Visualize o modo de failover do dispositivo.

Modo de failover	Descrição
Automático	Se ocorrer uma falha no banco de dados primário, o VMware Cloud Director acionará automaticamente um failover de banco de dados.
Manual	Se ocorrer uma falha no banco de dados primário, você deverá iniciar um failover de banco de dados usando a interface do usuário de gerenciamento de dispositivo do VMware Cloud Director ou a API de failover.
Indeterminado	O modo de failover não é consistente em todos os nós do cluster. Você deve diagnosticar o problema e corrigir a situação. Usando a API do dispositivo do VMware Cloud Director, redefina o <code>FailoverMode</code> como <code>Manual</code> ou <code>Automatic</code> . Consulte as informações do <i>Modo de Failover</i> no <i>Referência de esquemas de API do dispositivo do VMware Cloud Director</i> .

Exibir o status do serviço do dispositivo do VMware Cloud Director

Você pode monitorar o status dos serviços do dispositivo do VMware Cloud Director usando a interface de usuário de gerenciamento do dispositivo do VMware Cloud Director.

Na guia **Serviços**, você pode monitorar os serviços `vmware-vcd`, `vpostgres` e `appliance-sync.timer` para dispositivos primários e em espera, além dos serviços `vmware-vcd` e `appliance-sync.timer` para as células do aplicativo.

O serviço `appliance-sync.timer` executa periodicamente o `appliance-sync.service` que compartilha informações relevantes entre todos os nós no cluster de HA do banco de dados ou no grupo de servidores do VMware Cloud Director. O `appliance-sync.service` executa uma verificação periódica e uma sincronização dos arquivos necessários para a funcionalidade do dispositivo do VMware Cloud Director, lendo e gravando os arquivos de configuração dos dispositivos no grupo de dispositivos. Os estados de integridade do temporizador são `waiting` e `running`.

Procedimentos

- 1 Faça login como **root** na interface do usuário de gerenciamento do dispositivo em `https://primary_eth1_ip_address:5480`.
- 2 No painel esquerdo, selecione a guia **Serviços**.
- 3 Exiba o status dos serviços do VMware Cloud Director.

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 para o primário fornece informações sobre o nó, a versão PostgreSQL e os detalhes da replicação. Por exemplo:

```
Node "bos1-vcloud-static-161-5":  
  PostgreSQL version: 10.9  
  Total data size: 81 MB  
  Conninfo: host=172.18.36.193 user=repmgr dbname=repmgr connect_timeout=2  
  Role: primary  
  WAL archiving: off  
  Archive command: (none)  
  Replication connections: 2 (of maximal 10)  
  Replication slots: 0 physical (of maximal 10; 0 missing)  
  Replication lag: n/a
```

A saída do sistema para um nó em espera fornece informações sobre o nó, a versão do PostgreSQL, os detalhes da replicação e um nó superior. Por exemplo:

```
Node "bos1-vcloud-static-161-49":  
  PostgreSQL version: 10.9  
  Total data size: 83 MB  
  Conninfo: host=172.18.36.191 user=repmgr dbname=repmgr connect_timeout=2  
  Role: standby  
  WAL archiving: off  
  Archive command: (none)  
  Replication connections: 0 (of maximal 10)  
  Replication slots: 0 physical (of maximal 10; 0 missing)  
  Upstream node: bos1-vcloud-static-161-48 (ID: 683)  
  Replication lag: 0 seconds  
  Last received LSN: 2/D863B4E0  
  Last replayed LSN: 2/D863B4E0
```

- 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>select* from pg_stat_replication;</code>
Execute uma consulta em um nó em espera.	<code>select* from pg_stat_wal_receiver;</code>

Verificar o status dos serviços do VMware Cloud Director

É possível usar a interface do usuário de gerenciamento do dispositivo do VMware Cloud Director para exibir o status dos serviços do VMware Cloud Director para a célula na qual você está conectado.

Procedimentos

- 1 Faça login como **root** na interface do usuário de gerenciamento do dispositivo em `https://primary_eth1_ip_address:5480`.
- 2 Para exibir o status dos serviços, no painel esquerdo, selecione **Serviços**.

Se o dispositivo do VMware Cloud Director estiver funcionando corretamente, isso significará que os serviços do `vmware-vcd` e do `vpostgres` estão em execução.

Próximo passo

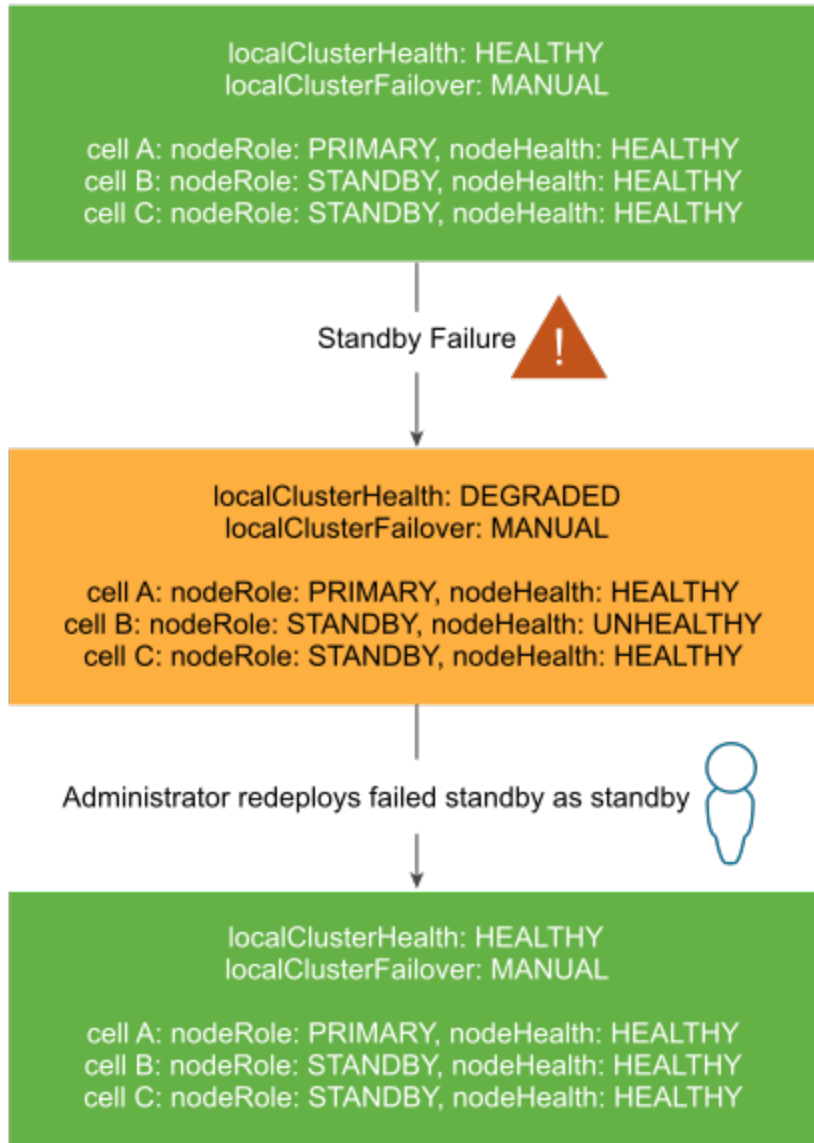
Se você precisar verificar o status do serviço `repmgrd` para fins de depuração, deverá usar a API do dispositivo do VMware Cloud Director.

Recuperação de clusters de banco de dados de dispositivo do VMware Cloud Director

Se houver uma falha com o banco de dados ou um dos nós do VMware Cloud Director, você poderá recuperar seu cluster de banco de dados.

Se uma célula no cluster de alta disponibilidade de banco de dados falhar, o status de funcionamento desse cluster indicará qual é a falha e como você pode resolver o problema. Por exemplo, a integridade do cluster *Degraded* indica uma falha com uma célula de espera. Um administrador do sistema deve reimplantar a célula com falha.

Figura 3-4. Recuperar-se de uma falha de célula de espera



Se uma célula primária no cluster de alta disponibilidade do banco de dados falhar, a integridade do cluster poderá mudar para *No_Active_Primary*, o que indica que um administrador do sistema deve reparar a célula primária que falhou.

Recuperar de uma falha de célula primária em um cluster de alta disponibilidade

Se a célula primária não estiver funcionando corretamente, para recuperar o banco de dados do VMware Cloud Director, uma das células em espera deverá se tornar a nova célula primária e você deverá implantar uma nova em espera. Dependendo do modo de falha, o dispositivo do VMware Cloud Director promove automaticamente uma célula em espera como a nova primária ou você deve promovê-la manualmente.

Dependendo do modo de failover do dispositivo VMware Cloud Director, existem dois fluxos de trabalho diferentes para a recuperação de uma falha de célula primária. Você pode usar esses fluxos de trabalho para reutilizar os endereços IP e o nome do host da célula primária com falha ao implantar a nova célula em espera.

Fluxo de trabalho de recuperação para o modo de failover manual

Se a célula primária estiver no estado `Not reachable` ou `Failed`, e as duas células em espera estiverem no estado `Running`, você poderá se recuperar da falha usando a interface de usuário HTML5 do dispositivo e a API do dispositivo VMware Cloud Director.

Para exibir o estado das células no cluster, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

- 1 Usando a ferramenta de gerenciamento de células, se possível, encerre o processo VMware Cloud Director. Na célula primária com falha, execute o seguinte comando

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <sysadmin user> cell --shutdown
```

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

A UI de gerenciamento mostra duas células com a função `primária`. A primária original tem um status com falha e a nova primária tem um status em execução. A integridade do cluster é Degradado.

- 4 Em qualquer célula diferente da primária com falha, usando o método `Unregister` da API do dispositivo, remova o dispositivo primário com falha do cluster de alta disponibilidade repmgr. Consulte a documentação da [API do dispositivo do VMware Cloud Director](#).
- 5 Remova o dispositivo principal com falha do grupo de servidores do VMware Cloud Director.
 - a Faça login como **administrador** no Service Provider Admin Portal.
 - b Na barra de navegação superior, em **Recursos**, selecione **Recursos de Nuvem**.
 - c No painel esquerdo, clique em **Células da Nuvem**.

- d Selecione a célula inativa e clique em **Cancelar registro**.
- 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 use o vSphere Client para excluí-lo.
- 7 Implante um novo appliance em espera. Você pode [Iniciar a implantação do dispositivo do VMware Cloud Director](#) ou pode [Implantação do dispositivo VMware Cloud Director usando o VMware OVF Tool](#).

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

- 8 Se o modo FIPS do dispositivo VMware Cloud Director estava ativo antes da restauração, você deve defini-lo novamente usando a API do dispositivo VMware Cloud Director.

O modo FIPS da célula é restaurado automaticamente.

Recuperação para o modo de failover automático

Se a primária estiver no estado *Failed*, o VMware Cloud Director promoverá automaticamente uma célula em espera como a nova primária em execução, mas o cluster estará no estado *Degradado*, pois há apenas uma célula em espera em execução. Você poderá se recuperar da falha usando a interface de usuário do HTML5 e a API do dispositivo do VMware Cloud Director.

Para exibir o estado das células no cluster, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

- 1 Se possível, usando a ferramenta de gerenciamento de células, encerre o processo VMware Cloud Director. Na célula primária com falha, execute o seguinte comando

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <sysadmin user> cell --shutdown
```

- 2 Desligue a VM primária com falha.

A UI de gerenciamento mostra duas células com a função *primária*. A primária original tem um status com *falha* e a nova primária tem um status em *execução*. A integridade do cluster é *Degradado*.

- 3 Em qualquer célula diferente da primária com falha, usando o método *Unregister* da API do dispositivo, remova o dispositivo primário com falha do cluster de alta disponibilidade repmgr. Consulte a documentação da [API do dispositivo do VMware Cloud Director](#).
- 4 Remova o dispositivo principal com falha do grupo de servidores do VMware Cloud Director.
 - a Faça login como **administrador** no Service Provider Admin Portal.
 - b Na barra de navegação superior, em **Recursos**, selecione **Recursos de Nuvem**.
 - c No painel esquerdo, clique em **Células da Nuvem**.
 - d Selecione a célula inativa e clique em **Cancelar registro**.

- 5 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 esteja desligado ou use o vSphere Client para excluí-lo.
- 6 Implante um novo appliance em espera. Você pode [Iniciar a implantação do dispositivo do VMware Cloud Director](#) ou pode [Implantação do dispositivo VMware Cloud Director usando o VMware OVF Tool](#). Após a implantação da nova célula em espera, o estado do cluster deve ser `Íntegro`.
- 7 Em qualquer célula diferente da célula primária com falha, use o método `Failover` da API do dispositivo para redefinir o modo de failover do cluster como `Automatic`. Consulte a documentação da [API do dispositivo do VMware Cloud Director](#).
- 8 Se o modo FIPS do dispositivo VMware Cloud Director estava ativo antes da restauração, você deve defini-lo novamente usando a API do dispositivo VMware Cloud Director.

O modo FIPS da célula é restaurado automaticamente.

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 `Not reachable` ou `Failed`, você poderá implantar uma nova célula. Para exibir o estado das células no cluster, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

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 VMware Cloud 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 Em qualquer célula diferente da em espera com falha, usando o método `Unregister` da API do dispositivo, remova a célula em espera com falha do cluster de alta disponibilidade `repmgr`. Consulte a documentação da [API do dispositivo do VMware Cloud Director](#).
- 4 Use o Service Provider Admin Portal para remover o dispositivo em espera com falha do grupo de servidores do VMware Cloud Director.
 - a Na barra de navegação superior, em **Recursos**, selecione **Recursos de Nuvem**.
 - b No painel esquerdo, clique em **Células da Nuvem**.
 - c Selecione uma célula inativa e clique em **Cancelar registro**.
- 5 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.

- 6 Implante um novo appliance em espera. Você pode [Iniciar a implantação do dispositivo do VMware Cloud Director](#) ou pode [Implantação do dispositivo VMware Cloud Director usando o VMware OVF Tool](#).

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

- 7 Para redefinir o modo de failover do cluster para *Automatic*, em qualquer célula diferente da célula em espera com falha, use o método `Failover` da API do dispositivo. Consulte a documentação da [API do dispositivo do VMware Cloud Director](#).

Para obter mais informações sobre o modo de failover automático, consulte [Failover automático do dispositivo do VMware Cloud Director](#).

- 8 Se o modo FIPS do dispositivo VMware Cloud Director estava ativo antes da restauração, você deve defini-lo novamente usando a API do dispositivo VMware Cloud Director.

O modo FIPS da célula é restaurado automaticamente.

Cancelar o registro de uma célula primária ou em espera com falha em um cluster de alta disponibilidade de banco de dados

Se o nó primário ou em espera no cluster de alta disponibilidade de banco de dados falhar, você poderá usar a API do VMware Cloud Director para cancelar o registro do nó com falha para removê-lo do cluster e evitar dados de status de cluster inconsistentes.

Para obter mais informações sobre como usar a API do VMware Cloud Director, consulte o método de API do `UNREGISTER` na documentação da API do Dispositivo do VMware Cloud Director em <https://developer.vmware.com/>.

Pré-requisitos

- Verifique se o nó cujo registro você deseja cancelar está inativo e anote seu nome. Para obter informações sobre o status das células e o nome da célula que as células em espera estão seguindo, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).
- Se quiser cancelar o registro de um nó primário, verifique se o primário com falha está inativo e sem qualquer um dos seguintes nós em espera e promova um novo primário.

Procedimentos

- ◆ Para remover o nó inativo, faça uma solicitação `DELETE` em um nó ativo no qual o comando será executado.

```
DELETE https://<Active_Node_FQDN>:5480/api/1.0.0/nodes/<Inactive_Node_Name>
```

Solucionando problemas do dispositivo

Se a implantação do appliance VMware Cloud 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 VMware Cloud Director. Para obter mais informações sobre como coletar informações de diagnóstico para o VMware Cloud 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>.

Examinar os arquivos de log no VMware Cloud Director Appliance

Depois de implantar o VMware Cloud Director Appliance, 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 usando um cliente SSH no console do dispositivo do VMware Cloud 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 VMware Cloud Director não é iniciada após a implantação do dispositivo

Você implantou o appliance VMware Cloud Director com êxito, mas os serviços VMware Cloud 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 VMware Cloud 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 VMware Cloud 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`.

Observação Se o cluster estiver configurado para failover automático, depois de implantar uma ou mais células adicionais, você deverá usar a API do Dispositivo para redefinir o modo de failover do cluster para o `Automatic`. Consulte a [API do dispositivo do VMware Cloud Director](#). O modo de failover padrão para novas células é `Manual`. Se o modo de failover estiver inconsistente em todos os nós do cluster, o modo de failover do cluster será `Indeterminate`. O modo de `Indeterminate` pode levar a estados de clusters inconsistentes entre os nós e os nós seguindo uma célula primária antiga. Para exibir o modo de failover do cluster, consulte [Visualizar o modo de integridade e failover do cluster do dispositivo do VMware Cloud Director](#).

Solução

- 1 Faça login diretamente ou usando um cliente SSH no console do dispositivo do VMware Cloud 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.

Recuperando após a validação do NFS falhar durante a configuração inicial do dispositivo

Se a validação de armazenamento compartilhado falhar durante a configuração inicial do dispositivo do VMware Cloud Director, o implantador exibirá mensagens de erro que você pode usar para corrigir o problema.

Problema

Durante a implantação do dispositivo do VMware Cloud Director, o implantador exibe uma mensagem de erro referente ao compartilhamento do NFS.

Causa

Se você não preparar o armazenamento do servidor de transferência para o VMware Cloud Director, a validação do NFS durante a implantação falhará.

Solução

Versão	Erro	Ação
10.2	<code>/opt/vmware/vcloud-director/data/transfer/xyz</code> pertence a um usuário desconhecido com UID 999; esperado 1003	Verifique a configuração de ID do usuário do vcloud no servidor NFS. O ID de usuário do vcloud deve ter o mesmo valor no servidor NFS e no dispositivo.
10.2	<code>/opt/vmware/vcloud-director/data/transfer/xyz</code> pertence a um usuário desconhecido com GID 999; esperado 1002	Verifique a configuração de ID do grupo do usuário do vcloud no servidor NFS. O ID de usuário do vcloud deve ter o mesmo valor no servidor NFS e no dispositivo.
10.2	Não é possível tocar o arquivo no <code>transfershare</code>	Determine por que o dispositivo não pode gravar no compartilhamento do NFS montado. Para confirmar por que ele não é gravável, tente montar o compartilhamento do NFS usando outra máquina Linux.
10.2	Tempo limite encontrado durante <code>/usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test</code> . Duração: 5 segundos	Determine por que este dispositivo não pode montar o compartilhamento do NFS especificado dentro de 5 segundos. Para confirmar se o compartilhamento do NFS não pode ser montado em tempo hábil, tente montá-lo usando outra máquina Linux. Como alternativa, verifique as configurações de exportação do servidor NFS para este compartilhamento do NFS.
10.2	Erro encontrado durante <code>/usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test</code>	Determine por que este dispositivo não pode montar o compartilhamento do NFS especificado. Para confirmar se o compartilhamento do NFS não pode ser montado, tente montá-lo usando outra máquina Linux. Como alternativa, verifique as configurações de exportação do servidor NFS para este compartilhamento do NFS.
10.2	O diretório de compartilhamento de transferência não existe: <code>/opt/vmware/vcloud-director/data/transfer</code>	O diretório de compartilhamento de transferência ou o ponto de montagem não existe. Crie esse diretório.

Versão	Erro	Ação
10.2	Permissões inesperadas no arquivo <code>/opt/vmware/vcloud-director/data/transfer/xyz</code> ao executar a operação: toque em xyz. Esperado: raiz raiz 644. Encontrado: raiz, raiz, 600	Determine por que o proprietário do arquivo, o grupo ou as permissões diferem dos valores esperados depois de executar a operação especificada no compartilhamento de transferência do NFS e corrija o problema.
10.2	O relógio do servidor NFS está fora de sincronia em relação ao relógio do dispositivo. Diferença de tempo: 3 minutos e 12 segundos	Verifique as configurações de hora no servidor NFS e no dispositivo. Se um ou ambos não forem precisos, configure-os para o horário correto e certifique-se de que estejam sincronizados usando o NTP.
10.2	Permissões inesperadas no arquivo <code>/opt/vmware/vcloud-director/data/transfer/xyz</code> ao executar a operação: <code>chmod xyz</code> . Esperado: raiz raiz 750. Encontrado: raiz, raiz, 700	Determine por que o proprietário do arquivo, o grupo ou as permissões diferem dos valores esperados depois de executar a operação especificada no compartilhamento de transferência do NFS e corrija o problema.
10.2	Permissões inesperadas no arquivo <code>/opt/vmware/vcloud-director/data/transfer/xyz</code> ao executar a operação: <code>chown xyz</code> . Esperado: raiz raiz 750. Encontrado: raiz, raiz, 700	Determine por que o proprietário do arquivo, o grupo ou as permissões diferem dos valores esperados depois de executar a operação especificada no compartilhamento de transferência do NFS e corrija o problema.
10.2 e posterior	Argumentos de comando inválidos ou ausentes. uso: <code>nfsValidate nfs_mount_string</code>	O corpo da solicitação JSON não pode ser analisado. Forneça um corpo da solicitação JSON válido.
10.2 e posterior	Cadeia de caracteres <code>nfs_mount</code> vazia	A cadeia de caracteres de montagem do NFS não está no corpo da solicitação. Forneça um argumento de cadeia de caracteres de montagem do NFS.
10.2 e posterior	Cadeia de caracteres <code>nfs_mount</code> inválida: <code>nfs_mount_string_argument</code>	Altere a cadeia de caracteres de montagem do NFS para o formato válido <code>IP_address:path</code>
10.2 e posterior	Tipo de célula inválido: <code>cell_type_string</code>	O tipo de célula deve ser <code>primary</code> , <code>standby</code> ou <code>cell</code> . Se o parâmetro OVF não for igual a qualquer um desses valores, verifique a configuração do dispositivo.
10.2 e posterior	A configuração do sistema operacional de pré-requisito não foi concluída	O arquivo <code>/opt/vmware/appliance/etc/os-configuration-completed</code> está faltando no dispositivo. Configure o sistema operacional.

Versão	Erro	Ação
10.2 e posterior	A configuração do sistema do dispositivo do Cloud Director já foi concluída.	O arquivo <code>/opt/vmware/appliance/etc/vcd-configuration-completed</code> foi encontrado no dispositivo. A configuração do diretório de nuvem já está concluída e você não deve executar esse script.
10.2 e posterior	O diretório <code>10.150.170.3:/data/transfer/cells</code> já existe. O dispositivo primário exige que este seja removido.	Esse diretório não deve existir no dispositivo primário. O diretório existe no servidor NFS e você deve removê-lo.
10.2 e posterior	O diretório <code>10.150.170.3:/data/transfer/appliance-nodes</code> já existe. O dispositivo primário exige que este seja removido.	Esse diretório não deve existir no dispositivo primário. O diretório existe no servidor NFS e você deve removê-lo.
10.2 e posterior	O arquivo <code>responses.properties</code> já existe no compartilhamento de transferência. O dispositivo primário exige que este seja removido.	No dispositivo primário, os arquivos <code>responses.properties</code> não devem existir e você deve removê-los.
10.2 e posterior	O arquivo <code>responses.properties</code> não existe no compartilhamento de transferência. Isso já deve existir em um dispositivo de espera ou de célula.	Em um dispositivo de espera ou de célula, o arquivo <code>responses.properties</code> deve existir. O dispositivo primário não pode ser configurado ainda. Você deve configurar o dispositivo primário antes de configurar células adicionais.
10.2 e posterior	<code>nfsValidate</code> não poderá ser executado enquanto a configuração do sistema estiver em andamento.	Aguarde até que a configuração do sistema seja concluída antes de tentar executar <code>nfsValidate</code> .
10.2 e posterior	Não é possível criar o diretório <code>tmp</code> para uso por este script: <code>/opt/vmware/vcloud-director/data/nfs-test</code>	Verifique as permissões do sistema de arquivos para determinar por que este diretório não pode ser criado.
10.2.1	Não é possível criar o arquivo no compartilhamento NFS fornecido. Ele pode não ser gravável. Isso pode ser devido ao fato de que o sistema de arquivos NFS exportado é somente leitura ou <code>no_root_squash</code> não foi especificado	Determine por que o dispositivo não pode gravar no compartilhamento do NFS montado. Para confirmar por que ele não é gravável, tente montar o compartilhamento do NFS usando outra máquina Linux.

Versão	Erro	Ação
10.2.1	Não é possível executar o <code>chmod</code> no arquivo no <code>transfershare</code> fornecido	Determine por que o dispositivo não pode alterar as permissões de acesso de objetos do sistema de arquivos no compartilhamento NFS montado. Tente montar o compartilhamento do NFS usando outra máquina Linux.
10.2.1	Não é possível executar o <code>chown</code> no arquivo no <code>transfershare</code> fornecido	Determine por que o dispositivo não pode alterar o proprietário dos objetos do sistema de arquivos no compartilhamento NFS montado. Tente montar o compartilhamento do NFS usando outra máquina Linux.
10.2.1	Tempo limite encontrado durante a montagem	Determine por que este dispositivo não pode montar o compartilhamento do NFS especificado dentro de 5 segundos. Para confirmar se o compartilhamento do NFS não pode ser montado em tempo hábil, tente montá-lo usando outra máquina Linux. Como alternativa, verifique as configurações de exportação do servidor NFS para este compartilhamento do NFS.
10.2.1	Erro encontrado durante a montagem	Determine por que este dispositivo não pode montar o compartilhamento do NFS especificado. Para confirmar se o compartilhamento do NFS não pode ser montado, tente montá-lo usando outra máquina Linux. Como alternativa, verifique as configurações de exportação do servidor NFS para este compartilhamento do NFS.
10.2.1	O compartilhamento NFS fornecido é de propriedade de um usuário desconhecido com UID 123; raiz esperada O compartilhamento NFS fornecido é de propriedade de um grupo desconhecido com GID 456; raiz esperada	Determine por que o proprietário do arquivo e/ou o grupo esperados diferem dos valores esperados depois de executar a operação especificada no compartilhamento de transferência do NFS e corrija o problema.

Versão	Erro	Ação
10.2.1	Propriedade e/ou permissões inesperadas no compartilhamento NFS fornecido. Esperado: root:root com modo: 750. Encontrado: root:root com modo 777	Determine por que alguns ou todos os valores esperados para o proprietário do arquivo, o grupo e o modo não são como esperado após a realização da operação especificada no compartilhamento de transferência NFS. Corrija o problema.
10.2.1	O relógio do servidor NFS está fora de sincronia em relação ao relógio do dispositivo. A diferença de tempo é: 1:55:14.603510	Verifique as configurações de hora no servidor NFS e no dispositivo. Se um ou ambos não forem precisos, configure-os para o horário correto e certifique-se de que estejam sincronizados usando o NTP.

A reconfiguração do serviço do VMware Cloud Director falha ao migrar ou restaurar para o dispositivo VMware Cloud Director

Quando você está migrando ou restaurando para o dispositivo do VMware Cloud Director, a execução do comando `configure` pode falhar.

Problema

Durante o procedimento para migrar ou restaurar o VMware Cloud Director para um novo ambiente de dispositivo do VMware Cloud Director, execute o comando `configure` para reconfigurar o serviço VMware Cloud 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`.

Um nó em espera de dispositivo do VMware Cloud Director torna-se inacessível

O VMware Cloud Director mantém a replicação síncrona de streaming entre os nós. Se um nó em espera ficar inacessível, você deverá determinar a causa e resolver o problema.

Problema

A UI de gerenciamento de dispositivo do VMware Cloud Director mostra a integridade do cluster como `DEGRADED`, e o status de um dos nós em espera é `inacessível`.

A API `/nodes` retorna informações de que `localClusterHealth` está `DEGRADED`, o status do nó é ? inacessível e `nodeHealth` é `UNHEALTHY`.

Por exemplo, a API `/nodes` pode retornar as seguintes informações para o nó.

```
{
  "localClusterFailover": "MANUAL",
  "localClusterHealth": "DEGRADED",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
          "status": "NOT APPLICABLE"
        }
      },
      "id": primary_node_ID,
      "location": "default",
      "name": "primary_host_name",
      "nodeHealth": "HEALTHY",
      "nodeRole": "PRIMARY",
      "role": "primary",
      "status": "* running",
      "upstream": ""
    },
    {
      "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover state unknown - unable to ssh to failed or unreachable
node",
        "mode": "UNKNOWN",
        "repmgrd": {
          "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = n/a",
          "status": "UNKNOWN"
        }
      },
      "id": unreachable_standby_node_ID,
      "location": "default",
      "name": "unreachable_standby_host_name",
      "nodeHealth": "UNHEALTHY",
      "nodeRole": "STANDBY",
      "role": "standby",
      "status": "? unreachable",
      "upstream": "primary_host_name"
    },
    {
      "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
```

```

    "failover": {
      "details": "failover = manual",
      "mode": "MANUAL",
      "repmgrd": {
        "details": "On node running_standby_node_ID (running_standby_host_IP):  
repmgrd = not applicable",
        "status": "NOT APPLICABLE"
      }
    },
    "id": running_standby_node_ID,
    "location": "default",
    "name": "running_standby_host_name",
    "nodeHealth": "HEALTHY",
    "nodeRole": "STANDBY",
    "role": "standby",
    "status": "running",
    "upstream": "primary_host_name"
  }
],
"warnings": [
  "unable to connect to node \"unreachable_standby_host_name\" (ID:  
unreachable_standby_node_ID) ",
  "node \"unreachable_standby_host_name\" (ID: unreachable_standby_node_ID) is  
registered as an active standby but is unreachable"
]
}

```

Causa

Para garantir a integridade dos dados, o banco de dados PostgreSQL usa o WAL (Write-Ahead Logging). O nó primário transmite o WAL constantemente aos nós ativos em espera para fins de replicação e recuperação. Os nós em espera processam o WAL quando o recebem. Se um nó em espera estiver inacessível, ele deixará de receber o WAL e não poderá ser um candidato para se tornar um novo nó primário.

Solução

- ◆ Verifique se a máquina virtual do nó em espera inacessível está em execução.
- ◆ Verifique se a conexão de rede com o nó em espera está funcionando.
- ◆ Verifique se não há problemas de SSH que possam impedir que o nó em espera se comunique com os outros nós.
- ◆ Verifique se o serviço `vpostgres` no nó em espera está em execução.

Próximo passo

Para verificar se não há problemas de rede ou SSH, consulte [Verificar o status de conectividade de um cluster de alta disponibilidade de banco de dados](#).

Um nó em espera de dispositivo do VMware Cloud Director torna-se desconectado

O VMware Cloud Director mantém a replicação síncrona de streaming entre os nós. Se um nó em espera ficar desconectado, você deverá determinar a causa e resolver o problema.

Problema

A UI de gerenciamento de dispositivo do VMware Cloud Director mostra a integridade do cluster como `DEGRADED`, o status de um dos nós em espera desconectados é em `execução` e há um ponto de exclamação (!) antes do nome do nó upstream do nó em espera.

O log do PostgreSQL mostra que o nó primário excluiu um segmento de WAL.

```
2020-10-08 04:10:50.064 UTC [13390] LOG:  started streaming WAL from primary at 21/80000000
on timeline 17
2020-10-08 04:10:50.064 UTC [13390] FATAL:  could not receive data from WAL stream: ERROR:
requested WAL segment 0000001100000002100000080 has already been removed
2020-10-08 04:10:55.047 UTC [13432] LOG:  started streaming WAL from primary at 21/80000000
on timeline 17
2020-10-08 04:10:55.047 UTC [13432] FATAL:  could not receive data from WAL stream: ERROR:
requested WAL segment 0000001100000002100000080 has already been removed
```

A API `/nodes` retorna informações de que `localClusterHealth` está `DEGRADED`, o status do nó é em `execução` e `nodeHealth` é `HEALTHY`. Há um ponto de exclamação (!) antes do nome do nó upstream do nó em espera, e a API `/nodes` retorna um aviso de que o nó em espera não está conectado ao seu nó upstream.

Por exemplo, a API `/nodes` pode retornar as seguintes informações para o nó.

```
{
  "localClusterFailover": "MANUAL",
  "localClusterHealth": "DEGRADED",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
          "status": "NOT APPLICABLE"
        }
      },
      "id": primary_node_ID,
      "location": "default",
      "name": "primary_host_name",
      "nodeHealth": "HEALTHY",
      "nodeRole": "PRIMARY",
      "role": "primary",
      "status": "* running",
```

```

        "upstream": ""
    },
    {
        "connectionString": "host=unattached_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node unattached_standby_node_ID
(unattached_standby_host_name): repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": unattached_standby_node_ID,
        "location": "default",
        "name": "unattached_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "! upstream_host_name"
    },
    {
        "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": running_standby_node_ID,
        "location": "default",
        "name": "running_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "upstream_host_name"
    }
],
"warnings": [
    "node \"unattached_standby_host_name\" (ID: unattached_standby_node_ID) is not
attached to its upstream node \"upstream_host_name\" (ID: upstream_node_id)"
]
}

```

Se um nó em espera se tornar desconectado, você deverá reconectá-lo o mais rápido possível. Se o nó permanecer desconectado por muito tempo, ele poderá ficar para trás no processamento dos registros de WAL em streaming contínuo do nó primário, a ponto de talvez que não seja possível para ele retomar a replicação.

Causa

Para garantir a integridade dos dados, o banco de dados PostgreSQL usa o WAL (Write-Ahead Logging). O nó primário transmite o WAL constantemente aos nós ativos em espera para fins de replicação e recuperação. Os nós em espera processam o WAL quando o recebem. Se um nó em espera ficar desconectado, ele deixará de receber o WAL e não poderá ser um candidato para se tornar um novo nó primário.

Solução

- 1 Implante um novo nó em espera.
- 2 Cancele o registro do nó em espera desconectado.

Próximo passo

Consulte [Recuperar de uma falha de célula em espera em um cluster de alta disponibilidade](#).

A integridade do cluster indica um problema de SSH

Em uma implantação de dispositivo VMware Cloud Director com configuração de HA do banco de dados, o usuário **postgres** não pode se conectar aos seus nós de banco de dados peer via SSH.

Problema

Quando há um problema de SSH entre os nós de banco de dados, o VMware Cloud Director mostra `localClusterHealth` como `SSH_PROBLEM`. Você deve corrigir esse problema crítico o mais rápido possível.

É possível exibir `localClusterHealth` usando a interface de usuário de gerenciamento do dispositivo VMware Cloud Director ou executar a API do dispositivo `/nodes` VMware Cloud Director. Consulte a documentação da [API do dispositivo do VMware Cloud Director](#).

Quando você executar a API `/nodes` em um nó peer que apresenta o problema de SSH, a API `/nodes` retorna informações de que `localClusterHealth` é `SSH_PROBLEM` e `localClusterFailover` é `INDETERMINATE`. O modo de failover é `INDETERMINATE` porque o nó no qual você executa a API `/nodes` não pode se conectar a um dos seus nós peer via SSH. O trecho "details" na parte da saída de "failover" do corpo de resposta para o nó com problema de SSH exibe: `ssh failed. command: ssh unreachable_standby_host_IP /usr/bin/grep failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf.`

Por exemplo, se um nó em espera tiver um problema de SSH e você executar `GET https://primary_host_IP:5480/api/1.0.0/nodes`, a API `/nodes` poderá retornar as seguintes informações.

```
{
  "localClusterFailover": "INDETERMINATE",
  "localClusterHealth": "SSH_PROBLEM",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
          "status": "NOT APPLICABLE"
        }
      },
      "id": primary_node_ID,
      "location": "default",
      "name": "primary_host_name",
      "nodeHealth": "HEALTHY",
      "nodeRole": "PRIMARY",
      "role": "primary",
      "status": "* running",
      "upstream": ""
    },
    {
      "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = not applicable",
          "status": "NOT APPLICABLE"
        }
      },
      "id": running_standby_node_ID,
      "location": "default",
      "name": "running_standby_host_name",
      "nodeHealth": "HEALTHY",
      "nodeRole": "STANDBY",
      "role": "standby",
      "status": "running",
      "upstream": "primary_host_name"
    },
    {
      "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "ssh failed. command: ssh unreachable_standby_host_IP /usr/bin/
```

```

grep failover>manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
    "mode": "UNKNOWN",
    "repmgrd": {
        "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = not running",
        "status": "NOT RUNNING"
    }
},
"id": unreachable_standby_node_ID,
"location": "default",
"name": "unreachable_standby_host_name",
"nodeHealth": "HEALTHY",
"nodeRole": "STANDBY",
"role": "standby",
"status": "running",
"upstream": "primary_host_name"
}
],
"warnings": []
}

```

Se você executar `GET https://unreachable_standby_host_IP:5480/api/1.0.0/nodes`, como o nó não é confiável, as informações de `localClusterFailover` e `localClusterState` poderão não estar corretas. A API `/nodes` retorna mensagens de aviso indicando que *unreachable_standby_host_name* não consegue se conectar aos seus nós peer.

Por exemplo, a API `/nodes` pode retornar as seguintes informações.

```

{
    "localClusterFailover": "MANUAL",
    "localClusterHealth": "SSH_PROBLEM",
    "localClusterState": [
        {
            "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "ssh failed. command: ssh primary_host_IP /usr/bin/grep
failover>manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
                "mode": "UNKNOWN",
                "repmgrd": {
                    "details": "On node primary_node_ID (primary_host_name): repmgrd = n/a",
                    "status": "UNKNOWN"
                }
            },
            "id": primary_node_ID,
            "location": "default",
            "name": "primary_host_name",
            "nodeHealth": "UNHEALTHY",
            "nodeRole": "PRIMARY",
            "role": "primary",
            "status": "? running",
            "upstream": ""
        },
        {

```

```

        "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "ssh failed. command: ssh running_standby_host_IP /usr/bin/grep
failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
            "mode": "UNKNOWN",
            "repmgrd": {
                "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = n/a",
                "status": "UNKNOWN"
            }
        },
        "id": running_standby_node_ID,
        "location": "default",
        "name": "running_standby_host_name",
        "nodeHealth": "UNHEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "? running",
        "upstream": "primary_host_name"
    },
    {
        "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": unreachable_standby_node_ID,
        "location": "default",
        "name": "unreachable_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "? primary_host_name"
    }
],
"warnings": [
    "unable to connect to node \"primary_host_name\" (ID: primary_node_ID)",
    "unable to connect to node \"running_standby_host_name\" (ID:
running_standby_node_ID)",
    "unable to connect to node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID)'s upstream node \"primary_host_name\" (ID: primary_node_ID)",
    "unable to determine if node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID) is attached to its upstream node \"primary_host_name\" (ID:
primary_node_ID)"
]
}

```

Causa

O VMware Cloud Director armazena os certificados SSH do usuário **postgres** no armazenamento do servidor de transferência compartilhado NFS. Todos os nós de banco de dados devem ter acesso ao armazenamento do servidor de transferência compartilhado. Se um nó do banco de dados se tornar não confiável, ou seja, se os certificados SSH do usuário **postgres** não forem mais válidos ou acessíveis, ele não poderá executar comandos em seus nós peer usando um cliente SSH. O dispositivo VMware Cloud Director deve ter esse recurso para ser executado corretamente quando está no modo HA.

Solução

- 1 Determine se há um problema de conectividade entre os nós e corrija o problema. Consulte [Verificar o status de conectividade de um cluster de alta disponibilidade de banco de dados](#).
- 2 Verifique se o serviço `appliance-sync.timer` está em execução nos nós que têm o problema de SSH, executando o seguinte comando.

```
systemctl status appliance-sync.timer
```

Por exemplo, o comando pode retornar:

```
* appliance-sync.timer - Periodic check and sync of needed files for Cloud Appliance
functionality
   Loaded: loaded (/lib/systemd/system/appliance-sync.timer; enabled; vendor preset:
enabled)
   Active: active (waiting) since Sat 2020-09-05 23:22:49 UTC; 1 months 9 days ago

Warning: Journal has been rotated since unit was started. Log output is incomplete or
unavailable.
```

- 3 Se o status do serviço `appliance-sync.timer` não for Ativo, reinicie esse serviço executando o seguinte comando.

```
systemctl start appliance-sync.timer
```

- 4 Aguarde aproximadamente 90 segundos e verifique se o estado do cluster é `HEALTHY` usando a UI de gerenciamento do VMware Cloud Director ou chame a API `/nodes`.

Usando os arquivos de log para solucionar problemas de atualizações e patches do VMware Cloud Director

Você pode examinar os arquivos de log em busca de erros e avisos ao aplicar patches ao dispositivo VMware Cloud 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 VMware Cloud Director como **root**.
- 2 Navegue até o arquivo de log apropriado.
 - Se `vamcli update --check` falhar, navegue até `/opt/VMware/var/log/vami/vami.log`.
 - Se houver falha no `vamcli update --install latest`, navegue até `/opt/VMware/var/log/vami/updatecli.log`.
- 3 Examine o arquivo de log.

Falha na verificação de atualizações do VMware Cloud Director

Quando você verifica se há atualizações no dispositivo VMware Cloud Director, a execução do comando `vamcli update --check` pode falhar.

Problema

Durante o procedimento de aplicação de um patch ao dispositivo VMware Cloud Director, você executa o comando `vamcli update --check` para verificar se há atualizações disponíveis. O comando `vamcli 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 `vamcli` com o caminho correto.

```
vamcli update --repo file:/root/local-update-repo
```

- 2 Execute novamente o comando para verificar se há atualizações.

```
vamcli update --check
```

Falha na instalação da atualização mais recente do VMware Cloud Director

Quando você estiver instalando as atualizações mais recentes do dispositivo VMware Cloud Director, a execução do comando `vamcli update --install latest` poderá falhar.

Problema

Durante o procedimento de aplicação de um patch ao dispositivo VMware Cloud Director, você executa o comando `vamcli update --install latest` para aplicar o patch mais recente disponível. O comando `vamcli 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.

```
vamcli update --install latest
```

Instalação, upgrade e administração do VMware Cloud Director no Linux

4

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

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

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

Quando você atualiza uma instalação existente do VMware Cloud Director, você atualiza o software VMware Cloud 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 VMware Cloud Director no Linux para o appliance VMware Cloud Director, você atualiza o software VMware Cloud Director e migra o banco de dados para o banco de dados incorporado no appliance.

Este capítulo inclui os seguintes tópicos:

- [Planejamento de configuração](#)
- [Preparando para a instalação do VMware Cloud Director](#)
- [Instalar o VMware Cloud Director no Linux](#)
- [Depois de instalar o VMware Cloud Director](#)
- [Fazendo upgrade do VMware Cloud Director no Linux](#)
- [Depois de fazer upgrade do VMware Cloud Director](#)

Planejamento de configuração

O vSphere fornece a capacidade de rede, processamento e armazenamento para o VMware Cloud Director. Antes de iniciar a instalação, considere quanta capacidade do vSphere e do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director atendam a pelo menos os requisitos mínimos de memória e armazenamento detalhado em *Notas da Versão do VMware Cloud Director*.
- Se você planeja instalar o VMware Cloud Director no Linux, configure o banco de dados do VMware Cloud Director conforme descrito em [Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux](#).

Preparando para a instalação do VMware Cloud Director

Antes de instalar o VMware Cloud Director em um servidor Linux, você deve preparar o seu ambiente.

Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux

As células do VMware Cloud Director usam um banco de dados para armazenar informações compartilhadas. Antes de instalar o VMware Cloud 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 VMware Cloud Director.

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

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

O VMware Cloud 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 VMware Cloud Director. Consulte [Referência de configuração autônoma](#) e [Realizar configurações adicionais no banco de dados PostgreSQL externo](#).

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

Pré-requisitos

Para obter informações sobre os bancos de dados do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director, você pode configurar o banco de dados PostgreSQL para exigir conexões SSL das células do VMware Cloud 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 o VMware Cloud Director no Linux

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 VMware Cloud Director.

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

- Durante transferências, uploads e downloads ocupam esse armazenamento. Quando a transferência termina, os uploads e downloads são removidos do armazenamento. As transferências que não fizeram 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.

Opções de armazenamento compartilhado

Um servidor NFS tradicional baseado em Linux ou outras soluções como o Microsoft Windows Server, o recurso NFS do VMware vSAN File Service e assim por diante podem fornecer o armazenamento compartilhado. A partir do vSAN 7.0, você pode usar a funcionalidade vSAN File Service para exportar compartilhamentos NFS usando os protocolos NFS 3.0 e NFS 4.1. Para obter mais informações sobre o vSAN File Service, consulte o guia *Administrando o VMware vSAN* na [Documentação do produto VMware vSphere](#).

Requisitos para a configuração do servidor NFS

Há requisitos específicos para a configuração do servidor NFS, para que o VMware Cloud 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 VMware Cloud 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 VMware Cloud 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.

Exemplo de servidor NFS do Linux

Se o servidor NFS do Linux tiver um diretório chamado `vCDspace` como o espaço de transferência para o grupo de servidores do VMware Cloud Director com a localização `/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 três células denominadas `vCD-Cell1-IP`, `vCD-Cell2-IP` e `vCD-Cell3-IP` é `no_root_squash`. Você deve adicionar as seguintes linhas ao arquivo `/etc/exports`.

```
/nfs/vCDspace vCD_Cell1_IP_Address(rw, sync, no_subtree_check, no_root_squash)
/nfs/vCDspace vCD_Cell2_IP_Address(rw, sync, no_subtree_check, no_root_squash)
/nfs/vCDspace vCD_Cell3_IP_Address(rw, sync, no_subtree_check, no_root_squash)
```

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.

Para cada servidor no grupo de servidores do VMware Cloud Director, você deve ter uma entrada correspondente no arquivo `/etc/exports` do servidor NFS para que eles possam montar esse compartilhamento NFS. Depois de fazer alterações no arquivo `/etc/exports` no servidor NFS, execute `exportfs -a` para exportar novamente todos os compartilhamentos NFS.

Considerações ao planejar o upgrade da sua instalação do VMware Cloud Director para uma versão posterior

Durante um upgrade de um grupo de servidores do VMware Cloud Director, você executa o arquivo de instalação para a versão atualizada para fazer upgrade de todos os membros desse grupo de servidores VMware Cloud 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.

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 VMware Cloud Director ou qualquer outro arquivo assinado baixado de `vmware.com`. Se você instalar a chave pública no computador no qual pretende instalar o VMware Cloud 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 VMware Cloud Director

Se você planeja a instalação do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director e outros produtos VMware, consulte as *Matrizes de interoperabilidade de produtos VMware* em 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 VMware Cloud Director](#).

Importante Esse procedimento é utilizado somente quando você está realizando uma nova instalação do VMware Cloud Director. Se você estiver atualizando uma instalação existente do VMware Cloud Director, consulte [Fazendo upgrade do VMware Cloud Director no Linux](#).

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 VMware Cloud Director na instalação do VMware Cloud Director planejada.
- 4 Configure o suporte VXLAN nas instâncias do NSX Manager associadas.

O VMware Cloud 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 VMware Cloud Director

Se você planeja que a instalação do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director](#).

Esse procedimento é utilizado somente quando você está realizando uma nova instalação do VMware Cloud Director. Se você estiver atualizando uma instalação existente do VMware Cloud Director, consulte [Fazendo upgrade do VMware Cloud Director no Linux](#).

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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director*.

Instalar o VMware Cloud Director no Linux

Você pode criar um grupo de servidores do VMware Cloud Director instalando o software VMware Cloud 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 VMware Cloud Director, consulte [Fazendo upgrade do VMware Cloud Director no Linux](#).

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

A partir da versão 10.1, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos que não são acessíveis aos tenants que estão usando a API do VMware Cloud Director para testes de conexão. Configure a lista de negação após a instalação ou o upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação para conexão de teste](#).

Pré-requisitos

- Verifique se os servidores de destino para o seu grupo de servidores atendem a [Capítulo 2 Requisitos de hardware e software do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. Consulte [Preparando o armazenamento do servidor de transferência para o VMware Cloud Director no Linux](#).
- Verifique se você criou um banco de dados do VMware Cloud Director que é acessível a todos os servidores no grupo. Consulte [Configurar um banco de dados PostgreSQL externo para VMware Cloud 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 VMware Cloud 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 VMware Cloud Director](#).
- Verifique se todos os servidores do VMware Cloud 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 VMware Cloud Director](#).
- Se você planeja importar usuários ou grupos de um serviço de LDAP, verifique se o serviço está acessível para cada servidor do VMware Cloud Director.
- Abra as portas de firewall conforme mostrado em [Requisitos de segurança de rede](#). A porta 443 deve estar aberta entre os sistemas do VMware Cloud Director e do vCenter Server.

Procedimentos

1 Instalar o VMware Cloud 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 VMware Cloud Director, executando o instalador do VMware Cloud Director no primeiro servidor Linux de destino.

2 Criação e gerenciamento de certificados SSL para o VMware Cloud Director no Linux

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

3 Configurar as conexões de rede e banco de dados

Depois de instalar o VMware Cloud 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.

4 Instalar o VMware Cloud Director em um membro adicional de um grupo de servidores

Você pode adicionar servidores a um grupo de servidores do VMware Cloud 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 VMware Cloud Director](#).

Instalar o VMware Cloud 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 VMware Cloud Director, executando o instalador do VMware Cloud Director no primeiro servidor Linux de destino.

O VMware Cloud 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 VMware Cloud Director.

O instalador do VMware Cloud Director verifica se o servidor de destino atende a todos os pré-requisitos de plataforma e instala o software VMware Cloud 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@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 VMware Cloud Director.

```
[root@cell11 /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@cell11 /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 `vccloud`.
- d Desempacota o pacote RPM do VMware Cloud 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.

Criação e gerenciamento de certificados SSL para o VMware Cloud Director no Linux

O VMware Cloud Director usa SSL para proteger comunicações entre clientes e servidores. Cada servidor do VMware Cloud 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.

Antes de criar certificados SSL para o VMware Cloud Director no Linux

Ao instalar o VMware Cloud 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 VMware Cloud Director no Linux. O dispositivo do VMware Cloud Director cria certificados SSL autoassinados durante a primeira inicialização.

Procedimentos

- 1 Faça login no servidor VMware Cloud 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 VMware Cloud Director no Linux](#).
- Para obter informações sobre como criar certificados SSL autoassinados, consulte [Criar certificados SSL autoassinados para o VMware Cloud 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 VMware Cloud Director no Linux](#).

Criar certificados SSL autoassinados para o VMware Cloud Director no Linux

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

Cada servidor do VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. Consulte [Configurar as conexões de rede e banco de dados](#).

Criar um armazenamento de chaves de certificados SSL assinado por CA para o VMware Cloud 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 VMware Cloud Director requer dois certificados SSL para proteger as comunicações entre clientes e servidores. Cada servidor do VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 [Gerando certificados autoassinados para os endpoints de proxy do console e HTTPS](#).
- Para obter mais detalhes sobre as opções disponíveis para o comando `certificates`, consulte [Substituindo certificados para os endpoints de proxy de console e HTTPS](#).

Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH no sistema operacional da célula de servidor do VMware Cloud 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 VMware Cloud 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 PKCS12 -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 PKCS12 -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 PKCS12.

- 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 PKCS12 -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 PKCS12 -storepass keystore_password -keystore
certificates.ks -alias intermediate -file intermediate_certificate_file
```

- c Importe o certificado do serviço HTTPS.

```
keytool -import -storetype PKCS12 -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 PKCS12 -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 PKCS12, execute o comando para listar o conteúdo do arquivo do armazenamento de chaves.

```
keytool -storetype PKCS12 -storepass keystore_password -keystore certificates.ks -list
```

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

Próximo passo

- Se você ainda não tiver configurado sua instância do VMware Cloud Director, execute o script `configure` para importar o repositório de chaves de certificados para o VMware Cloud 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 VMware Cloud 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 HTTPS](#).

Criar um armazenamento de chaves de certificados SSL assinado por CA com chaves privadas importadas para o VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 HTTPS](#).

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.p12 -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.p12 -chain
```

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

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

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks -deststoretype PKCS12 -srckeystore http.p12 -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 PKCS12 -srckeystore consoleproxy.p12 -srcstoretype PKCS12 -srcstorepass keystore_password
```

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

```
keytool -storetype PKCS12 -storepass keystore_password -keystore certificates.ks -list
```

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

Próximo passo

- Se você ainda não tiver configurado sua instância do VMware Cloud Director, execute o script `configure` para importar o repositório de chaves de certificados para o VMware Cloud 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 VMware Cloud 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 HTTPS](#).

Configurar as conexões de rede e banco de dados

Depois de instalar o VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 HTTPS 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 5 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 VMware Cloud Director está instalado. Normalmente, esse valor é `/opt/vmware/vcloud-director`.

Procedimentos

1 Faça login no servidor VMware Cloud 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 Cloud Director** depois que o serviço do VMware Cloud Director é iniciado.
- c Oferece para iniciar a célula do VMware Cloud Director.

3 (Opcional) Anote a URL do assistente de **Configuração do VMware Cloud Director** e insira `y` para iniciar o serviço do VMware Cloud 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 4-1. Informações necessárias durante uma configuração de rede e banco de dados interativa

Informações necessárias	Descrição
Endereço IP do serviço HTTPS	O padrão é o primeiro endereço IP disponível.
Endereço IP do serviço de proxy do console	O padrão é o primeiro endereço IP disponível. Observação Se você quiser usar um único endereço IP com duas portas diferentes para o serviço HTTPS 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 Antes de criar certificados SSL para o VMware Cloud Director no Linux .
Senha da chave privada para o certificado SSL HTTPS	Consulte Antes de criar certificados SSL para o VMware Cloud Director no Linux .
Senha da chave privada para o certificado SSL do proxy de console	Consulte Antes de criar certificados SSL para o VMware Cloud Director no Linux .
Habilitar o log de auditoria remoto para um host syslog	Serviços em todas as mensagens de log de auditoria de célula do VMware Cloud Director para o banco de dados VMware Cloud Director, onde elas são preservadas por 90 dias. Para preservar as mensagens de auditoria por mais tempo, você pode configurar serviços do VMware Cloud Director para enviar mensagens de auditoria para o utilitário do <code>syslog</code> além do banco de dados do VMware Cloud Director. <ul style="list-style-type: none"> ■ Para ignorar, pressione Enter. ■ Para habilitar, insira o nome do host ou o endereço IP do syslog.
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 <code>vcloud</code> .
Nome de usuário do banco de dados	Consulte Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux .

Tabela 4-1. Informações necessárias durante uma configuração de rede e banco de dados interativa (continuação)

Informações necessárias	Descrição
Senha do banco de dados	Consulte Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux .
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 & 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. Consulte Capítulo 5 Referência da ferramenta de gerenciamento de células.</p> <p>Para participar do programa, insira y.</p> <p>Se você preferir não participar do programa CEIP da VMware, insira n.</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 4-2. 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 VMware Cloud 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 VMware Cloud Director.

Tabela 4-2. Argumentos e opções do utilitário de configuração (continuação)

Opção	Argumento	Descrição
<code>--database-ssl</code>	<code>true</code> OU <code>false</code>	Você pode configurar o banco de dados PostgreSQL para exigir uma conexão SSL bem sinalizada do VMware Cloud Director. Se você deseja configurar o banco de dados PostgreSQL para usar um certificado autoassinado ou privado, consulte Realizar configurações adicionais no banco de dados PostgreSQL externo .
<code>--database-host (-dbhost)</code>	Endereço IP ou nome de domínio completo do host do banco de dados do VMware Cloud Director	Consulte Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux .
<code>--database-name (-dbname)</code>	O nome do serviço de banco de dados	Consulte Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux .
<code>--database-password (-dbpassword)</code>	Senha para o usuário do banco de dados. Ele pode ser nulo.	Consulte Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux .
<code>--database-port (-dbport)</code>	Número da porta usada pelo serviço de banco de dados no host do banco de dados	Consulte Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux .
<code>--database-type (-dbtype)</code>	O tipo de banco de dados. O tipo com suporte é <code>postgres</code> .	Opcional. O tipo de banco de dados padrão será <code>postgres</code> . Consulte Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux .
<code>--database-user (-dbuser)</code>	Nome de usuário do usuário de banco de dados.	Consulte Configurar um banco de dados PostgreSQL externo para VMware Cloud Director no Linux .

Tabela 4-2. Argumentos e opções do utilitário de configuração (continuação)

Opção	Argumento	Descrição
<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 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. Consulte Capítulo 5 Referência da ferramenta de gerenciamento de células .
<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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 4-2. 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 VMware Cloud Director para o banco de dados VMware Cloud Director, onde elas são preservadas por 90 dias. Para preservar as mensagens de auditoria por mais tempo, você pode configurar serviços do VMware Cloud Director para enviar mensagens de auditoria para o utilitário do <code>syslog</code> além do banco de dados do VMware Cloud Director.
<code>--syslog-port (-logport)</code>	Inteiro no intervalo de 0 a 65535	A porta na qual o processo do <code>syslog</code> 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>Importante 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 do VMware Cloud Director com dois endereços IP diferentes para o serviço HTTPS e o serviço de proxy de console.

```
[root@cell11 /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 do VMware Cloud Director com um endereço IP único com duas portas diferentes para o serviço HTTPS e o serviço de proxy de console.

```
[root@cell11 /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 VMware Cloud 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 VMware Cloud 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 `vcloud.vcloud`, conforme mostrado neste exemplo.

```
[root@cell11 /tmp]# ls -l responses.properties
-rw----- 1 vcloud vcloud 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@cell11 /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 VMware Cloud Director em um membro adicional de um grupo de servidores

Você pode adicionar servidores a um grupo de servidores do VMware Cloud 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 VMware Cloud Director no Linux e as implantações de appliance VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

```
[root@cell11 /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@cell11 /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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

- 9 (Opcional) Insira `y` para iniciar o serviço do VMware Cloud 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 VMware Cloud Director estão em execução em todos os servidores, você deve inicializar o banco de dados do VMware Cloud 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 VMware Cloud Director](#).

Depois de instalar o VMware Cloud Director

Depois de criar o grupo de servidores do VMware Cloud Director, você poderá instalar os arquivos de Sysprep da Microsoft e o banco de dados Cassandra. Se estiver usando um banco de dados do PostgreSQL, você poderá configurar o SSL e ajustar alguns parâmetros no banco de dados.

A partir da versão 10.1, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos que não são acessíveis aos tenants que estão usando a API do VMware Cloud Director para testes de conexão. Configure a lista de negação após a instalação ou o upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação para conexão de teste](#).

Personalizar endereços públicos para o VMware Cloud Director no Linux

Para atender aos requisitos de balanceador de carga ou de proxy, você pode alterar os endereços da Web do endpoint padrão para o Portal da Web do VMware Cloud Director, a API do VMware Cloud Director e o proxy do console.

Pré-requisitos

Verifique se você está conectado como **administrador do sistema**. Somente um **administrador do sistema** pode personalizar os endpoints públicos.

Procedimentos

- 1 Na barra de navegação superior do Service Provider Admin Portal, selecione **Administração**.
- 2 No painel esquerdo, em **Configurações**, clique em **Endereços Públicos**.
- 3 Para personalizar os endpoints públicos, clique em **Editar**.
- 4 Para personalizar as URLs do VMware Cloud Director, edite os endpoints do **Portal da Web**.
 - a Insira uma URL pública personalizada do VMware Cloud Director para conexões HTTP (não seguras).
 - b Insira a URL pública personalizada do VMware Cloud Director para conexões HTTPS (seguras) e clique em **Carregar** para carregar os certificados que estabelecem a cadeia de confiança para esse endpoint.

A cadeia de certificados deve corresponder ao certificado usado pelo endpoint de serviço, que é o certificado carregado para cada armazenamento de chaves de célula do VMware Cloud Director com o alias `consoleproxy`. Não há suporte para a terminação SSL das conexões de proxy do console em um balanceador de carga. A cadeia de certificados deve incluir um certificado de endpoint, certificados intermediários e um certificado raiz no formato `PEM` sem uma chave privada.

- 5 (Opcional) Para personalizar as URLs da REST API e do OpenAPI do Cloud Director, desative a opção **Usar Configurações do Portal da Web**.

- a Insira uma URL base HTTP personalizada.

Por exemplo, se você definir a URL base HTTP como **http://vcloud.example.com**, poderá acessar a API do VMware Cloud Director em **http://vcloud.example.com/api** e poderá acessar o OpenAPI do VMware Cloud Director em **http://vcloud.example.com/cloudapi**.

- b Insira uma URL de base da REST API de HTTPS e clique em **Carregar** para carregar os certificados que estabelecem a cadeia de confiança para esse endpoint.

Por exemplo, se você definir a URL base da API REST HTTPS como **https://vcloud.example.com**, poderá acessar a API do VMware Cloud Director em **https://vcloud.example.com/api** e o OpenAPI do VMware Cloud Director em **https://vcloud.example.com/cloudapi**.

A cadeia de certificados deverá corresponder ao certificado usado pelo endpoint de serviço, que é o certificado carregado para cada armazenamento de chaves de célula do VMware Cloud Director com o alias `http`, ou ao certificado VIP do balanceador de carga se for usada uma terminação SSL. A cadeia de certificados deve incluir um certificado de endpoint, certificados intermediários e um certificado raiz no formato PEM sem uma chave privada.

- 6 Insira um endereço de proxy personalizado do console público do VMware Cloud Director.

Esse endereço é o nome de domínio totalmente qualificado (FQDN) do servidor do VMware Cloud Director ou do balanceador de carga com o número da porta. A porta padrão é 443.

Importante O VMware Cloud Director Appliance usa o NIC do seu `eth0` com a porta personalizada 8443 para o serviço de proxy do console.

Por exemplo, para uma instância do VMware Cloud Director Appliance com FQDN `vcloud.example.com`, insira **vcloud.exemplo.com:8443**.

O VMware Cloud Director usa o endereço de proxy do console ao abrir uma janela de console remoto em uma VM.

- 7 Para salvar as alterações, clique em **Salvar**.

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

O VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. A recuperação das métricas atuais não exige o software de banco de dados opcional.

Pré-requisitos

- Verifique se o VMware Cloud 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 VMware Cloud 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 VMware Cloud 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@cell11 /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 5 Referência da ferramenta de gerenciamento de células](#).

- 2 (Opcional) Se você está atualizando o VMware Cloud 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@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --add-
rollup \ --username admin --password 'P@55w0rd'
```

- 3 Reinicie cada célula do VMware Cloud Director.

Realizar configurações adicionais no banco de dados PostgreSQL externo

Depois de criar o seu grupo de servidores do VMware Cloud Director, você pode configurar o banco de dados PostgreSQL externo para exigir conexões SSL das células do VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director, execute o comando para importar o certificado do banco de dados para o truststore do VMware Cloud 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 VMware Cloud 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 5 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 VMware Cloud 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.

Instalar e configurar um agente RabbitMQ AMQP

Se quiser usar tarefas de bloqueio, notificações ou extensões de API do VMware Cloud Director, como Container Service Extension (CSE) e VMware Cloud Director App Launchpad, deverá instalar e configurar um Agente RabbitMQ AMQP.

O protocolo AMQP (Advanced Message Queuing Protocol) é um padrão aberto para enfileiramento de mensagens que oferece suporte a mensagens flexíveis para sistemas empresariais. O VMware Cloud Director usa o agente RabbitMQ AMQP para fornecer o barramento de mensagem usado por serviços de extensão, extensões de objeto e notificações.

Para o VMware Cloud Director, o uso de um cliente MQTT pode ser uma alternativa para o Agente RabbitMQ AMQP durante a configuração de notificações. Consulte [Assinar eventos, tarefas e métricas usando um cliente MQTT](#).

Procedimentos

- 1 Baixe o Servidor do RabbitMQ do <https://www.rabbitmq.com/download.html>.

Consulte *Notas da Versão do VMware Cloud 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 VMware Cloud Director.

- 3 Durante a instalação do RabbitMQ, anote os valores necessários para configurar o VMware Cloud 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 para não SSL. A porta padrão para SSL/TLS é 5671.
- O protocolo de comunicação é TCP.
- O host virtual do RabbitMQ. O padrão é `"/"`.

Próximo passo

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

Para ativar o SSL com o serviço AMQP do VMware Cloud Director, consulte as informações em [configurar um agente deAMQP](#) no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

Assinar eventos, tarefas e métricas usando um cliente MQTT

Você pode usar um cliente MQTT para assinar mensagens sobre eventos e tarefas do VMware Cloud Director.

O MQTT é um protocolo de transporte de mensagens leve e binário. O VMware Cloud Director usa MQTT para publicar informações sobre eventos e tarefas nos quais você pode assinar usando um cliente MQTT. As mensagens do MQTT passam por um agente do MQTT que também pode armazenar mensagens caso os clientes não estejam online.

Começando com o VMware Cloud Director 10.2.2, é possível usar um cliente MQTT para assinar métricas.

Pré-requisitos

- Verifique se você tem um cliente MQTT que oferece suporte ao WebSocket.
- Verifique se você pode adicionar cabeçalhos a uma solicitação do WebSocket atualizada.
- Se quiser assinar métricas, configure a coleção de métricas e habilite a publicação de métricas. Consulte [Configurar a coleção e a publicação de métricas](#).

Procedimentos

- 1 Faça login no VMware Cloud Director usando o endpoint do OpenAPI.
- 2 Para estabelecer uma conexão WebSocket, defina a propriedade Sec-WebSocket-Protocol como `mqtt`, defina o cliente para se conectar ao caminho `/messaging/mqtt`, adicione um cabeçalho de autorização e siga o fluxo de conexão padrão do MQTT.

Você recebe o token JWT da solicitação de login padrão para o VMware Cloud Director. Você pode deixar o nome de usuário e a senha vazios.

```
Sec-WebSocket-Protocol: mqtt
```

```
Authorization: Bearer {JWT_token}
```

- 3 Quando a conexão for estabelecida com êxito, assine os tópicos por meio do cliente MQTT.

```
publish/{user_org_id}/{user_id}
```

```
publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
```

Os administradores da organização podem usar curingas para acessar todos os tópicos da organização.

```
publish/{user_org_id}/+
```

Os **administradores do sistema** podem usar curingas para acessar todos os tópicos.

```
publish/#
```

- 4 (Opcional) Para o VMware Cloud Director 10.2.2 ou versões posteriores, assine métricas.

```
metrics/{org_id}/{vApp_id}
```

Somente **administradores do sistema** podem acessar o tópico de métricas.

Grupos de Dimensionamento Automático

Começando com o VMware Cloud Director 10.2.2, você pode permitir que os usuários do tenant dimensionem aplicativos automaticamente, dependendo do uso atual de CPU e memória.

Dependendo de critérios predefinidos para o uso de CPU e memória, os tenants podem usar o VMware Cloud Director para ampliar ou reduzir automaticamente o número de VMs em um grupo de dimensionamento selecionado. Para permitir que os tenants dimensionem aplicativos automaticamente, você deve configurar, publicar e conceder acesso à solução de dimensionamento automático.

Para balancear a carga dos servidores configurados para executar o mesmo aplicativo, você pode usar o VMware NSX Advanced Load Balancer (Avi Networks).

Configurar e publicar o plug-in de dimensionamento automático

Antes de conceder acesso aos tenants, você deve configurar a solução de grupos de dimensionamento automático. O dimensionamento automático pode ser usado a partir do VMware Cloud Director 10.2.2.

- 1 Faça login diretamente ou usando um cliente SSH no sistema operacional de qualquer uma das células no cluster como **root**.
- 2 Ative a coleta de dados de métricas configurando a coleta de métricas em um banco de dados Cassandra ou colete métricas sem persistência de dados de métricas.
 - [Instalar e configurar um banco de dados Cassandra para armazenar dados de métricas de históricos](#)
 - Para coletar dados de métricas sem persistência de dados, execute os seguintes comandos:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n  
statsFeeder.metrics.collect.only -v true
```

- 3 Ative a publicação de métricas.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n  
statsFeeder.metrics.publishing.enabled -v true
```

- 4 Crie um arquivo `metrics.groovy` na pasta `/tmp` com o seguinte conteúdo.

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
        historicInterval=20
        entity="VM"
        instance=""
        minReportingInterval=300
        aggregator="AVERAGE"
    }
}
```

- 5 Importe o arquivo.

```
$VCLLOUD_HOME/bin/cell-management-tool configure-metrics --metrics-config /tmp/
metrics.groovy
```

- 6 Se você tiver configurado o Cassandra anteriormente, atualize o esquema Cassandra fornecendo os endereços de nós corretos, os detalhes de autenticação do banco de dados, a porta e o tempo de vida de métricas em dias.

```
$VCLLOUD_HOME/bin/cell-management-tool cassandra -configure -cluster-nodes
nodes_IP_addresses -username cassandra -password cassandra_password -port port_number -ttl
TTL_days -update-schema
```

- 7 Se você executar a célula com um certificado assinado por CA, para ativar o dimensionamento automático, execute o seguinte comando.

```
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set enabled=true
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set username=<username>
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --encrypt --set
password=<password>
```

Ao executar o comando no terminal, faça o escape de qualquer caractere especial usando o sinal de barra invertida (`\`).

- 8 Reinicie a célula.

```
service vmware-vcd restart
```

- 9 [Publicar o pacote de direitos de dimensionamento automático.](#)

Publicar o pacote de direitos de dimensionamento automático

Se quiser que os tenants dimensionem aplicativos automaticamente, você deverá publicar o pacote de direitos em uma ou mais organizações do seu sistema. O dimensionamento automático pode ser usado a partir do VMware Cloud Director 10.2.2.

Pré-requisitos

[Configurar e publicar o plug-in de dimensionamento automático](#)

Procedimentos

- 1 Na barra de navegação superior, selecione **Administração**.
- 2 No painel esquerdo, em **Controle de Acesso do Tenant**, selecione **Pacotes de Direitos**.
- 3 Verifique se não há **Pacotes de Direitos Legados** para as organizações de tenants às quais você deseja conceder acesso para dimensionamento automático.
- 4 Selecione o pacote **vmware:scalegroup Entitlement** e clique em **Publicar**.
- 5 Para publicar o pacote:
 - a Selecione **Publicar em Tenants**.
 - b Selecione as organizações para a qual você deseja publicar a função.
 - Se você quiser publicar o pacote para todas as organizações existentes e recém-criadas no seu sistema, selecione **Publicar para Todos os Tenants**.
 - Se você deseja publicar o pacote para organizações específicas no seu sistema, selecione essas organizações individualmente.
- 6 Clique em **Salvar**.

Próximo passo

Adicione os direitos **VMWARE:SCALEGROUP** necessários para as funções de tenant que você deseja usar para grupos de dimensionamento. Consulte [Exibir e editar uma função de tenant global](#) no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

Fazendo upgrade do VMware Cloud Director no Linux

Para fazer upgrade do VMware Cloud Director para uma nova versão, encerre os serviços do VMware Cloud Director em todas as células no grupo de servidores, instale a nova versão em cada servidor, faça upgrade do banco de dados do VMware Cloud Director e reinicie as células do VMware Cloud Director.

Se o seu grupo de servidores do VMware Cloud Director existente consistir em instalações do VMware Cloud Director no Linux, você poderá usar o instalador do VMware Cloud Director para Linux para atualizar seu ambiente.

Para instalações do VMware Cloud Director no Linux, você pode executar um upgrade orquestrado ou fazer o upgrade manualmente do VMware Cloud Director. Consulte [Realizar uma atualização orquestrada de uma instalação do VMware Cloud Director](#) ou [Atualizar manualmente uma instalação do VMware Cloud 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.

Iniciando com o VMware Cloud Director 9.5:

- Os bancos de dados Oracle não têm suporte. Se a sua instalação existente do VMware Cloud Director usar um banco de dados Oracle, consulte a tabela [Fazer upgrade de caminhos e fluxos de trabalho](#).
- Não há suporte para a ativação e a desativação de hosts do ESXi. Antes de iniciar o upgrade, você deve ativar todos os hosts do ESXi. Você pode colocar os hosts do ESXi no modo de manutenção usando o vSphere Client.
- O VMware Cloud 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 VMware Cloud Director 10.0, os bancos de dados Microsoft SQL Server não têm suporte.

Quando você atualiza o VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Para obter informações sobre a compatibilidade do VMware Cloud 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. Se você planeja fazer upgrade dos componentes do vSphere ou do NSX como parte do upgrade do VMware Cloud Director, deverá fazer o upgrade deles após o upgrade do VMware Cloud Director. Consulte [Depois de fazer upgrade do VMware Cloud Director](#).

Depois de atualizar pelo menos um servidor VMware Cloud Director, você pode atualizar o banco de dados VMware Cloud Director. O banco de dados armazena informações sobre o estado de tempo de execução do servidor, incluindo o estado de todas as tarefas VMware Cloud 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 VMware Cloud 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 VMware Cloud 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`.

A partir da versão 10.1, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos que não são acessíveis aos tenants que estão usando a API do VMware Cloud Director para testes de conexão. Configure a lista de negação após a instalação ou o upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação para conexão de teste](#).

Importante Após o upgrade para a versão 10.1 e posterior, o VMware Cloud Director sempre verificará certificados para todos os endpoints de infraestrutura conectados a ele. Isso ocorre devido a uma alteração na maneira como o VMware Cloud Director gerencia certificados SSL. Se você não importar seus certificados para o VMware Cloud Director antes do upgrade, as conexões do vCenter Server e do NSX poderão apresentar erros de conexão devido a problemas de verificação de SSL. Nesse caso, após o upgrade, você tem duas opções:

- 1 Execute o comando `trust-infra-certs` da ferramenta de gerenciamento de células para importar automaticamente todos os certificados para o armazenamento centralizado de certificados. Consulte [importar os certificados de Endpoints dos recursos do vSphere](#).
 - 2 Na interface do usuário do Service Provider Admin Portal, selecione cada instância do vCenter Server e do NSX e insira novamente as credenciais ao aceitar o certificado.
-

Fazer upgrade de caminhos e fluxos de trabalho

Ambiente de origem	Ambiente de destino
	VMware Cloud Director 10.2 no Linux com um banco de dados PostgreSQL externo
VMware Cloud Director 9.7 no Linux com um banco de dados Microsoft SQL Server externo	<ol style="list-style-type: none"> 1 Migre o banco de dados Microsoft SQL Server para um banco de dados PostgreSQL. Consulte Migrar para um banco de dados PostgreSQL. 2 Faça upgrade do seu ambiente para o VMware Cloud Director 10.2 no Linux. Consulte Realizar uma atualização orquestrada de uma instalação do VMware Cloud Director ou Atualizar manualmente uma instalação do VMware Cloud Director.
VMware Cloud Director 9.7, 10.0 ou 10.1 no Linux com um banco de dados PostgreSQL externo	Faça upgrade do seu ambiente para o VMware Cloud Director 10.2 no Linux. Consulte Realizar uma atualização orquestrada de uma instalação do VMware Cloud Director ou Atualizar manualmente uma instalação do VMware Cloud Director .
Dispositivo do VMware Cloud Director 9.7, 10.0 e 10.1 com um banco de dados PostgreSQL incorporado	Sem suporte

Realizar uma atualização orquestrada de uma instalação do VMware Cloud Director

Você pode atualizar todas as células no grupo de servidores junto com o banco de dados compartilhado executando o instalador do VMware Cloud Director com a opção `--private-key-path`.

Você pode usar o instalador do VMware Cloud Director para Linux para fazer upgrade de um grupo de servidor do VMware Cloud Director que consiste de instalações do VMware Cloud Director em um SO Linux com suporte. Se o seu grupo de servidores VMware Cloud Director consistir de implantações de dispositivos do VMware Cloud Director 9.5, use o instalador do VMware Cloud Director para Linux para atualizar o ambiente existente somente como parte do fluxo de trabalho de migração. Consulte [Fazendo upgrade e migrando o dispositivo do VMware Cloud Director](#).

O VMware Cloud 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 VMware Cloud Director.

Quando você executa o instalador do VMware Cloud 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 VMware Cloud Director, os componentes do vSphere e os componentes do NSX são compatíveis com a nova versão do VMware Cloud Director.

Importante Se a sua instalação existente do VMware Cloud 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 da atualização. Para os caminhos de upgrade possíveis, consulte [Fazendo upgrade do VMware Cloud Director no Linux](#).

- 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 VMware Cloud 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 VMware Cloud Director para ser usado como uma identidade com a qual os processos do VMware Cloud Director são executados. O usuário do `vcloud` não tem nenhuma senha.

- Verifique se todos os hosts do ESXi estão ativados. Não há suporte aos hosts do ESXi desativados.
- 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 para o VMware Cloud Director no Linux](#).
- Se a instalação do VMware Cloud 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 VMware Cloud Director.

```
[root@cell11 /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 VMware Cloud Director e solicita que você confirme o upgrade.

Se o instalador detectar uma versão do VMware Cloud 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 VMware Cloud Director.
- 3 Atualiza o software do VMware Cloud Director na célula atual.
- 4 Atualiza o banco de dados VMware Cloud Director.
- 5 Atualiza o software VMware Cloud Director em cada uma das células restantes e reinicia os serviços do VMware Cloud Director na célula.
- 6 Reinicia os serviços do VMware Cloud Director na célula atual.

Próximo passo

Inicie os serviços do VMware Cloud 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 VMware Cloud Director

Você pode atualizar uma única célula executando o instalador do VMware Cloud 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 VMware Cloud Director para Linux para fazer upgrade de um grupo de servidor do VMware Cloud Director que consiste de instalações do VMware Cloud Director em um SO Linux com suporte. Se o seu grupo de servidores VMware Cloud Director consistir de implantações de dispositivos do VMware Cloud Director 9.5, use o instalador do VMware Cloud Director para Linux para atualizar o ambiente existente somente como parte do fluxo de trabalho de migração. Consulte [Fazendo upgrade e migrando o dispositivo do VMware Cloud Director](#).

Para uma instalação do VMware Cloud 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 VMware Cloud Director. Consulte [Realizar uma atualização orquestrada de uma instalação do VMware Cloud Director](#).

Pré-requisitos

- Verifique se o banco de dados do VMware Cloud Director, os componentes do vSphere e os componentes do NSX são compatíveis com a nova versão do VMware Cloud Director.

Importante Se a sua instalação existente do VMware Cloud 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 da atualização. Para os caminhos de upgrade possíveis, consulte [Fazendo upgrade do VMware Cloud Director no Linux](#).

- Verifique se você tem credenciais de superusuário para os servidores no seu grupo de servidores do VMware Cloud 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 VMware Cloud Director para o qual você está atualizando.
- Verifique se todos os hosts do ESXi estão ativados. Não há suporte aos hosts do ESXi desativados.

Procedimentos

1 [Atualizar uma célula do VMware Cloud Director](#)

O instalador do VMware Cloud Director verifica se o servidor de destino atende a todos os pré-requisitos de atualização e atualiza o software do VMware Cloud Director no servidor.

2 [Atualizar o banco de dados do VMware Cloud Director](#)

De um servidor VMware Cloud Director atualizado, você executa uma ferramenta que atualiza o banco de dados do VMware Cloud Director. Você não deve reiniciar qualquer servidor VMware Cloud Director atualizado antes de atualizar o banco de dados compartilhado.

Próximo passo

- Depois de atualizar todos os servidores do VMware Cloud Director no grupo de servidores e no banco de dados, você pode iniciar os serviços do VMware Cloud 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 VMware Cloud Director

O instalador do VMware Cloud Director verifica se o servidor de destino atende a todos os pré-requisitos de atualização e atualiza o software do VMware Cloud Director no servidor.

O VMware Cloud 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 VMware Cloud Director.

Para uma instalação do VMware Cloud Director de várias células, você deve executar o instalador do VMware Cloud Director em cada membro do grupo de servidores do VMware Cloud 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@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 VMware Cloud Director.

```
[root@cell11 /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@cell11 /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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.
- c Depois que todos os trabalhos ativos do VMware Cloud Director ativos na célula forem finalizados, ele interrompe os serviços do VMware Cloud Director no servidor e atualiza o software do VMware Cloud 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
Se você não alterou as propriedades de log existentes	Copie este arquivo para <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> .
Se você alterou as propriedades de log	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 VMware Cloud 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 VMware Cloud Director.

Repita esse procedimento em cada célula do VMware Cloud Director no grupo de servidores.

Importante Não inicie os serviços do VMware Cloud Director até atualizar todas as células no grupo de servidores e no banco de dados.

Atualizar o banco de dados do VMware Cloud Director

De um servidor VMware Cloud Director atualizado, você executa uma ferramenta que atualiza o banco de dados do VMware Cloud Director. Você não deve reiniciar qualquer servidor VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director do grupo de servidores estão interrompidas. As células atualizadas são interrompidas durante o processo de atualização. Se existirem servidores VMware Cloud 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 5 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 VMware Cloud 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 VMware Cloud Director atualizados.

Você pode atualizar o restante dos membros do VMware Cloud Director do grupo de servidores e iniciar seus serviços. Consulte [Atualizar uma célula do VMware Cloud 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 4-3. 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 VMware Cloud 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> .

Tabela 4-3. Opções e argumentos do utilitário de atualização de banco de dados (continuação)

Opção	Argumento	Descrição
<code>--enable-ceip</code>	Escolha um: <ul style="list-style-type: none"> ■ <code>true</code> ■ <code>false</code> 	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 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. Consulte Capítulo 5 Referência da ferramenta de gerenciamento de células .
<code>--installer-path</code>	Nome do caminho completo para o arquivo de instalação do VMware Cloud 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> .
<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> .

Tabela 4-3. Opções e argumentos do utilitário de atualização de banco de dados (continuação)

Opção	Argumento	Descrição
<code>--multisite-user</code>	O nome de usuário para a conta de sistema multisite.	Essa conta é usada pelo recurso Multisite do VMware Cloud 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 Realizar uma atualização orquestrada de uma instalação do VMware Cloud Director 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 VMware Cloud Director para ser usado como uma identidade com a qual os processos do VMware Cloud Director são executados. O usuário do `vcloud` não tem nenhuma senha.

Depois de fazer upgrade do VMware Cloud Director

Depois que fazer upgrade de todos os servidores do VMware Cloud Director e o banco de dados compartilhado, poderá fazer upgrade das instâncias do NSX Manager que fornecem serviços de

rede à nuvem. Depois disso, você poderá atualizar os hosts do ESXi e as instâncias do vCenter Server que estão registradas em sua instalação do VMware Cloud Director.

Importante O VMware Cloud Director oferece suporte somente a edge gateways avançados. Você deve converter qualquer edge gateway não avançado herdado em um gateway avançado. Consulte <https://kb.vmware.com/kb/66767>.

A partir da versão 10.1, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e verificar a identidade do servidor como parte de um handshake SSL. Para proteger conexões de rede do VMware Cloud Director, configure uma lista de negação de hosts internos que não são acessíveis aos tenants que estão usando a API do VMware Cloud Director para testes de conexão. Configure a lista de negação após a instalação ou o upgrade do VMware Cloud Director e antes de conceder aos tenants acesso ao VMware Cloud Director. Consulte [Configurar uma lista de negação para conexão de teste](#).

Importante Após o upgrade para a versão 10.1 e posterior, o VMware Cloud Director sempre verificará certificados para todos os endpoints de infraestrutura conectados a ele. Isso ocorre devido a uma alteração na maneira como o VMware Cloud Director gerencia certificados SSL. Se você não importar seus certificados para o VMware Cloud Director antes do upgrade, as conexões do vCenter Server e do NSX poderão apresentar erros de conexão devido a problemas de verificação de SSL. Nesse caso, após o upgrade, você tem duas opções:

- 1 Execute o comando `trust-infra-certs` da ferramenta de gerenciamento de células para importar automaticamente todos os certificados para o armazenamento centralizado de certificados. Consulte [importar os certificados de Endpoints dos recursos do vSphere](#).
 - 2 Na interface do usuário do Service Provider Admin Portal, selecione cada instância do vCenter Server e do NSX e insira novamente as credenciais ao aceitar o certificado.
-

Atualizar cada NSX Manager associado a um sistema vCenter Server anexado

Antes de atualizar um vCenter Server e hosts ESXi registrados no VMware Cloud 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 VMware Cloud Director, mesmo que as células do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director e o NSX Manager, você deve atualizar os sistemas vCenter Server e os hosts ESXi que estão registrados no VMware Cloud 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 Na barra de navegação superior do VMware Cloud Director Service Provider Admin Portal, em **Recursos**, selecione **Recursos do vSphere**.
 - b No painel esquerdo, clique em **Instâncias do vCenter Server**.
 - c Selecione o botão de opção ao lado da instância 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 VMware Cloud Director.
 - a Na barra de navegação superior, 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 VMware Cloud Director.
 - a Na barra de navegação superior do VMware Cloud Director Service Provider Admin Portal, em **Recursos**, selecione **Recursos do vSphere**.
 - b No painel esquerdo, clique em **Instâncias do vCenter Server**.
 - 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 VMware Cloud 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/br/>.
- Para usar o VMware Cloud Director para fazer upgrade do edge gateway do NSX, você deve operar no objeto de rede do VMware Cloud Director ao qual o Edge oferece suporte:
 - Um upgrade apropriado de um Edge Gateway ocorre automaticamente quando você usa o VMware Cloud Director ou a API do VMware Cloud Director 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 VMware Cloud Director*.

Próximo passo

Repita esse procedimento para os outros sistemas vCenter Server registrados na sua instalação do VMware Cloud Director.

Referência da ferramenta de gerenciamento de células

5

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 VMware Cloud 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@cell11 /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 VMware Cloud 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.

- [Desativar o acesso do provedor de serviços ao endpoint da API herdada](#)

A partir do VMware Cloud Director 10.0, você pode usar endpoints separados de login do VMware Cloud Director OpenAPI para o provedor de serviços e de acesso de tenant ao VMware Cloud 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 VMware Cloud Director usando o subcomando `reconfigure-database` da ferramenta de gerenciamento de célula.

- [Detectar e reparar dados corrompidos do agendador](#)

O VMware Cloud 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.

- [Gerando certificados autoassinados para os endpoints de proxy do console e HTTPS](#)

Use o comando `generate-certs` da ferramenta de gerenciamento de célula para gerar certificados SSL autoassinados para os endpoints de proxy do console e HTTPS.

- [Substituindo certificados para os endpoints de proxy de console e HTTPS](#)

Use o comando `certificates` da ferramenta de gerenciamento de célula para substituir certificados SSL para os endpoints de proxy de console e HTTPS.

- [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 VMware Cloud Director.

- [Importar os certificados de endpoints dos recursos do vSphere](#)

Após o upgrade, use o comando `trust-infra-certs` da ferramenta de gerenciamento de células para coletar e importar certificados dos recursos do vSphere no seu ambiente para o banco de dados do VMware Cloud Director.

- [Configurar uma lista de negação para conexão de teste](#)

Após a instalação ou o upgrade, use o comando `manage-test-connection-blacklist` da ferramenta de gerenciamento de células para bloquear o acesso a hosts internos antes de fornecer aos tenants acesso à rede do VMware Cloud Director.

- [Visualizar o status FIPS de todas as células ativas](#)

Começando com o VMware Cloud Director 10.2.2, para verificar o status FIPS de todas as células ativas do VMware Cloud Director, você pode usar o comando `fips-status`. O comando não mostra o status FIPS do dispositivo VMware Cloud 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](#)

Para configurar o conjunto de protocolos SSL que a célula oferece para uso durante o processo de handshake de SSL, use o comando `ssl-protocols` da ferramenta de gerenciamento de células.

- [Configurar a coleção e a publicação de métricas](#)

Você pode usar o comando `configure-metrics` da ferramenta de gerenciamento de células 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 VMware Cloud Director, poderá usar o comando `recover-password` da ferramenta de gerenciamento de célula para recuperar a senha do administrador do sistema do VMware Cloud 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.

- [Configurando modelos de e-mail](#)

Para gerenciar os modelos que o sistema usa ao criar alertas por e-mail, você pode usar o comando `manage-email` da ferramenta de gerenciamento de célula.

- [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 VMware Cloud 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 VMware Cloud Director](#)

Para visualizar e atualizar os endereços IP e as entradas DNS válidos para as células do VMware Cloud Director em seu ambiente do VMware Cloud 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 VMware Cloud 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 VMware Cloud Director

Para atualizar os endereços IP das células do VMware Cloud Director em um cluster de alta disponibilidade de banco de dados, você deve usar a ferramenta de gerenciamento de células.

Configurar uma instalação do VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 5-1. 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 VMware Cloud 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 VMware Cloud Director.

Tabela 5-1. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `system-setup` (continuação)

Opção	Argumento	Descrição
<code>--installation-id</code>	Um número inteiro no intervalo de 1 a 63	O ID de instalação dessa instalação do VMware Cloud Director. O sistema usa o ID de instalação ao gerar endereços MAC para NICs virtuais. Observação Se você planeja criar redes estendidas entre instalações do VMware Cloud Director numa implantação multi-site, considere definir um ID exclusivo de instalação para cada instalação do VMware Cloud Director.
<code>--password</code>	A senha do administrador do sistema que você está criando. Necessária quando você usa a opção <code>--unattended</code> . Se você não usar a opção <code>--unattended</code> , 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 VMware Cloud Director.
<code>--serial-number</code>	O número de série (chave de licença) para essa instalação.	Opcional. Deverá ser um número de série válido do VMware Cloud Director.
<code>--system-name</code>	O nome a ser usado para a pasta do vCenter Server do VMware Cloud Director.	Essa instalação do VMware Cloud Director é representada por uma pasta com esse nome em cada vCenter Server no qual ela se registra.
<code>--unattended</code>	Nenhum	Opcional. O comando não solicita entrada adicional quando chamado com essa opção.
<code>--user</code>	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 VMware Cloud Director.

Exemplo: Especifique as configurações de sistema do VMware Cloud Director

Um comando como esse especifica todas as configurações de sistema de uma nova instalação do VMware Cloud 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@cell11 /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.
```

Desativar o acesso do provedor de serviços ao endpoint da API herdada

A partir do VMware Cloud Director 10.0, você pode usar endpoints separados de login do VMware Cloud Director OpenAPI para o provedor de serviços e de acesso de tenant ao VMware Cloud Director.

Você pode usar dois novos endpoints da OpenAPI para aumentar a segurança por meio da restrição do acesso ao VMware Cloud Director.

- `/cloudapi/1.0.0/sessions/provider` - Endpoint do OpenAPI para o login do provedor de serviços. Os tenants não podem acessar o VMware Cloud 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 VMware Cloud Director usando esse endpoint.

Por padrão, os administradores de provedor e os usuários da organização podem acessar o VMware Cloud 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.

Observação Quando você desativar o acesso do provedor de serviços ao endpoint de API `/api/sessions`, as solicitações desse provedor de serviços que fornecem apenas um token SAML no cabeçalho de autorização falharão para todos os endpoints de API herdados.

Procedimentos

- 1 Faça login ou conecte-se via SSH como `root` no sistema operacional de qualquer uma das células do VMware Cloud 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 VMware Cloud Director. Os tenants podem acessar o VMware Cloud 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 5-2. 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> .
<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 administrador do sistema do VMware Cloud 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 VMware Cloud Director no servidor.
<code>--status</code> (-t)	Nenhum	Exibe informações sobre o número de tarefas em execução na célula e o status da célula.

Tabela 5-2. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `cell` (continuação)

Opção	Argumento	Descrição
<code>--status-verbose</code> (<code>-tt</code>)	Nenhum	Exibe informações detalhadas sobre as tarefas em execução na célula e o status da célula.
<code>--username</code> (<code>-u</code>)	Nome de usuário do administrador do sistema do VMware Cloud 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 VMware Cloud Director executa uma série de aplicativos que fornecem serviços que os clientes do VMware Cloud Director necessitam. A célula inicia um subconjunto desses aplicativos por padrão. Normalmente, todos os membros desse subconjunto são necessários para suportar uma instalação do VMware Cloud 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 VMware Cloud Director

sysadmin-password

Senha do administrador do sistema do VMware Cloud Director. Você deverá usar a senha se ela contiver caracteres especiais.

Observação Você pode fornecer a senha de administrador do sistema do VMware Cloud 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 5-3. 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 VMware Cloud Director	Opcional. O comando solicitará a senha se você não a fornecer na linha de comando.
<code>--set</code>	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 <code>--enable</code> ou <code>--disable</code> para alterar o estado de inicialização de um único aplicativo.
<code>--username (-u)</code>	Nome de usuário do administrador do VMware Cloud Director.	Obrigatório se não especificar <code>--pid</code>

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@cell11 /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 VMware Cloud Director usando o subcomando `reconfigure-database` da ferramenta de gerenciamento de célula.

Durante a instalação do VMware Cloud Director ou o processo de implantação do dispositivo VMware Cloud Director, você configura as propriedades de tipo de banco de dados e conexões de banco de dados. Consulte [Instalar o VMware Cloud Director no Linux](#) e [Implantação e configuração inicial do dispositivo do VMware Cloud Director](#).

Após concluir a configuração do banco de dados do VMware Cloud Director, você pode atualizar as conexões de banco de dados usando o subcomando `reconfigure-database`. Você pode mover o banco de dados existente do VMware Cloud 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 [Instalar o VMware Cloud Director no Linux](#).

Se você não usar a opção `--pid`, deverá reiniciar a célula para aplicar as alterações.

Tabela 5-4. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `reconfigure-database`

Opção	Argumento	Descrição
<code>--help</code> (-h)	Nenhum	Fornece um resumo das opções disponíveis nessa categoria.
<code>--database-host</code> (-dbhost)	Endereço IP ou nome de domínio completo do host do banco de dados do VMware Cloud Director	Atualiza o valor da propriedade <code>database.jdbcUrl</code> . Importante O comando valida apenas o formato do valor.

Tabela 5-4. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `reconfigure-database` (continuação)

Opção	Argumento	Descrição
<code>--database-instance</code> (<code>-dbinstance</code>)	Instância do banco de dados SQL Server.	<p>Opcional. Usado se o tipo de banco de dados for <code>sqlserver</code>.</p> <p>Importante Se você incluir essa opção, deverá fornecer o mesmo valor que especificou ao configurar o banco de dados pela primeira vez.</p>
<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.	<p>Atualiza o valor da propriedade <code>database.jdbcUrl</code>.</p> <p>Importante O comando valida apenas o formato do valor.</p>
<code>--database-type</code> (<code>-dbtype</code>)	<p>O tipo de banco de dados. Um destes:</p> <ul style="list-style-type: none"> ■ <code>sqlserver</code> ■ <code>postgres</code> 	Atualiza o valor da propriedade <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 <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 VMware Cloud Director.
<code>--pid</code> (<code>-i</code>)	O ID de processo da célula.	<p>Opcional. Executa uma reconfiguração ativa em uma célula do VMware Cloud Director em execução. Não requer uma reinicialização da célula.</p> <p>Se for usado com o <code>--private-key-path</code>, você poderá executar o comando em células locais e remotas imediatamente.</p>

Tabela 5-4. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `reconfigure-database` (continuação)

Opção	Argumento	Descrição
<code>--private-key-path</code>	Nome do caminho para a Private Key da célula.	<p>Opcional. Todas as células no grupo de servidores encerram normalmente, atualizam suas propriedades de banco de dados e reiniciam.</p> <hr/> <p>Importante Todas as células devem permitir conexões SSH pelo superusuário sem uma senha.</p>
<code>--remote-sudo-user</code>	Um nome de usuário com direitos de sudo.	<p>Usado com a opção <code>--private-key-path</code> quando o usuário remoto é diferente de raiz.</p> <p>Para o dispositivo, você pode usar essa opção para o usuário postgres, por exemplo, <code>--remote-sudo-user=postgres</code>.</p>

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 VMware Cloud Director para ser usado como uma identidade com a qual os processos do VMware Cloud 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 VMware Cloud Director

Para alterar o nome de usuário e a senha do banco de dados do VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 5-5. 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 VMware Cloud Director.	Deve ser fornecido na linha de comando.
<code>--dbpassword</code>	Senha do usuário de banco de dados do VMware Cloud Director.	Solicitado se não for fornecido.

Gerando certificados autoassinados para os endpoints de proxy do console e HTTPS

Use o comando `generate-certs` da ferramenta de gerenciamento de célula para gerar certificados SSL autoassinados para os endpoints de proxy do console e HTTPS.

Cada grupo de servidores do VMware Cloud Director deve oferecer suporte a dois endpoints SSL: um para o serviço HTTPS e outro para o serviço de proxy do console. O endpoint do serviço HTTPS oferece suporte ao VMware Cloud Director Service Provider Admin Portal, ao VMware Cloud Director Tenant Portal e à API do VMware Cloud Director. 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 VMware Cloud 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 5-6. 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 5-6. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `generate-certs` (continuação)

Opção	Argumento	Descrição
<code>--issuer (-i)</code>	<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.
<code>--httpcert (-j)</code>	Nenhum	Gere um certificado para o endpoint HTTPS.
<code>--type (-t)</code>	<i>keystore-type</i>	Formato do armazenamento de chaves. O padrão é <i>PKCS12</i> . Você também pode criar um armazenamento de chaves <i>JCEKS</i> .
<code>--key-size (-s)</code>	<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.
<code>--keystore-pwd (-w)</code>	<i>keystore-password</i>	Senha para o armazenamento de chaves desse host.
<code>--out (-o)</code>	<i>keystore-pathname</i>	Nome de caminho completo para o armazenamento de chaves desse host.
<code>--consoleproxycert (-p)</code>	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@cell11 /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 HTTPS. 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 HTTPS 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@cell11 /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 VMware Cloud Director cria esse usuário e grupo.

Substituindo certificados para os endpoints de proxy de console e HTTPS

Use o comando `certificates` da ferramenta de gerenciamento de célula para substituir certificados SSL para os endpoints de proxy de console e HTTPS.

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 formatado PKCS12 ou 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 contendo certificados assinados, consulte [Criar certificados SSL autoassinados para o VMware Cloud 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 5-7. 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.
<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 formatado PKCS12 ou 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 formatado PKCS12 ou JCEKS referenciado pela opção <code>--keystore</code> . Substitui as opções <code>-kspassword</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@cell11 /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 VMware Cloud Director.

Antes que ele possa fazer uma conexão segura com um serviço externo, o VMware Cloud 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 5-8. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `import-trusted-certificates`

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--destination</code>	nome do caminho	Nome completo do caminho para o truststore de destino. O padrão será <code>/opt/vmware/vcloud-director/etc/certificates</code> se não for fornecido na linha de comando.
<code>--destination-password</code>	cadeia de caracteres	Senha para o truststore de destino. O padrão será o valor de <code>vcloud.ssl.truststore.password</code> se não for fornecido na linha de comando.

Tabela 5-8. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `import-trusted-certificates` (continuação)

Opção	Argumento	Descrição
<code>--destination-type</code>	tipo de armazenamento de chaves	Tipo de armazenamento de chaves do truststore de destino. Pode ser JKS ou JCEKS. O padrão é JCEKS.
<code>--force</code>	Nenhum	Substitui os certificados existentes no truststore de destino.
<code>--source</code>	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 VMware Cloud Director em `/opt/vmware/vcloud-director/etc/certificates`. O VMware Cloud 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
```

Importar os certificados de endpoints dos recursos do vSphere

Após o upgrade, use o comando `trust-infra-certs` da ferramenta de gerenciamento de células para coletar e importar certificados dos recursos do vSphere no seu ambiente para o banco de dados do VMware Cloud Director.

O comando `trust-infra-certs` da ferramenta de gerenciamento de células reúne automaticamente os certificados SSL dos recursos do vSphere no seu ambiente e os importa para o banco de dados do VMware Cloud Director.

Pré-requisitos

Verifique se as instâncias do vCenter Server e do NSX Manager para as quais você deseja importar os endpoints estão funcionando.

Procedimentos

- 1 Faça login ou conecte-se via SSH como raiz no sistema operacional da célula do VMware Cloud Director.
- 2 Execute o comando no formulário a seguir.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs options
```

Tabela 5-9. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando trust-infra-certs

Opção	Argumento	Descrição
--help (-h)	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
--vsphere	Nenhum	Solicita que você confie nos certificados de todas as instâncias do vCenter Server, NSX Data Center for vSphere e NSX-T Data Center registradas nesta instalação.
--trust	Nenhum	Opcional. Adiciona certificados ao truststore do VMware Cloud Director.
--inspect	Opcional. O caminho do arquivo.	Opcional. Exibe os certificados em um arquivo.
--unattended	Nenhuma	Opcional. O comando não solicita entrada adicional quando chamado com essa opção. Todos os certificados de infraestrutura são automaticamente confiáveis.

Exemplo: Confiar e importar todos os certificados de endpoints de recursos do vSphere

Para confiar e importar os certificados dos endpoints de recursos do vSphere sem precisar de mais informações, execute o comando com as seguintes opções.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs --vsphere --unattended
```

Configurar uma lista de negação para conexão de teste

Após a instalação ou o upgrade, use o comando `manage-test-connection-blacklist` da ferramenta de gerenciamento de células para bloquear o acesso a hosts internos antes de fornecer aos tenants acesso à rede do VMware Cloud Director.

Do VMware Cloud Director 10.1 em diante, os provedores de serviços e tenants podem usar a API do VMware Cloud Director para testar conexões com servidores remotos e para verificar a identidade do servidor como parte de um handshake SSL.

Para proteger a rede interna na qual uma instância do VMware Cloud Director é implantada de ataques maliciosos, os provedores de sistema podem configurar uma lista de negação de hosts internos que são inacessível para tenants.

Dessa forma, se um invasor mal-intencionado com acesso ao tenant tentar usar a API de teste de conexão do VMware Cloud Director para mapear a rede na qual o VMware Cloud Director está instalado, ele não poderá se conectar aos hosts internos na lista de bloqueios.

Após a instalação ou o upgrade e antes de fornecer aos tenants acesso à rede do VMware Cloud Director, use o comando `manage-test-connection-blacklist` da ferramenta de gerenciamento de células para bloquear o acesso do tenant aos hosts internos.

Procedimentos

- 1 Faça login ou conecte-se via SSH como raiz no sistema operacional da célula do VMware Cloud Director.
- 2 Execute o comando para adicionar uma entrada à lista de negação.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-test-connection-blacklist
option
```

Tabela 5-10. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `manage-test-connection-blacklist`

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--add-ip</code>	Endereço IPv4 ou IPv6	Adiciona um endereço IP à lista de negação.
<code>--add-name</code>	Um subdomínio ou um nome de domínio completo para um host	Adiciona um subdomínio ou um nome de domínio à lista de negação.
<code>--add-range</code>	Intervalo de endereços IPv4 ou IPv6 no formato CIDR ou hifenizado	Adiciona um intervalo de endereços IP à lista de negação.
<code>--list</code>	Nenhuma	Lista todas as entradas existentes com acesso negado.

Visualizar o status FIPS de todas as células ativas

Começando com o VMware Cloud Director 10.2.2, para verificar o status FIPS de todas as células ativas do VMware Cloud Director, você pode usar o comando `fips-status`. O comando não mostra o status FIPS do dispositivo VMware Cloud Director.

Para obter mais informações sobre como ativar o modo FIPS para o VMware Cloud Director no Linux, consulte [Ativar o modo FIPS](#) no *Guia do Portal de Administração do Provedor de Serviços do VMware Cloud Director*.

O comando `fips-status` exibe as informações de status FIPS para todas as células ativas, incluindo o nome da célula, o UUID, o endereço IP e o status FIPS.

Para obter informações sobre o modo FIPS do dispositivo, consulte [Visualizar o modo FIPS do dispositivo VMware Cloud Director](#).

Para receber os dados no formato JSON, você pode especificar o sinalizador `--json`.

Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH no sistema operacional da célula do VMware Cloud Director como **root**.
- 2 Visualize o status FIPS de todas as células ativas.

```
/opt/vmware/vcloud-director/bin/cell-management-tool fips-status
```

Tabela 5-11. Argumentos e opções da Ferramenta de gerenciamento de células, comando `fips-status`

Comando	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--json</code>	Nenhum	Exibe as informações no formato JSON.

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.

Observação O comando do `ciphers` só se aplica ao conjunto de certificados que o VMware Cloud Director usa para HTTPS e comunicações de proxy do console, e não aos certificados que o dispositivo do VMware Cloud Director usa para sua interface de usuário e API de gerenciamento de dispositivo.

Quando um cliente faz uma conexão SSL com uma célula do VMware Cloud 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 VMware Cloud Director, o script de instalação ou atualização examina os certificados da célula. Se qualquer um dos certificados for criptografado usando uma codificação que não esteja na lista de codificações permitidas, a instalação ou a atualização falhará. Você pode realizar as seguintes etapas para substituir os certificados e reconfigurar a lista de codificações permitidas:

- 1 Crie certificados que não usem codificações não autorizadas. Você pode usar o `cell-management-tool ciphers -a`, conforme mostrado no exemplo abaixo 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.

- Use o comando `cell-management-tool ciphers` para reconfigurar a lista de codificações permitidas e incluir todas as codificações necessárias para uso com os novos certificados.

Importante Como o console do VMRC requer o uso das codificações AES256-SHA e AES128-SHA, não é possível desautorizar os clientes do VMware Cloud 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 5-12. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `ciphers`

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--all-allowed (-a)</code>	Nenhuma	Liste todas as cifras com suporte do VMware Cloud Director.
<code>--compatible-reset (-c)</code> (Obsoleto)	Nenhum	Obsoleto. Use a opção <code>--reset</code> para redefinir a lista padrão de codificações permitidas.
<code>--disallow (-d)</code>	Lista separada por vírgulas de nomes de cifras.	<p>Não permitir as cifras na lista separada por vírgulas especificada. Toda vez que você executar essa opção, deverá incluir a lista completa de codificações que deseja desativar, pois a execução da opção substitui a configuração anterior.</p> <p>Importante Executar a opção sem nenhum valor ativa todas as cifras.</p> <p>Para exibir todas as cifras possíveis, execute a opção <code>-a</code>.</p> <p>Importante Você deve reiniciar a célula após a execução de <code>cifras--proibir</code>.</p>

Tabela 5-12. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `ciphers` (continuação)

Opção	Argumento	Descrição
<code>--list (-l)</code>	Nenhuma	Liste o conjunto de cifras permitidas que estão em uso no momento.
<code>--reset (-r)</code>	Nenhuma	Redefinir 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 usem uma codificação permitida.

Importante Você deve reiniciar a célula após a execução de **`cifras--redefinir`**.

Exemplo: Desautorizar duas codificações

O VMware Cloud Director inclui uma lista pré-configurada de codificações ativadas.

Este exemplo mostra como ativar codificações adicionais da lista de codificações permitidas e como desautorizar codificações que você não deseja usar.

- 1 Obtenha a lista das cifras que estão ativadas por padrão.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -l
```

A saída do comando retorna a lista de cifras ativadas.

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

- 2 Obtenha uma lista de todas as cifras que a célula pode oferecer durante um handshake de SSL.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
```

A saída do comando retorna a lista de cifras permitidas.

```
# ./cell-management-tool ciphers -a
Product default ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
```

```
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
```

3 Especifique as codificações a serem desativadas.

Se você executar o comando e não desativar explicitamente uma codificação, ela será ativada.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -d
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
```

4 Execute o comando para verificar a lista de codificações ativadas. Qualquer codificação que estiver ausente da lista será desativada.

```
root@bos1-vcd-static-211-90 [ /opt/vmware/vcloud-director/bin ]# ./cell-management-tool
ciphers -l
```

A saída retorna uma lista de todas as codificações que agora estão ativadas.

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
```

Gerenciar a lista de protocolos SSL permitidos

Para configurar o conjunto de protocolos SSL que a célula oferece para uso durante o processo de handshake de SSL, use o comando `ssl-protocols` da ferramenta de gerenciamento de células.

Quando um cliente faz uma conexão SSL com uma célula do VMware Cloud 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 ter vulnerabilidades graves de segurança.

Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH no sistema operacional da célula do VMware Cloud Director como **root**.
- 2 Execute o comando para gerenciar a lista de protocolos SSL permitidos.

```
cell-management-tool ssl-protocols options
```

Tabela 5-13. 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	Liste todos os protocolos SSL com suporte do VMware Cloud Director.
<code>--disallow (-d)</code>	Lista separada por vírgulas de nomes de protocolo SSL.	Reconfigure a lista de protocolos SSL não permitidos para aqueles especificados na lista. Toda vez que você executar essa opção, deverá incluir a lista completa de protocolos SSL que deseja desativar, pois a execução da opção substitui a configuração anterior.
<p>Importante Executar a opção sem nenhum valor ativa todos os protocolos SSL.</p> <p>Para exibir todos os protocolos SSL possíveis, execute a opção <code>-a</code>.</p> <p>Importante Você deve reiniciar a célula após a execução de <code>ssl-protocols--não permitir</code>.</p>		

Tabela 5-13. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `ssl-protocols` (continuação)

Opção	Argumento	Descrição
<code>--list (-l)</code>	Nenhuma	Liste o conjunto de protocolos SSL permitidos que estão em uso no momento.
<code>--reset (-r)</code>	Nenhuma	Redefina a lista de protocolos SSL configurados para o padrão de fábrica.
Importante Você deve reiniciar a célula após a execução de <code>ssl-protocols--redefinir</code> .		

Exemplo: Listar protocolos SSL permitidos e configurados e reconfigurar a lista de protocolos SSL não permitidos

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@cell11 /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@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

* TLSv1.2
* TLSv1.1
```

Para reconfigurar a lista de protocolos SSL não permitidos, use a opção `--disallow (-d)`.

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 vCenter Server anteriores à 5.5 Update 3e requerem o TLSv1.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -d
SSLv3,SSLv2Hello
```

Você deve reiniciar a célula depois de executar esse comando.

Configurar a coleção e a publicação de métricas

Você pode usar o comando `configure-metrics` da ferramenta de gerenciamento de células para configurar o conjunto de métricas a serem coletadas.

O VMware Cloud 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 VMware Cloud Director coleta. Use o subcomando `cell-management-toolcassandra` para configurar um banco de dados Cassandra Apache para uso como um repositório de métricas do VMware Cloud Director. Consulte [Configuração de um banco de dados de métricas do Cassandra](#).

Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH no sistema operacional da célula do VMware Cloud Director como **root**.
- 2 Configure as métricas coletadas pelo VMware Cloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool configure-metrics --metrics-config
pathname
```

Tabela 5-14. Argumentos e opções da Ferramenta de gerenciamento de células, subcomando `configure-metrics`

Comando	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--repository-host (obsoleto)</code>	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 VMware Cloud Director.
<code>--repository-port (obsoleto)</code>	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 VMware Cloud Director.
<code>--metrics-config</code>	nome do caminho	Caminho para o arquivo de configuração de métricas

- 3 Se a versão do VMware Cloud Director for 10.2.2 ou posterior, você também poderá ativar a publicação de métricas executando o seguinte comando.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

No VMware Cloud Director 10.2.2, a publicação de métricas está desativada por padrão.

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@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool configure-metrics --
metrics-config /tmp/metrics.groovy
```

O serviço de coleta de métricas do VMware Cloud 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 5-15. 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.

Tabela 5-15. Nomes de métrica (continuação)

Nome de métrica	Descrição
<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, o VMware Cloud Director relata métricas 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 5-16. Parâmetros de coleta de métricas

Nome do parâmetro	Valor	Descrição
<code>currentInterval</code>	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. O valor padrão é 20. O VMware Cloud Director oferece suporte a valores maiores que 20 apenas para métricas de Nível 1, conforme definido pelo vSphere Performance Manager.
<code>historicInterval</code>	Quantidade de segundos em número inteiro	O intervalo em segundos a ser usado ao consultar os valores de métricas históricas. O valor padrão é 20. O VMware Cloud Director oferece suporte a valores maiores que 20 apenas para métricas de Nível 1, conforme definido pelo vSphere Performance Manager.
<code>entity</code>	Um destes: <code>HOST</code> , <code>VM</code>	O tipo de objeto VC para o qual a métrica está disponível. O padrão é <code>VM</code> . Nem todas as métricas estão disponíveis para todas as entidades.
<code>instance</code>	Um identificador de instância <code>PerfMetricId</code> do vSphere Performance Manager	Indica se deve ser realizada a recuperação de dados para instâncias individuais de uma métrica, por exemplo, núcleos de CPU individuais, um agregado de todas as instâncias ou ambos. Um valor de <code>"*"</code> coleta todas as métricas, instâncias e agregados. Uma cadeia de caracteres vazia, <code>" "</code> , coleta apenas os dados agregados. Uma cadeia de caracteres específica como <code>"DISKFILE"</code> coleta dados apenas para essa instância. O padrão é <code>"*"</code> .

Tabela 5-16. Parâmetros de coleta de métricas (continuação)

Nome do parâmetro	Valor	Descrição
<code>minReportingInterval</code>	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 a granularidade dos relatórios quando a granularidade do intervalo de coleta não é suficiente. O padrão é 0, ou seja, nenhum intervalo de relatório dedicado.
<code>aggregator</code>	Um destes: AVERAGE, MINIMUM, MAXIMUM e SUMMATION	O tipo de agregação a ser executado durante o <code>minReportingInterval</code> . O padrão é 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 VMware Cloud 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 VMware Cloud Director. Use o subcomando `cell-management-tool configure-metrics` para ferramenta para configurar o conjunto de métricas a serem coletadas. Consulte [Configurar a coleção e a publicação 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 VMware Cloud Director e um banco de dados Cassandra Apache, use uma linha de comando da seguinte forma:

```
cell-management-tool cassandra options
```

Tabela 5-17. 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 Instalar e configurar um banco de dados Cassandra para armazenar dados de métricas de históricos .

Tabela 5-17. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `cassandra` (continuação)

Comando	Argumento	Descrição
<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 VMware Cloud Director.
<code>--clean</code>	Nenhum	Remova as definições de configuração do Cassandra do banco de dados do VMware Cloud Director.
<code>--configure</code>	Nenhum	Configure VMware Cloud 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 VMware Cloud Director no Cassandra como <i>cadeia de caracteres</i> . O padrão é <code>vcloud_metrics</code> .
<code>--offline</code>	Nenhum	Configure o Cassandra para uso pelo VMware Cloud Director, mas não teste a configuração por conexão com o VMware Cloud 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 VMware Cloud 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@cell11 /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 VMware Cloud Director, poderá usar o comando `recover-password` da ferramenta de gerenciamento de célula para recuperar a senha do administrador do sistema do VMware Cloud 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 VMware Cloud Director pode recuperar a senha do administrador do sistema do VMware Cloud Director.

Para recuperar a senha do administrador do sistema, use uma linha de comando da seguinte forma:

```
cell-management-toolrecover-passwordoptions
```

Tabela 5-18. 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 VMware Cloud Director.	Deve ser fornecido na linha de comando.
<code>--dbpassword</code>	Senha do usuário de banco de dados do VMware Cloud 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 5-19. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `fail-tasks`

Comando	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer 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@cell11 /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 VMware Cloud Director para o banco de dados VMware Cloud Director, onde elas são preservadas por 90 dias. Para preservar as mensagens de auditoria por mais tempo, você pode configurar serviços do VMware Cloud Director para enviar as mensagens de auditoria para o utilitário Linux `syslog` além do banco de dados do VMware Cloud Director.

O script de configuração do sistema permite que você especifique como as mensagens de auditoria são tratadas. Consulte "Configurar conexões de rede e de banco de dados" no *Guia de instalação, configuração e upgrade do VMware Cloud 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 5-20. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `configure-audit-syslog`

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornece um resumo dos comandos disponíveis nessa categoria.
<code>--disable (-d)</code>	Nenhuma	Desativar log de eventos de auditoria para <code>syslog</code> . Registra eventos de auditoria somente no banco de dados do VMware Cloud Director. Esta opção desfaz a definição dos valores de <code>audit.syslog.host</code> e das propriedades <code>audit.syslog.port</code> em <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 syslog	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 instalação, configuração e upgrade do VMware Cloud Director*.

Para alterar o host ao qual as mensagens syslog são enviadas, use um comando como este:

```
[root@cell11 /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.

Configurando modelos de e-mail

Para gerenciar os modelos que o sistema usa ao criar alertas por e-mail, você pode usar o comando `manage-email` da ferramenta de gerenciamento de célula.

Por padrão, o sistema envia 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 VMware Cloud Director 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 5-21. 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.

Tabela 5-21. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `manage-email` (continuação)

Opção	Argumento	Descrição
<code>--locale</code>	localidade do modelo	Por padrão, esse comando opera em modelos na localidade en-US. Para especificar uma localidade diferente, use essa opção.
<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>

Existem diferentes nomes de modelo permitidos que você pode usar para diferentes notificações por e-mail.

Tabela 5-22. Nomes de notificação por e-mail do VMware Cloud Director

Nome	Descrição	Quando o e-mail é enviado	Destinatários
VAPP_UNDEPLOY_NOTIFICATION_EXPIRE	Alerta quando a locação de tempo de execução do vApp está prestes a expirar. Quando o lease expirar, o VMware Cloud Director suspenderá ou desligará o vApp.	Antes que o lease de tempo de execução de um vApp expire, dependendo do tempo de alerta de locação de armazenamento e implantação configurados.	O proprietário do vApp, ou se o proprietário for um administrador do sistema , os administradores da organização receberão a notificação.
VAPP_STORAGE_NOTIFICATION_EXPIRE	Alerta quando a locação de armazenamento do vApp está prestes a expirar. Quando o lease expirar, o VMware Cloud Director excluirá o vApp.	Antes que a locação de armazenamento de um vApp expire, dependendo do tempo de alerta de locação de armazenamento e implantação configurados.	O proprietário do vApp, ou se o proprietário for um administrador do sistema , os administradores da organização receberão a notificação.
VAPP_STORAGE_NOTIFICATION_EXPIRE	Alerta quando a locação de armazenamento do vApp está prestes a expirar. Quando o lease expirar, o VMware Cloud Director marcará o vApp como expirado.	Antes que a locação de armazenamento de um vApp expire, dependendo do tempo de alerta de locação de armazenamento e implantação configurados.	O proprietário do vApp, ou se o proprietário for um administrador do sistema , os administradores da organização receberão a notificação.
VAPPTEMPLATE_STORAGE_NOTIFICATION_EXPIRE	Alerta quando a locação de armazenamento do modelo do vApp está prestes a expirar. Quando a locação expirar, o VMware Cloud Director excluirá o modelo do vApp.	Antes que a locação de armazenamento de um modelo do vApp expire, dependendo do tempo de alerta de locação de armazenamento e implantação configurados.	O proprietário do Modelo do vApp, ou se o proprietário for um administrador do sistema , os administradores da organização receberão a notificação.
VAPPTEMPLATE_STORAGE_NOTIFICATION_EXPIRE	Alerta quando a locação de armazenamento do modelo do vApp está prestes a expirar. Quando a locação expirar, o VMware Cloud Director excluirá o modelo do vApp.	Antes que a locação de armazenamento de um modelo do vApp expire,	O proprietário do Modelo do vApp, ou se o proprietário for um

Tabela 5-22. Nomes de notificação por e-mail do VMware Cloud Director (continuação)

Nome	Descrição	Quando o e-mail é enviado	Destinatários
VAPPTEMPLATE_STORAGE_NOTIFICATION_EXPIRE	Quando o lease expirar, o VMware Cloud Director marcará o modelo do vApp como expirado.	dependendo do tempo de alerta de locação de armazenamento e implantação configurados.	administrador do sistema , os administradores da organização receberão a notificação.
DISK_STORAGE_ALERT	Alerta de Armazenamento em disco (alerta vermelho)	Quando há pouco espaço em disco no repositório de dados e atinge o limite vermelho.	Administradores do sistema
DISK_STORAGE_ALERT_VDCS	Alerta de armazenamento em disco para VDCs de provedor. O e-mail contém os VDCs de provedor de lista usando o repositório de dados que tem um alerta vermelho devido ao pouco espaço no disco rígido.	Quando há pouco espaço em disco no repositório de dados e atinge o limite vermelho.	Administradores do sistema
VM_HW_UPGRADE_INVALID_POWERSTATE	Uma notificação sobre o estado de energia de uma VM.	Quando um usuário tenta atualizar a versão de hardware de uma VM.	O proprietário da VM, ou se o proprietário for um administrador do sistema , os administradores da organização receberão a notificação.
VM_UPDATE_NESTED_HV_INVALID_POWERSTATE	Para fazer upgrade do hardware virtual, você deve desligar a VM.		
FEDERATION_CERTIFICATE_SUCCESS_EXPIRE	Notificação de expiração do certificado de Federação enviada a todos os administradores da organização quando um certificado para um servidor SSO externo está prestes a expirar. Ele solicita que os administradores da organização baixem um novo certificado do servidor SSO e atualizem o VMware Cloud Director.	Se um certificado de federação expirar dentro de 7 dias a partir da data atual.	Administradores da organização
FEDERATION_CERTIFICATE_SUCCESS_EXPIRE_SUMMARY			
IPSEC_VPN_TUNNEL_ERROR	Erro de Túnel VPN (alerta vermelho)	Quando o túnel VPN não estiver operacional.	Administradores do sistema
IPSEC_VPN_TUNNEL_ERROR_SUMMARY			
IPSEC_VPN_TUNNEL_ENABLED	Túnel VPN ativado (alerta verde)	Quando o túnel VPN estiver funcionando novamente depois de não estar operacional.	Administradores do sistema
IPSEC_VPN_TUNNEL_ENABLED_SUMMARY			

Tabela 5-23. Modelos de e-mail não personalizáveis

Notificação	Quando o e-mail é enviado	Destinatários
Alerta por e-mail de vCenter Server reconectado	Quando um vCenter Server é reconectado.	Administradores do sistema
Alerta por e-mail de vCenter Server desconectado. O e-mail indica se um erro ou uma solicitação de usuário causou a desconexão do servidor do vCenter Server.	Quando um vCenter Server é desconectado.	Administradores do sistema
Alerta por e-mail de Conexão perdida com o AMQP. Alerta notificando que o VMware Cloud Director está desconectado do servidor AMQP.	Quando o RabbitMQ para de funcionar.	Administradores do sistema
Alerta por e-mail de Conexão de banco de dados interrompido	Quando o VMware Cloud Director está desconectado do banco de dados.	Administradores do sistema
Alerta por e-mail de Conexão do banco de dados restaurado	Quando o VMware Cloud Director é reconectado ao banco de dados.	Administradores do sistema
Alerta por e-mail de Host desconectado do switch	Quando um host é desconectado dos switches disponíveis.	Administradores do sistema
Alerta por e-mail de Host desconectado do switch virtual distribuído	Quando um host é desconectado dos switches virtuais distribuídos disponíveis.	Administradores do sistema
Alerta por e-mail de Erro LDAP	Durante a sincronização com o LDAP.	Administradores do sistema
Alerta por e-mail de Sincronização do usuário LDAP	Durante a renomeação de um usuário LDAP.	Administradores do sistema
Alerta por e-mail de Alteração de status de associações de sites	Os sites perderam a conexão recentemente, recuperaram a conexão ou ainda estão inativos.	Administradores do sistema

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@cell11 /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-vm`s 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 VMware Cloud Director.

As máquinas virtuais que são referenciadas no banco de dados do vCenter, mas não no banco de dados do VMware Cloud Director, são consideradas VMs órfãs, pois o VMware Cloud 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-vm`s permite que um administrador liste essas VMs para que elas possam ser removidas ou reimportadas para o VMware Cloud Director. Este comando tem provisão para especificar um armazenamento de confiança alternativo, que poderá ser necessário se você estiver trabalhando com instalações do VMware Cloud Director ou do vCenter que usam certificados autoassinados.

Use um comando com o seguinte formato:

```
cell-management-tool find-orphan-vm options
```

Tabela 5-24. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `find-orphan-vm`s

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 VMware Cloud Director para pesquisar VMs órfãs.

Tabela 5-24. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `find-orphan-vm` (continuação)

Opção	Argumento	Descrição
<code>--output-file</code>	nome do caminho ou <code>-</code>	Nome do caminho completo do arquivo no qual a lista de VMs órfãs deve ser gravada. Especifique um nome de caminho de <code>-</code> para gravar a lista na saída padrão.
<code>--password (-p)</code>	Obrigatório	Senha de administrador do sistema do VMware Cloud Director.
<code>--port</code>	Porta HTTPS do VMware Cloud Director.	Especifique isso somente se você não quiser que esse comando use a porta HTTPS padrão do VMware Cloud 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 VMware Cloud 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 VMware Cloud 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@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vm \
--host 10.20.30.40 -u vadmin -vc-name vcenter1 -vc-password P@55w0rd --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 5-25. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `configure-ceip`

Opção	Argumento	Descrição
<code>--help</code> (-h)	Nenhum	Fornecer um resumo dos comandos disponíveis nessa categoria.
<code>--disable</code>	Nenhuma	Sai do Programa de aperfeiçoamento da experiência do cliente da VMware.

Tabela 5-25. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `configure-ceip` (continuação)

Opção	Argumento	Descrição
<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 5-26. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `manage-config`

Opção	Argumento	Descrição
<code>--help (-h)</code>	Nenhum	Fornecer 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.

Tabela 5-26. Argumentos e opções de ferramenta de gerenciamento de célula, subcomando `manage-config` (continuação)

Opção	Argumento	Descrição
<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 VMware Cloud 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 5-27. Definições de configuração para otimização do catálogo

Definição de configuração	Valor padrão	Descrição
<code>vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit</code>	30	<p>O limite de itens de biblioteca que todos os catálogos publicados na instância do VMware Cloud Director podem baixar do vCenter Server para o VMware Cloud Director ao mesmo tempo.</p> <p>Se o número total de itens de biblioteca publicados para download na instância do VMware Cloud 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.</p>
<code>vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit</code>	30	<p>O limite dos itens de biblioteca que todos os catálogos inscritos em uma instância do VMware Cloud Director podem sincronizar ao mesmo tempo.</p> <p>Se o número total de itens de biblioteca inscritos para sincronização na instância do VMware Cloud Director for maior do que esse limite, os itens serão divididos em partes de acordo com esse limite e sincronizados em uma sequência.</p>
<code>contentLibrary.item.sync.batch.size</code>	10	<p>O limite dos itens de biblioteca que um único catálogo inscrito pode sincronizar ao mesmo tempo.</p> <p>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.</p>

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 VMware Cloud Director

Para visualizar e atualizar os endereços IP e as entradas DNS válidos para as células do VMware Cloud Director em seu ambiente do VMware Cloud Director, você pode usar o subcomando do `manage-config` da ferramenta de gerenciamento de célula.

Problema

Não é possível acessar o VMware Cloud Director Service Provider Admin Portal ou o VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director.

Durante a configuração da célula das implantações do dispositivo, a lista não é atualizada com os nomes DNS das células do VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 5-28. 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@cell11 /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 VMware Cloud 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 VMware Cloud Director, você define um ID de instalação. O VMware Cloud Director usa o ID de instalação para regenerar os endereços MAC para as interfaces de rede da máquina virtual. Duas instalações do VMware Cloud 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 VMware Cloud Director do grupo de servidores. O comando é executado no banco de dados do VMware Cloud 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 VMware Cloud Director. Antes de iniciar a regeneração, você deve desativar as atividades em todas as células no grupo de servidores.

Tabela 5-29. 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.

Observação Todas as células no grupo de servidores devem ser inativas. Para obter informações sobre a desativação das atividades em uma célula, consulte [Como gerenciar uma célula](#).

Tabela 5-29. 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. Observação Todas as células no grupo de servidores devem ser inativas. Para obter informações sobre a desativação das atividades em uma célula, consulte Como gerenciar uma célula .
<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 VMware Cloud 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@cell11 /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@cell11 /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 VMware Cloud Director

Para atualizar os endereços IP das células do VMware Cloud Director em um cluster de alta disponibilidade de banco de dados, você deve usar a ferramenta de gerenciamento de células.

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 localizar o endereço IP, você deve usar a API do appliance do VMware Cloud Director para anotar os IDs dos nós em espera no cluster. Consulte *Referência de esquemas de API do dispositivo do VMware Cloud Director* em <http://code.vmware.com>.

Procedimentos

- 1 Faça login diretamente ou usando um cliente SSH no sistema operacional de qualquer uma das células no cluster como **root**.
- 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 VMware Cloud Director estará em execução, e você poderá alterar o endereço IP do banco de dados sem reiniciar a célula do VMware Cloud 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 VMware Cloud 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
```

Coletar logs do VMware Cloud Director

6

O VMware Cloud Director fornece informações de log para cada célula de nuvem no seu grupo de servidores. Você pode visualizar os logs para monitorar as células e solucionar quaisquer problemas que encontrar durante a execução cotidiana do VMware Cloud Director.

Logs do VMware Cloud Director

Arquivo ou diretório do log	Descrição
/opt/vmware/vcloud-director/logs/cell.log	Saída do console da célula do VMware Cloud Director.
/opt/vmware/vcloud-director/logs/cell-management-tool	Mensagens do log de Ferramenta de gerenciamento de célula vindas da célula.
/opt/vmware/vcloud-director/logs/cell-runtime	Mensagens de log de tempo de execução da célula.
/opt/vmware/vcloud-director/logs/cloud-proxy	Mensagens de log de proxy de nuvem da célula.
/opt/vmware/vcloud-director/logs/console-proxy	Mensagens de log de proxy do console remoto da célula.
/opt/vmware/vcloud-director/logs/server-group-communications	Comunicações de grupo de servidor da célula.
/opt/vmware/vcloud-director/logs/statsfeeder	Recuperação de métrica de máquina virtual do vCenter Server e informações de armazenamento e mensagens de erro.
/opt/vmware/vcloud-director/logs/vcloud-container-debug.log	Mensagens de log da célula no nível de depuração.
/opt/vmware/vcloud-director/logs/vcloud-container-info.log	Mensagens de log informativas vindas da célula. Esse log também mostra avisos ou erros encontrados pela célula.
/opt/vmware/vcloud-director/logs/vmware-vcd-watchdog.log	Mensagens informativas de log vindas do watchdog da célula. Ele registra quando a célula para de responder, é reiniciada, etc.
/opt/vmware/vcloud-director/logs/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.
/opt/vmware/vcloud-director/logs/YYYY_MM_DD.request.log	Os logs de solicitação HTTP no formato de log comum do Apache.

Logs do dispositivo do VMware Cloud Director

O dispositivo do VMware Cloud Director apresenta alguns arquivos de log adicionais.

Arquivo de log	Descrição
/opt/vmware/var/log/firstboot	Contém informações de log relacionadas com a primeira inicialização do dispositivo.
/opt/vmware/var/log/vcd	Contém logs relacionados com a configuração do pacote de ferramentas do Replication Manager (<code>repmgr</code>), reconfiguração e sincronização do dispositivo.
/opt/vmware/var/log/vcd/pg	Contém logs relacionados com o backup do banco de dados do dispositivo incorporado.
/opt/vmware/etc/vami/ovfEnv.xml	Contém os parâmetros de implantação do OVF.
/var/vmware/vpostgres/current/pgdata/log	Contém logs relacionados com o banco de dados PostgreSQL incorporado.
/opt/vmware/var/log/vami/updatecli.log	Contém logs relacionados com os upgrades do dispositivo.

Use qualquer editor de texto, visualizador de texto ou ferramenta de terceiros para visualizar os logs.

Desinstalar o software VMware Cloud Director

7

Use o comando Linux `rpm` para desinstalar o software VMware Cloud 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-phonhome 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 VMware Cloud Director.