

Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director

Geändert am 8. April 2021
VMware Cloud Director 10.2

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2010-2021 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise.](#)

Inhalt

Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director™ 7

- 1 VMware Cloud Director-Architektur 8**
- 2 VMware Cloud Director-Hardware- und Softwareanforderungen 11**
 - Netzwerkkonfigurationsanforderungen für VMware Cloud Director 12
 - Empfehlungen für die Netzwerksicherheit 14
- 3 Bereitstellung, Upgrade und Verwaltung der VMware Cloud Director-Appliance 16**
 - Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration 16
 - Automatisches Failover der VMware Cloud Director-Appliance 20
 - Automatisches Fencing einer fehlgeschlagenen primären Zelle 22
 - Vorbereiten der VMware Cloud Director-Appliance-Bereitstellung 23
 - Vorbereiten des Übertragungsserverspeichers für die VMware Cloud Director-Appliance 23
 - Installieren und Konfigurieren von NSX Data Center for vSphere für VMware Cloud Director 25
 - Installieren und Konfigurieren von NSX-T Data Center für VMware Cloud Director 26
 - Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance 28
 - Größenrichtlinien für die VMware Cloud Director-Appliance 30
 - Voraussetzungen für die Bereitstellung der VMware Cloud Director-Appliance 35
 - Bereitstellen der VMware Cloud Director-Appliance unter Verwendung des vSphere Clients 36
 - Bereitstellen der VMware Cloud Director-Appliance mit dem VMware OVF Tool 43
 - Bereitstellen der VMware Cloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation 53
 - Erstellen und Importieren der von einer Zertifizierungsstelle signierten SSL-Zertifikate in die VMware Cloud Director-Appliance 55
 - Importieren von privaten Schlüsseln und den von einer Zertifizierungsstelle signierten SSL-Zertifikaten in die VMware Cloud Director-Appliance 59
 - Nach der Bereitstellung der VMware Cloud Director-Appliance 61
 - Ändern des Root-Kennworts der VMware Cloud Director-Appliance 66
 - Upgrade und Migration der VMware Cloud Director-Appliance 68
 - Upgrade der VMware Cloud Director-Appliance mithilfe eines Update-Pakets 72
 - Upgrade der VMware Cloud Director-Appliance mit dem VMware Update Repository 74
 - Rollback einer VMware Cloud Director-Appliance, wenn ein Upgrade fehlschlägt 77
 - Migrieren von VMware Cloud Director mit einer externen PostgreSQL-Datenbank auf eine VMware Cloud Director-Appliance 78
 - Nach dem Upgrade von VMware Cloud Director 83

Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist	84
Upgrade von vCenter Server-Systemen, ESXi-Hosts und NSX Edges	85
Verwaltung der VMware Cloud Director-Appliance	87
Sichern und Wiederherstellen der eingebetteten Datenbank der VMware Cloud Director-Appliance	87
Ändern des Failover-Modus der VMware Cloud Director-Appliance	96
Konfigurieren des externen Zugriffs auf die VMware Cloud Director-Datenbank	96
Aktivieren oder Deaktivieren des SSH-Zugriffs auf die VMware Cloud Director-Appliance	97
Aktivieren oder Deaktivieren des FIPS-Modus auf der VMware Cloud Director-Appliance	98
Konfigurieren des SNMP-Agenten der VMware Cloud Director-Appliance	101
Bearbeiten der DNS-Einstellungen der VMware Cloud Director-Appliance	108
Bearbeiten der statischen Routen für die Netzwerkschnittstellen der VMware Cloud Director-Appliance	109
Konfigurationsskripts in der VMware Cloud Director-Appliance	110
Verlängern der VMware Cloud Director-Appliance-Zertifikate	111
Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und VMware Cloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats	113
Ersetzen des Übertragungsserverspeichers für die VMware Cloud Director-Appliance	114
Erhöhen der Kapazität der eingebetteten PostgreSQL-Datenbank auf einer VMware Cloud Director-Appliance	115
Ändern der PostgreSQL-Konfigurationen in der VMware Cloud Director-Appliance	117
Aufheben der Registrierung einer aktiven Standby-Zelle in einem Datenbank-Hochverfügbarkeits-Cluster	118
Tauschen der Rollen der primären Zelle und einer Standby-Zelle in einem Datenbank-Hochverfügbarkeits-Cluster	118
Abonnieren von Ereignissen, Aufgaben und Metriken mithilfe eines MQTT-Clients	120
Automatische Skalierungsgruppen	121
Überwachen der Integrität des VMware Cloud Director-Appliance-Datenbankclusters	123
Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance	124
Anzeigen des Dienststatus der VMware Cloud Director-Appliance	126
Überprüfen des Verbindungsstatus eines Datenbank-Hochverfügbarkeits-Clusters	127
Überprüfen des Replizierungsstatus eines Knotens in einem Datenbank-Hochverfügbarkeits-Cluster	128
Überprüfen des Status von VMware Cloud Director-Diensten	130
Wiederherstellung des Datenbankclusters der VMware Cloud Director-Appliance	130
Wiederherstellen nach einem Ausfall der primären Zelle in einem Hochverfügbarkeits-Cluster	132
Wiederherstellen nach einem Ausfall einer Standby-Zelle in einem Hochverfügbarkeits-Cluster	134
Aufheben der Registrierung einer fehlgeschlagenen primären oder Standby-Zelle in einem Hochverfügbarkeits-Datenbankcluster	136
Behebung von Fehlern der Appliance	136

- Prüfen der Protokolldateien in der VMware Cloud Director-Appliance 137
- Die VMware Cloud Director-Zelle kann nach der Bereitstellung der Appliance nicht gestartet werden 137
- Die Wiederherstellung nach der NFS-Validierung schlägt während der anfänglichen Konfiguration der Appliance fehl 138
- Neukonfigurieren des VMware Cloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der VMware Cloud Director-Appliance fehl 143
- Der Standby-Knoten einer VMware Cloud Director-Appliance ist nicht mehr erreichbar 144
- Der Standby-Knoten einer VMware Cloud Director-Appliance ist nicht mehr angehängt 146
- Die Clusterintegrität weist auf ein SSH-Problem hin 148
- Verwenden der Protokolldateien zur Fehlerbehebung bei VMware Cloud Director-Updates und -Patches 153
- Suchen nach VMware Cloud Director-Updates schlägt fehl 153
- Installieren des neuesten Updates von VMware Cloud Director schlägt fehl 154

4 Installation, Upgrade und Verwaltung von VMware Cloud Director unter Linux 155

- Konfigurationsplanung 155
- Vorbereitung der Installation von VMware Cloud Director 156
 - Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux 156
 - Vorbereiten des Übertragungsserverspeichers für VMware Cloud Director unter Linux 158
 - Herunterladen und Installieren des öffentlichen Schlüssels von VMware 160
 - Installieren und Konfigurieren von NSX Data Center for vSphere für VMware Cloud Director 161
 - Installieren und Konfigurieren von NSX-T Data Center für VMware Cloud Director 162
- Installieren von VMware Cloud Director unter Linux 163
 - Installieren von VMware Cloud Director auf dem ersten Mitglied einer Servergruppe 165
 - Erstellen und Verwalten von SSL-Zertifikaten für VMware Cloud Director unter Linux 167
 - Konfigurieren der Netzwerk- und Datenbankverbindungen 175
 - Installieren von VMware Cloud Director auf einem weiteren Mitglied einer Servergruppe 184
- Nach dem Installieren von VMware Cloud Director 186
 - Anpassen öffentlicher Adressbücher für VMware Cloud Director unter Linux 187
 - Installieren und Konfigurieren einer Cassandra-Datenbank zum Speichern von historischen Metrikdaten 188
 - Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank 190
 - Installieren und Konfigurieren einer RabbitMQ AMQP Broker-Instanz 192
 - Abonnieren von Ereignissen, Aufgaben und Metriken mithilfe eines MQTT-Clients 193
 - Automatische Skalierungsgruppen 194
- Upgrade von VMware Cloud Director unter Linux 197
 - Durchführen eines koordinierten Upgrades einer VMware Cloud Director-Installation 200
 - Manuelles Upgrade einer VMware Cloud Director-Installation 203
 - Referenz zum Datenbank-Upgrade-Dienstprogramm 208
- Nach dem Upgrade von VMware Cloud Director 210

Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist 211

Upgrade von vCenter Server-Systemen, ESXi-Hosts und NSX Edges 212

5 Überblick über das Zellenverwaltungstool 215

Konfigurieren einer VMware Cloud Director-Installation 219

Deaktivieren des Dienstanbieterzugriffs auf den Legacy-API-Endpoint 221

Verwalten einer Zelle 222

Verwalten von Zellenanwendungen 224

Aktualisieren der Datenbankverbindungseigenschaften 226

Erkennen und Reparieren von beschädigten Scheduler-Daten 230

Generieren von selbstsignierten Zertifikaten für die HTTPS- und Konsolenproxy-Endpoints 230

Ersetzen der Zertifikate für die HTTPS- und Konsolenproxy-Endpoints 232

Importieren von SSL-Zertifikaten aus externen Diensten 234

Importieren von Endpoint-Zertifikaten aus vSphere-Ressourcen 235

Konfigurieren einer Negativliste für Testverbindungen 236

Anzeigen des FIPS-Status aller aktiven Zellen 237

Verwalten der Liste zulässiger SSL-Verschlüsselungen 238

Verwalten der Liste der zulässigen SSL-Protokolle 242

Konfigurieren der Erfassung und Veröffentlichung von Metriken 244

Konfigurieren einer Cassandra-Metrikendatenbank 248

Wiederherstellen des Kennworts für den Systemadministrator 250

Aktualisieren des Fehlerstatus einer Aufgabe 250

Konfigurieren der Behandlung von Überwachungsmeldungen 251

Konfigurieren von E-Mail-Vorlagen 253

Finden von verwaisten VMs 257

Beitreten zum Programm zur Verbesserung der Kundenzufriedenheit von VMware bzw. Verlassen dieses Programms 259

Aktualisieren von Anwendungskonfigurationseinstellungen 261

Konfigurieren von Katalogsynchronisierungsdrosselung 261

Fehlerbehebung bei fehlgeschlagenem Zugriff auf die VMware Cloud Director-Benutzeroberfläche 264

Debuggen der vCenter-VM-Erkennung 265

Erneutes Erzeugen von MAC-Adressen für ausgeweitete Multisite-Netzwerke 266

Aktualisieren der Datenbank-IP-Adressen auf VMware Cloud Director-Zellen 269

6 Erfassen von VMware Cloud Director-Protokollen 271

7 Deinstallieren der VMware Cloud Director-Software 273

Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director™

Das *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director* enthält Informationen zur Installation und zum Upgrade der Software VMware Cloud Director™ und zur Konfiguration der Software für die Verwendung mit VMware vSphere®, VMware NSX® for vSphere® und VMware NSX-T™-Datencenter.

Zielgruppe

Das *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director* richtet sich an alle Benutzer, die VMware Cloud Director-Software installieren oder aktualisieren möchten. Die Informationen in diesem Handbuch sind für erfahrene Systemadministratoren bestimmt, die mit Linux, Windows, IP-Netzwerken und vSphere vertraut sind.

VMware Cloud Director- Architektur

1

Eine VMware Cloud Director-Servergruppe besteht aus einem oder mehreren VMware Cloud Director-Servern, die auf Linux oder Bereitstellungen der VMware Cloud Director-Appliance installiert sind. Jeder Server in der Gruppe führt eine Sammlung von Diensten aus, die VMware Cloud Director-Zelle genannt werden. Alle Zellen nutzen gemeinsam eine einzige VMware Cloud Director-Datenbank und einen Übertragungsserverspeicher und stellen eine Verbindung zu den vSphere-Ressourcen und den Netzwerkressourcen her.

Wichtig Gemischte VMware Cloud Director-Installationen unter Linux und VMware Cloud Director-Appliance-Bereitstellungen in einer Servergruppe werden nicht unterstützt.

Um Hochverfügbarkeit für VMware Cloud Director zu gewährleisten, müssen Sie mindestens zwei VMware Cloud Director-Zellen in einer Servergruppe installieren. Wenn Sie einen Lastausgleichsdienst eines Drittanbieters verwenden, können Sie einen automatischen Failover ohne Ausfallzeit sicherstellen.

Sie können eine VMware Cloud Director-Installation mit mehreren VMware vCenter Server[®]-Systemen und den VMware ESXi[™]-Hosts, die diese verwalten, verbinden. Für Netzwerkdienste kann VMware Cloud Director NSX Data Center for vSphere verknüpft mit vCenter Server verwendet, oder Sie können NSX-T Data Center bei VMware Cloud Director registrieren. Eine Kombination aus NSX Data Center for vSphere und NSX-T Data Center wird ebenfalls unterstützt.

Abbildung 1-1. Diagramm der Architektur der VMware Cloud Director-Linux-Installation

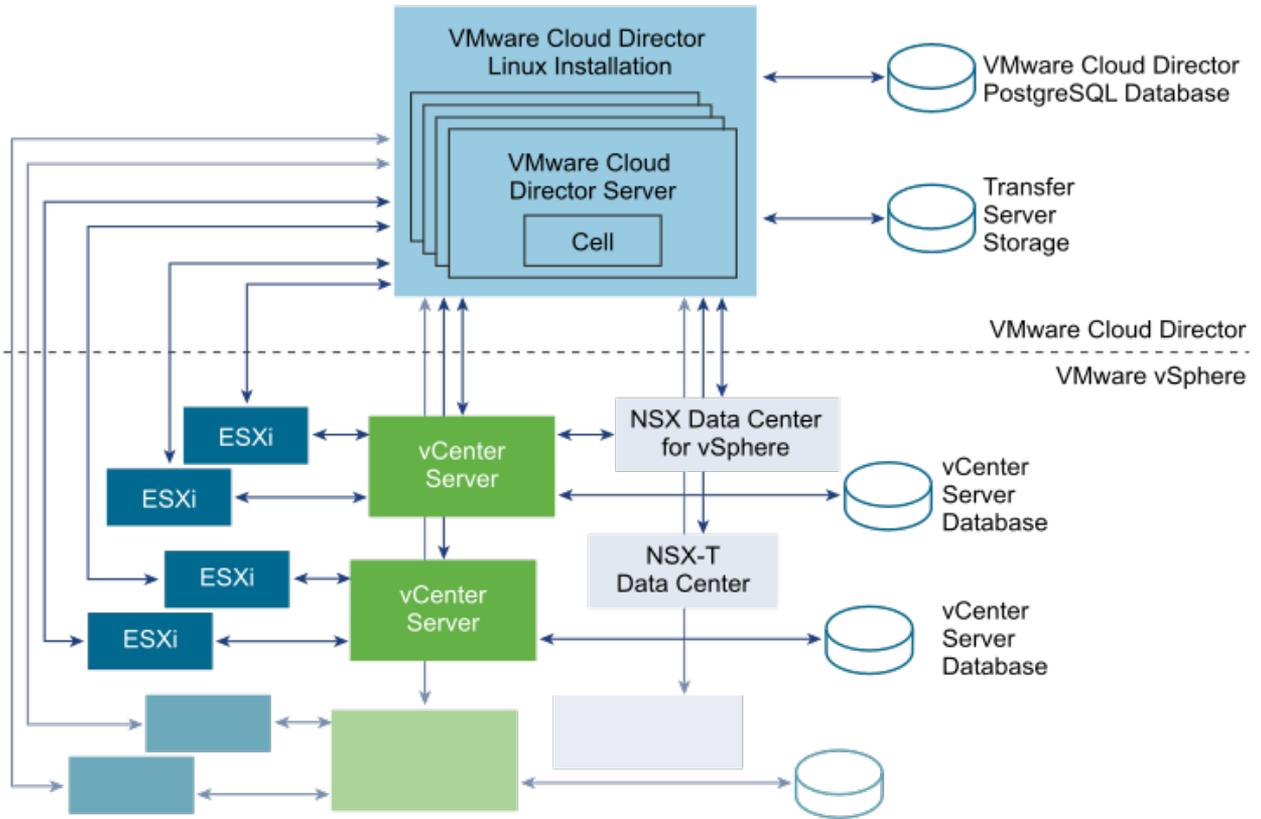
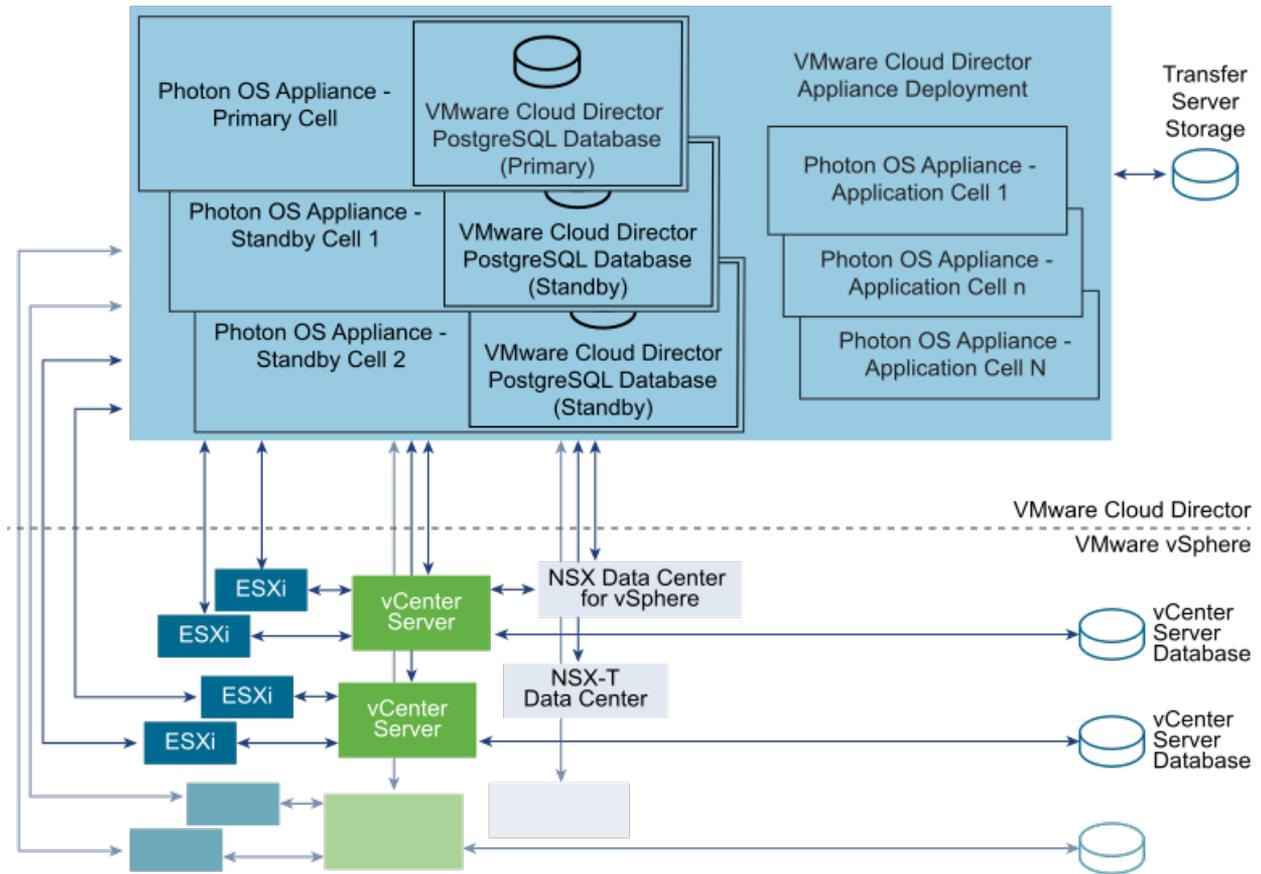


Abbildung 1-2. Diagramm der VMware Cloud Director-Appliance-Architektur



Eine auf Linux installierte VMware Cloud Director-Servergruppe verwendet eine externe Datenbank.

Eine VMware Cloud Director-Servergruppe, die aus Appliance-Bereitstellungen besteht, verwendet die eingebettete Datenbank im ersten Mitglied der Servergruppe. Sie können die Hochverfügbarkeit einer VMware Cloud Director-Datenbank konfigurieren, indem Sie zwei Instanzen der Appliance als Standby-Zellen in derselben Servergruppe bereitstellen. Weitere Informationen finden Sie unter [Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration](#).

Abbildung 1-3. VMware Cloud Director-Appliances mit einem Hochverfügbarkeits-Cluster mit eingebetteter Datenbank

Beim VMware Cloud Director-Installations- und Konfigurationsvorgang werden die Zellen erstellt, sie werden mit der gemeinsam genutzten Datenbank und dem Übertragungsserverspeicher verbunden, und das **Systemadministrator**-Konto wird erstellt. Anschließend stellt der **Systemadministrator** Verbindungen mit dem vCenter Server-System, den ESXi-Hosts und den NSX Manager- oder NSX-T Manager-Instanzen her.

Informationen zum Hinzufügen von vSphere-Ressourcen und Netzwerkressourcen finden Sie im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

VMware Cloud Director- Hardware- und Softwareanforderungen

2

Jeder Server in einer VMware Cloud Director-Servergruppe muss bestimmte Hardware- und Softwareanforderungen erfüllen. Außerdem muss für alle Mitglieder der Gruppe der Zugriff auf eine unterstützte Datenbank möglich sein. Jede Servergruppe benötigt Zugriff auf ein vCenter Server-System, eine NSX Manager-Instanz und einen oder mehrere ESXi-Hosts.

Kompatibilität mit anderen VMware-Produkten

Die neuesten Informationen zur Kompatibilität zwischen VMware Cloud Director und anderen VMware-Produkten finden Sie in den *VMware-Produkt-Interoperabilitätstabellen* unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

vSphere-Konfigurationsanforderungen

vCenter Server-Instanzen und ESXi-Hosts, die mit VMware Cloud Director verwendet werden sollen, müssen bestimmte Konfigurationsanforderungen erfüllen.

- vCenter Server-Netzwerke, die als externe VMware Cloud Director-Netzwerke oder Netzwerkpools verwendet werden sollen, müssen für alle Hosts in jedem Cluster verfügbar sein, der für die Verwendung durch VMware Cloud Director vorgesehen ist. Wenn diese Netzwerke für alle Hosts in einem Datacenter verfügbar gemacht werden, wird die Aufgabe, VMware Cloud Director neue vCenter Server-Instanzen hinzuzufügen, vereinfacht.
- vSphere Distributed Switches sind für isolierte Netzwerke und Netzwerkpools erforderlich, die von NSX Data Center for vSphere unterstützt werden.
- vCenter Server-Cluster, die mit VMware Cloud Director verwendet werden, müssen die vSphere DRS-Automatisierungsebene **Vollautomatisiert** aufweisen. Speicher-DRS kann bei Aktivierung mit jeder Automatisierungsebene konfiguriert werden.
- vCenter Server-Instanzen müssen ihren Hosts vertrauen. Alle Hosts in allen von VMware Cloud Director verwalteten Clustern müssen so konfiguriert werden, dass verifizierte Hostzertifikate erforderlich sind. Insbesondere müssen Sie für alle Hosts die passenden Fingerabdrücke bestimmen, vergleichen und auswählen. Weitere Informationen erhalten Sie unter "Konfigurieren von SSL-Einstellungen" in der Dokumentation zu *vCenter Server und Hostverwaltung*.

Unterstützte Plattformen, Datenbanken und Browser

In den *Versionshinweisen zu VMware Cloud Director* finden Sie Informationen zu Serverplattformen, Browsern, LDAP-Servern und Datenbanken, die von dieser Version von VMware Cloud Director unterstützt werden.

Festplattenspeicher, Arbeitsspeicher und CPU-Anforderungen

Weitere Informationen zu Festplattenspeicher, Arbeitsspeicher und CPU-Anforderungen finden Sie in den [Größenrichtlinien für die VMware Cloud Director-Appliance](#).

Freigegebener Speicher

NFS oder ein anderes freigegebenes Speichervolume für den VMware Cloud Director-Übertragungsdienst. Das Speichervolume muss erweiterbar und für alle Server in der Servergruppe zugänglich sein.

Dieses Kapitel enthält die folgenden Themen:

- [Netzwerkkonfigurationsanforderungen für VMware Cloud Director](#)
- [Empfehlungen für die Netzwerksicherheit](#)

Netzwerkkonfigurationsanforderungen für VMware Cloud Director

Der sichere und zuverlässige Betrieb von VMware Cloud Director ist von einem sicheren und zuverlässigen Netzwerk abhängig, das Forward-Lookups und Reverse-Lookups von Hostnamen, einen Netzwerkzeitdienst und andere Dienste unterstützt. Ihr Netzwerk muss diese Anforderungen erfüllen, bevor Sie mit der Installation von VMware Cloud Director beginnen.

Das Netzwerk, in dem die VMware Cloud Director-Server, die Datenbankserver, die vCenter Server-Systeme und die NSX-Komponenten miteinander verbunden sind, muss verschiedene Anforderungen erfüllen:

IP-Adressen

Jeder VMware Cloud Director-Server muss zwei unterschiedliche SSL-Endpoints unterstützen. Ein Endpoint ist für den HTTPS-Dienst. Der andere Endpoint ist für den Konsolen-Proxy-Dienst erforderlich. Diese Endpoints können separate IP-Adressen oder eine einzelne IP-Adresse mit zwei verschiedenen Ports sein. Sie können diese Adressen mithilfe von IP-Aliassen oder mehreren Netzwerkschnittstellen erstellen. Verwenden Sie nicht den Linux-Befehl `ip addr add` zum Erstellen der zweiten Adresse.

Die VMware Cloud Director-Appliance verwendet ihre `eth0`-IP-Adresse an dem benutzerdefinierten Port 8443 für den Konsolen-Proxy-Dienst.

Proxy-Adresse der Konsole

Die als der Konsolen-Proxy-Endpoint konfigurierte IP-Adresse darf sich nicht hinter einem SSL beendenden Lastenausgleichsdienst oder Reverse-Proxy befinden. Alle Anforderungen an den Konsolen-Proxy müssen direkt an die IP-Adresse des Konsolen-Proxys weitergeleitet werden.

Bei einer Installation mit einer einzelnen IP-Adresse können Sie die Konsolen-Proxy-Adresse über das Service Provider Admin Portal anpassen. Für die VMware Cloud Director-Appliance müssen Sie die Konsolen-Proxy-Adresse beispielsweise auf `vcloud.example.com:8443` anpassen.

Netzwerkzeitdienst

Sie müssen mithilfe eines Netzwerkzeitdiensts wie NTP die Uhren aller VMware Cloud Director-Server, d. h. auch des Datenbankservers, synchronisieren. Die maximal zulässige Abweichung der Uhren von synchronisierten Servern beträgt zwei Sekunden.

Für die Bereitstellungen der VMware Cloud Director-Appliance muss der für die Übertragungsfreigabe verwendete NFS-Server einen Netzwerkzeitdienst wie NTP verwenden, um seine Uhrzeit mit derjenigen der VMware Cloud Director-Appliances zu synchronisieren. Die maximal zulässige Abweichung der Uhren von synchronisierten Servern beträgt zwei Sekunden.

Serverzeitzonen

Alle VMware Cloud Director-Server, einschließlich des für die Übertragungsfreigabe verwendeten NFS-Servers und des Datenbankservers, müssen so konfiguriert werden, dass sie sich in derselben Zeitzone befinden.

Auflösung des Hostnamens

Alle von Ihnen während der Installation und Konfiguration angegebenen Hostnamen müssen von DNS mithilfe eines Forward- und Reverse-Lookups des vollqualifizierten Domännennamens oder des unqualifizierten Hostnamens aufgelöst werden können. Für einen Host namens `vcloud.example.com` beispielsweise müssen die beiden folgenden Befehle auf einem VMware Cloud Director-Host erfolgreich ausgeführt werden können:

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

Wenn der Host namens `vcloud.example.com` die IP-Adresse 192.168.1.1 hat, muss der folgende Befehl `vcloud.example.com` zurückgeben:

```
nslookup 192.168.1.1
```

Es ist ein Reverse-DNS-Lookup der `eth0`-IP-Adresse für die Appliance erforderlich. Der folgende Befehl muss in Ihrer Umgebung erfolgreich ausgeführt werden:

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

Empfehlungen für die Netzwerksicherheit

Voraussetzung für den sicheren Betrieb von VMware Cloud Director ist eine sichere Netzwerkumgebung. Konfigurieren und testen Sie diese Netzwerkumgebung, bevor Sie mit der Installation von VMware Cloud Director beginnen.

Verbinden Sie alle VMware Cloud Director-Server mit einem gesicherten und überwachten Netzwerk.

Informationen zu den von VMware Cloud Director verwendeten Netzwerkports und -protokollen finden Sie unter [VMware Ports and Protocols](#).

VMware Cloud Director-Netzwerkverbindungen weisen mehrere zusätzliche Anforderungen auf:

- Verbinden Sie VMware Cloud Director nicht direkt mit dem öffentlichen Internet. Schützen Sie die Netzwerkverbindungen von VMware Cloud Director stets mit einer Firewall. Nur Port 443 (HTTPS) muss für eingehende Verbindungen geöffnet sein. Die Ports 22 (SSH) und 80 (HTTP) können bei Bedarf ebenfalls für eingehende Verbindungen geöffnet sein. Zusätzlich dazu benötigt das `cell-management-tool` Zugriff auf die Loopback-Adresse der Zelle. Der gesamte übrige eingehende Datenverkehr von einem öffentlichen Netzwerk, einschließlich der Anforderungen an JMX (Port 8999), muss von der Firewall zurückgewiesen werden.

Informationen zu den Ports, die eingehende Pakete aus VMware Cloud Director-Hosts zulassen müssen, finden Sie unter [VMware Ports and Protocols](#).

- Verbinden Sie die für ausgehende Verbindungen verwendeten Ports nicht mit dem öffentlichen Netzwerk.

Informationen zu den Ports, die ausgehende Pakete aus VMware Cloud Director-Hosts zulassen müssen, finden Sie unter [VMware Ports and Protocols](#).

- Ab Version 10.1 können Dienstanbieter und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Negativliste interner Hosts, die für Mandanten, die die VMware Cloud Director-API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Negativliste, nachdem Sie die Installation oder das Upgrade von VMware Cloud Director durchgeführt haben und bevor Sie Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie unter [Konfigurieren einer Negativliste für Testverbindungen](#).
- Leiten Sie den Datenverkehr zwischen VMware Cloud Director-Servern und den folgenden Servern über ein dediziertes privates Netzwerk weiter.
 - VMware Cloud Director-Datenbankserver

- RabbitMQ
- Cassandra
- Leiten Sie den Datenverkehr soweit möglich zwischen vSphere-Servern, NSX und VMware Cloud Director über ein dediziertes privates Netzwerk weiter.
- Virtuelle Switches und Distributed Virtual Switches, die Provider-Netzwerke unterstützen, müssen voneinander isoliert sein. Sie können das physische Layer 2-Netzwerksegment nicht gemeinsam nutzen.
- Verwenden Sie NFSv4 für den Übertragungsdienstspeicher. Die am häufigsten verwendete NFS-Version NFSv3 bietet keine Transit-Verschlüsselung, was bei manchen Konfigurationen das Ermitteln oder Manipulieren von übertragenen Daten in Echtzeit ermöglicht. In NFSv3 vorhandene Bedrohungen werden im SANS-Whitepaper [NFS Security in Both Trusted and Untrusted Environments](#) (NFS-Sicherheit in vertrauenswürdigen und nicht vertrauenswürdigen Umgebungen) beschrieben. Weitere Informationen zum Konfigurieren und Sichern des VMware Cloud Director-Übertragungsdienstes finden Sie im VMware-Knowledgebase-Artikel [2086127](#).

Bereitstellung, Upgrade und Verwaltung der VMware Cloud Director-Appliance

3

Ab Version 9.7 enthält die VMware Cloud Director-Appliance eine eingebettete PostgreSQL-Datenbank mit einer Hochverfügbarkeitsfunktion. Wenn Sie die VMware Cloud Director-Appliance bereitstellen, aktualisieren oder migrieren, können Sie Verwaltungs-, Überwachungs-, Standardisierungs- oder Fehlerbehebungsvorgänge durchführen.

Dieses Kapitel enthält die folgenden Themen:

- [Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration](#)
- [Vorbereiten der VMware Cloud Director-Appliance-Bereitstellung](#)
- [Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance](#)
- [Upgrade und Migration der VMware Cloud Director-Appliance](#)
- [Nach dem Upgrade von VMware Cloud Director](#)
- [Verwaltung der VMware Cloud Director-Appliance](#)
- [Überwachen der Integrität des VMware Cloud Director-Appliance-Datenbankclusters](#)
- [Wiederherstellung des Datenbankclusters der VMware Cloud Director-Appliance](#)
- [Behebung von Fehlern der Appliance](#)

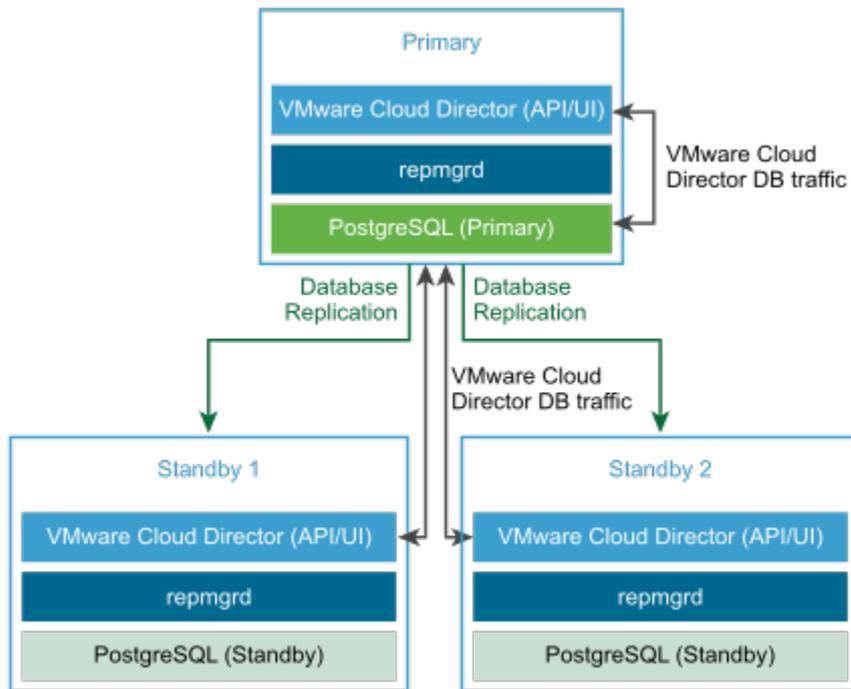
Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration

Die VMware Cloud Director-Appliance umfasst eine eingebettete PostgreSQL-Datenbank. Die eingebettete PostgreSQL-Datenbank enthält die Tool-Suite Replication Manager (repmgr), die eine Hochverfügbarkeitsfunktion (HA) für einen Cluster von PostgreSQL-Servern bereitstellt. Sie können eine Appliance-Bereitstellung mit einem Datenbank-HA-Cluster erstellen, der Failover-Funktionen für Ihre VMware Cloud Director-Datenbank bereitstellt.

Sie können die VMware Cloud Director-Appliance als primäre Zelle, Standby-Zelle oder VMware Cloud Director-Anwendungszelle bereitstellen. Weitere Informationen finden Sie unter [Bereitstellen der VMware Cloud Director-Appliance unter Verwendung des vSphere Clients](#), [Bereitstellen der VMware Cloud Director-Appliance mit dem VMware OVF Tool](#) oder [Bereitstellen der VMware Cloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation](#).

Um HA für Ihre VMware Cloud Director-Datenbank zu konfigurieren, können Sie beim Erstellen Ihrer Servergruppe einen Datenbank-HA-Cluster konfigurieren, indem Sie eine primäre und zwei Standby-Instanzen der VMware Cloud Director-Appliance bereitstellen. Sie können Ihre Servergruppe horizontal skalieren, indem Sie zusätzlich Anwendungszellen bereitstellen. Weitere Informationen finden Sie in der Abbildung [Abbildung 3-1. HA-Cluster der VMware Cloud Director-Appliance-Datenbank](#).

Abbildung 3-1. HA-Cluster der VMware Cloud Director-Appliance-Datenbank



Erstellen einer VMware Cloud Director-Appliance-Bereitstellung mit Datenbank-HA

Um eine VMware Cloud Director-Servergruppe mit einer Datenbank-HA-Konfiguration zu erstellen, führen Sie folgenden Workflow durch:

- 1 Stellen Sie die VMware Cloud Director-Appliance als primäre Zelle bereit.

Die primäre Zelle ist das erste Mitglied in der VMware Cloud Director-Servergruppe. Die eingebettete Datenbank ist als VMware Cloud Director-Datenbank konfiguriert. Der Datenbankname lautet `vcloud` und der Datenbankbenutzer ist `vcloud`.
- 2 Stellen Sie sicher, dass die primäre Zelle aktiv ist und ausgeführt wird.
 - a Melden Sie sich zum Überprüfen der Integrität des VMware Cloud Director-Diensts mit den Anmeldedaten des **Systemadministrators** bei dem VMware Cloud Director Service Provider Admin Portal unter `https://primary_eth0_ip_address/provider` an.

- b Melden Sie sich zum Überprüfen der Integrität der PostgreSQL-Datenbank als **root** bei der Verwaltungsbenutzeroberfläche der Appliance unter `https://primary_eth1_ip_address:5480` an.

Der primäre Knoten muss ausgeführt werden.

- 3 Stellen Sie zwei Instanzen der VMware Cloud Director-Appliance als Standby-Zellen bereit.

Die eingebetteten Datenbanken werden in einem Replizierungsmodus mit der primären Datenbank konfiguriert.

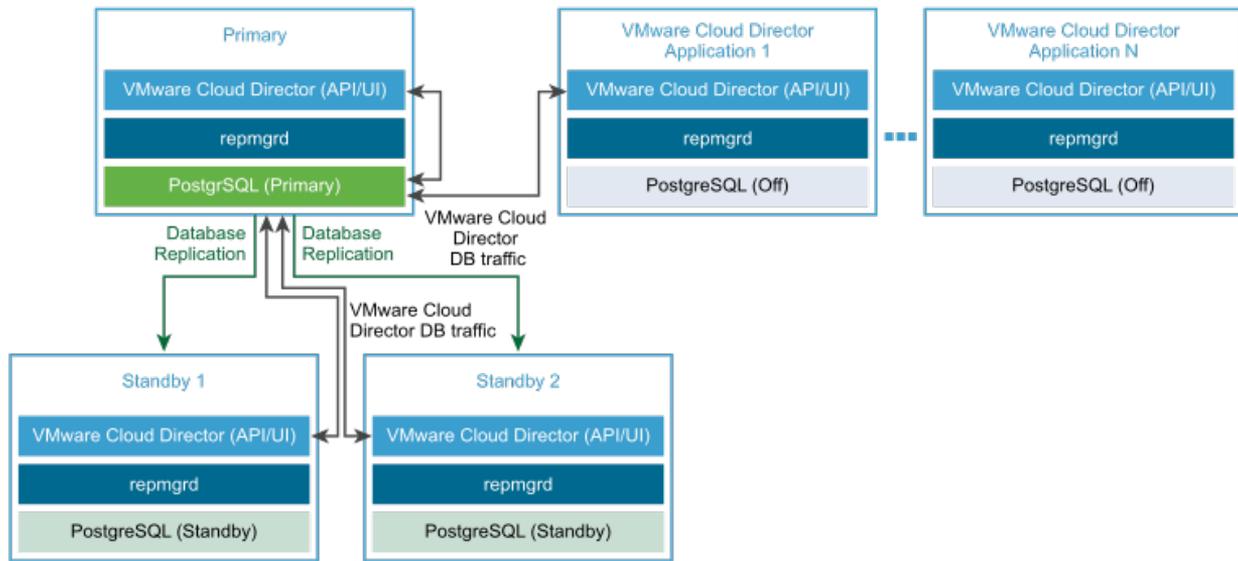
Hinweis Nach der anfänglichen Bereitstellung der Standby-Appliance beginnt der Replication Manager mit der Synchronisierung ihrer Datenbank mit der primären Appliance-Datenbank. Während dieser Zeit ist die VMware Cloud Director-Datenbank und damit auch die VMware Cloud Director-Benutzeroberfläche nicht verfügbar.

- 4 Stellen Sie sicher, dass alle Zellen im HA-Cluster ausgeführt werden.

Weitere Informationen finden Sie im [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

- 5 (Optional) Stellen Sie eine oder mehrere Instanzen der VMware Cloud Director-Appliance als VMware Cloud Director-Anwendungszellen bereit.

Die eingebetteten Datenbanken werden nicht verwendet. Die VMware Cloud Director-Anwendungszelle stellt eine Verbindung mit der primären Datenbank her.



Hinweis Wenn Ihr Cluster für automatisches Failover konfiguriert ist, müssen Sie nach der Bereitstellung einer zusätzlichen oder mehrerer zusätzlicher Zellen die Appliance-API verwenden, um den Failover-Modus auf `Automatic` zurückzusetzen. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API](#). Der standardmäßige Failover-Modus für neue Zellen lautet `Manual`. Wenn der Failover-Modus für die Knoten des Clusters inkonsistent ist, lautet der Failover-Modus des Clusters `Indeterminate`. Der Modus `Indeterminate` kann zwischen den Knoten und den einer alten primären Zelle folgenden Knoten zu inkonsistenten Clusterzuständen führen. Informationen zum Anzeigen des Failover-Modus des Clusters finden Sie unter [Anzeigen des Clusterzustands](#) und [des Failover-Modus der VMware Cloud Director-Appliance](#).

Erstellen einer VMware Cloud Director-Appliance-Bereitstellung ohne Datenbank-HA

Hinweis Sie können einen VMware Cloud Director-Cluster mit einer primären Zelle und ohne Standby-Zellen oder Anwendungszellen bereitstellen. VMware bietet keinen Support für Bereitstellungen mit einer einzelnen Zelle in einer Produktionsumgebung, da sie aus Datenbanksicht eine einzelne Fehlerquelle sind. Bereitstellungen mit einer Zelle erhalten keinen Support für Probleme im Zusammenhang mit der Leistung oder Stabilität.

Um einen VMware Cloud Director-Server ohne Datenbank-HA-Konfiguration zu erstellen, folgen Sie diesem Workflow:

- 1 Stellen Sie die VMware Cloud Director-Appliance als primäre Zelle bereit.

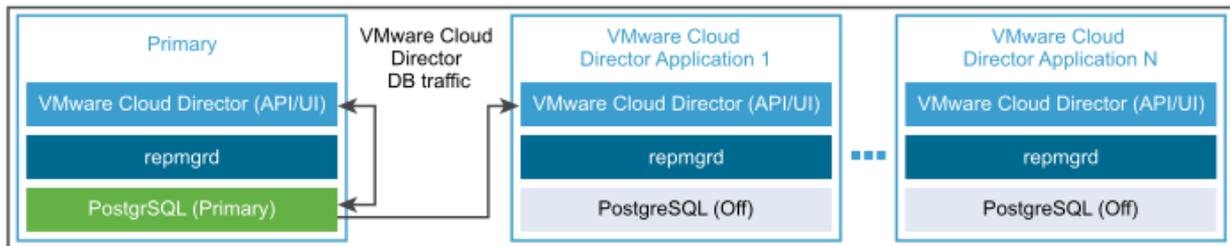
Die primäre Zelle ist das erste Mitglied in der VMware Cloud Director-Servergruppe. Die eingebettete Datenbank ist als VMware Cloud Director-Datenbank konfiguriert. Der Datenbankname lautet `vc1oud`, und der Datenbankbenutzer ist `vc1oud`.

- 2 Stellen Sie sicher, dass die primäre Zelle aktiv ist und ausgeführt wird.
 - a Melden Sie sich zum Überprüfen der Integrität des VMware Cloud Director-Diensts mit den Anmeldedaten des **Systemadministrators** bei dem VMware Cloud Director Service Provider Admin Portal unter `https://primary_eth0_ip_address/provider` an.
 - b Melden Sie sich zum Überprüfen der Integrität der PostgreSQL-Datenbank als **root** bei der Verwaltungsbenuer Oberfläche der Appliance unter `https://primary_eth1_ip_address:5480` an.

Der primäre Knoten muss ausgeführt werden.

- 3 (Optional) Stellen Sie eine oder mehrere Instanzen der VMware Cloud Director-Appliance als VMware Cloud Director-Anwendungszellen bereit.

Die eingebettete Datenbank wird nicht verwendet. Die VMware Cloud Director-Anwendungszelle stellt eine Verbindung mit der primären Datenbank her.



Automatisches Failover der VMware Cloud Director-Appliance

Ab VMware Cloud Director 10.1 können Sie bei Ausfall des primären Datenbankdiensts VMware Cloud Director aktivieren, um ein automatisches Failover auf eine neue primäre Zelle durchzuführen.

Durch das automatische Failover entfällt die Notwendigkeit, dass ein Administrator die Failover-Aktion initiiert, wenn der primäre Datenbankdienst seine Funktionen aus irgendeinem Grund nicht ausführen kann. Standardmäßig ist der Failover-Modus auf „Manuell“ festgelegt. Sie können den Failover-Modus mithilfe der VMware Cloud Director-Appliance-API auf „Automatisch“ oder „Manuell“ festlegen. Weitere Informationen dazu finden Sie im *API-Schema-Referenz für VMware Cloud Director-Appliance*.

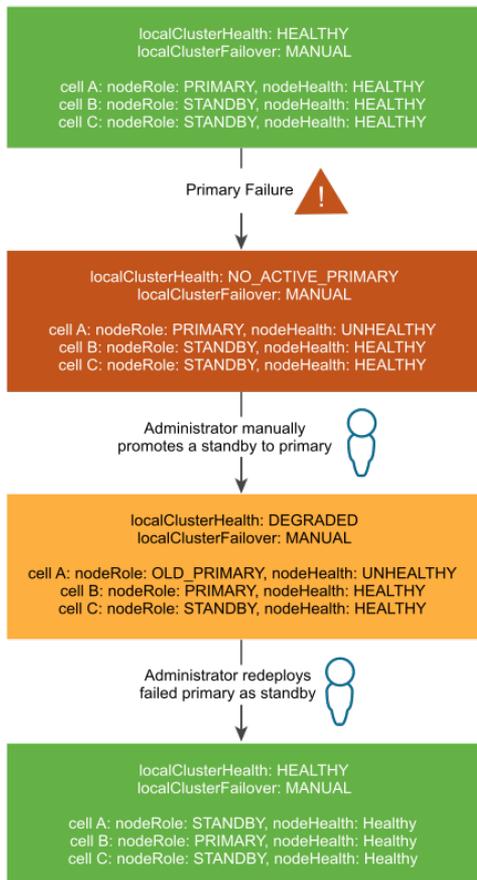
Hinweis Wenn Ihr Cluster für automatisches Failover konfiguriert ist, müssen Sie nach der Bereitstellung einer zusätzlichen oder mehrerer zusätzlicher Zellen die Appliance-API verwenden, um den Failover-Modus auf `Automatic` zurückzusetzen. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API](#). Der standardmäßige Failover-Modus für neue Zellen lautet `Manual`. Wenn der Failover-Modus für die Knoten des Clusters inkonsistent ist, lautet der Failover-Modus des Clusters `Indeterminate`. Der Modus `Indeterminate` kann zwischen den Knoten und den einer alten primären Zelle folgenden Knoten zu inkonsistenten Clusterzuständen führen. Informationen zum Anzeigen des Failover-Modus des Clusters finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

Wenn die Umgebung über mindestens zwei aktive Standby-Zellen verfügt, wird bei einem Ausfall der primären Datenbank automatisch ein Datenbank-Failover initiiert. Nach dem Failover muss mindestens eine aktive Standby-Zelle vorhanden sein, damit die neue primäre Datenbank aktualisierbar ist. Unter normalen Umständen muss die Bereitstellung der VMware Cloud Director-Appliance zu jeder Zeit mindestens zwei aktive Standby-Zellen aufweisen. Wenn nur eine aktive Standby-Zelle für einen kurzen Zeitraum vorhanden ist, z. B. aufgrund des Ausfalls der primären Zelle und des Heraufstufens einer der Standby-Zellen, muss die alte fehlgeschlagene primäre Zelle so bald wie möglich durch eine neue Standby-Zelle ersetzt werden.

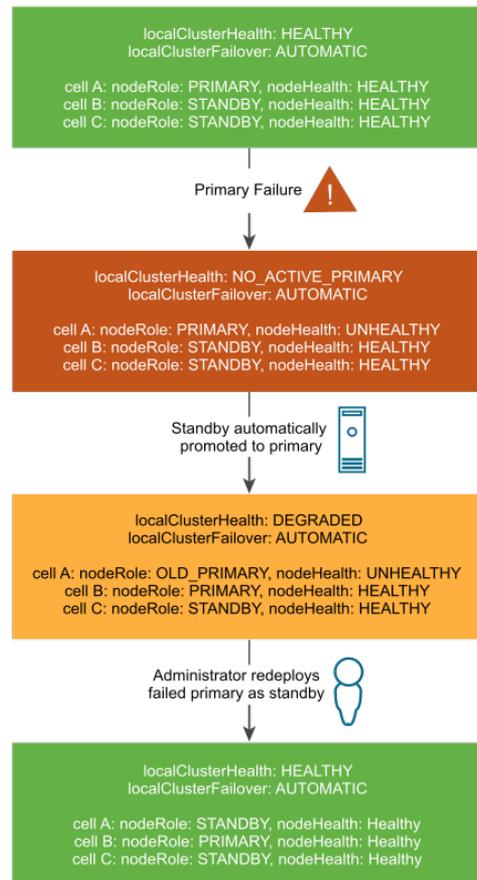
Wenn eine aktive primäre Zelle und mindestens zwei aktive Standby-Zellen vorhanden sind, wird davon ausgegangen, dass der Cluster sich im Zustand `Healthy` befindet. Sofern nur eine aktive primäre Zelle und nur ein aktive Standby-Zelle vorhanden sind, befindet sich der Cluster in dem Zustand `Degraded`. Tritt ein weiterer Datenbankausfall auf, während sich der Cluster im Zustand `Degraded` befindet, ist die primäre Zelle erst aktualisierbar, wenn eine weitere Standby-Zelle online geschaltet wird. Wenn die primäre Datenbank nicht aktualisierbar ist, ist VMware Cloud Director nicht verfügbar, da die VMware Cloud Director-Zellen die Datenbank erst aktualisieren können, wenn mindestens eine aktive Standby-Zelle zur Verarbeitung einer Streaming-Replizierung aus der primären Datenbank vorhanden ist. Das Konzept eines Clusterzustands von `Healthy` bzw. `Degraded` bleibt unverändert, unabhängig davon, ob Sie das manuelle oder automatische Failover aktivieren.

Abbildung 3-2. Manuelles und automatisches Failover der VMware Cloud Director-Appliance

Manual VMware Cloud Director Appliance Failover



Automatic VMware Cloud Director Appliance Failover



Automatisches Fencing einer fehlgeschlagenen primären Zelle

Wenn nach einem Ausfall einer primären Zelle eine neue Zelle zur primären Zelle heraufgestuft wird, grenzt VMware Cloud Director die alte primäre Zelle automatisch mit Fencing aus, um deren Neustart zu verhindern.

Wenn bei einem Failover eine fehlgeschlagene primäre Datenbank neu gestartet wird, nachdem eine neue Zelle zur primären Zelle heraufgestuft wurde, grenzt VMware Cloud Director die alte primäre Zelle automatisch mit Fencing aus. Diese Automatisierung verhindert das Split Brain-Syndrom, bei dem zwei aktive Datenbanken voneinander abweichen können. Die Fencing-Automatisierung stoppt und deaktiviert den vpostgres-Dienst auf dem alten primären Knoten. Danach können Sie den fehlgeschlagenen primären Knoten als Standby-Zelle erneut bereitstellen, um den Clusterzustand `Healthy` wiederherzustellen.

Weitere Informationen zum Anzeigen des Clusterzustands und des Failover-Modus finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

Vorbereiten der VMware Cloud Director-Appliance-Bereitstellung

Bevor Sie die VMware Cloud Director-Appliance bereitstellen, müssen Sie Ihre Umgebung vorbereiten.

Vorbereiten des Übertragungsserverspeichers für die VMware Cloud Director-Appliance

Sie müssen ein NFS oder ein anderes freigegebenes Speicher-Volumen für alle Server in einer VMware Cloud Director-Servergruppe zugänglich machen. VMware Cloud Director verwendet den Übertragungsserverspeicher für die Clusterverwaltung für die Appliance und bei der Bereitstellung von temporärem Speicher für Uploads, Downloads und Katalogelemente, die extern veröffentlicht oder abonniert werden.

Wichtig Die VMware Cloud Director-Appliance unterstützt nur den NFS-Typ des freigegebenen Speichers. Der Appliance-Bereitstellungsvorgang umfasst das Mounten des gemeinsam genutzten NFS-Übertragungsserverspeichers. Die VMware Cloud Director-Appliance validiert auch die meisten Details des NFS-Servers während der Bereitstellung, einschließlich Verzeichnisberechtigungen und Besitz. Sie müssen sicherstellen, dass ein gültiger NFS-Mount-Punkt vorhanden ist, auf den die VMware Cloud Director-Appliance-Instanzen zugreifen können.

Jedes Mitglied der Servergruppe mountet dieses Volumen am selben Mount-Punkt: `/opt/vmware/vcloud-director/data/transfer`. Der Speicher auf diesem Volumen wird auf viele Arten genutzt, einschließlich der folgenden:

- Während der Übertragung wird dieser Speicher durch Uploads und Downloads belegt. Wenn die Übertragung abgeschlossen ist, werden die Uploads und Downloads aus dem Speicher entfernt. Übertragungen, bei denen 60 Minuten lang keine Fortschritte erzielt werden, werden als „Abgelaufen“ markiert und vom System bereinigt. Da zu übertragende Bilder groß sein können, wird empfohlen, für diesen Zweck mindestens mehrere hundert Gigabyte zuzuweisen.
- Katalogobjekte in Katalogen, die extern veröffentlicht werden und für die Zwischenspeicherung von veröffentlichten Inhalten aktiviert ist, belegen diesen Speicher. Objekte von Katalogen, die extern veröffentlicht werden, aber keine Zwischenspeicherung ermöglichen, belegen diesen Speicher nicht. Wenn Sie Unternehmen in Ihrer Cloud die Möglichkeit bieten, Kataloge zu erstellen, die extern veröffentlicht werden, können Sie davon ausgehen, dass Hunderte oder sogar Tausende Katalogobjekte Speicherplatz auf diesem Volumen benötigen. Die Größe der einzelnen Katalogelemente entspricht ungefähr der Größe einer virtuellen Maschine im komprimierten OVF-Format.
- VMware Cloud Director speichert die Appliance-Datenbanksicherungen im Verzeichnis `pgdb-backup` in der Übertragungsfreigabe. Diese Sicherungspakete verbrauchen möglicherweise erheblichen Speicherplatz.
- Der Protokollpaket-Collector mit mehreren Zellen belegt diesen Speicherplatz.

- Appliance-Knotendaten und die Datei `response.properties` belegen diesen Speicherplatz.

Hinweis Das Volume des Übertragungsserverspeichers muss über Kapazitäten für zukünftige Erweiterungen verfügen.

Hinweis Ein NFS-Ausfall kann zu fehlerhaften Clusterfunktionalitäten bei der VMware Cloud Director-Appliance führen. Die Appliance-Verwaltungsbenuzoberfläche reagiert nicht mehr, während das NFS ausgefallen ist oder nicht erreicht werden kann. Weitere Funktionen, die möglicherweise davon betroffen sind: Fencing einer fehlgeschlagenen primären Zelle, Switchover, Heraufstufen einer Standby-Zelle usw.

Hinweis Wenn Sie Ubuntu- oder Debian-basierte Linux-Verteilungen für das NFS verwenden, schlägt die Erstellung von Datenbanksicherungen möglicherweise fehl.

Optionen für den freigegebenen Speicher

Ein herkömmlicher Linux-basierter NFS-Server oder andere Lösungen wie Microsoft Windows Server, die NFS-Funktion VMware vSAN-Dateidienst usw. können den freigegebenen Speicher bereitstellen. Ab vSAN 7.0 können Sie die Funktion vSAN-Dateidienst zum Exportieren von NFS-Freigaben unter Verwendung der Protokolle NFS 3.0 und NFS 4.1 verwenden. Weitere Informationen zum vSAN-Dateidienst finden Sie im Handbuch *Verwalten von VMware vSAN* in der [Produktdokumentation zu VMware vSphere](#).

Anforderungen an die Konfiguration des NFS-Servers

Es gibt bestimmte Anforderungen an die Konfiguration des NFS-Servers, damit VMware Cloud Director Dateien in einen NFS-basierten Übertragungsserverspeicher schreiben und daraus lesen kann. Wegen dieser Anforderungen kann der **vCloud**-Benutzer die standardmäßigen Cloud-Vorgänge durchführen, während der **root**-Benutzer für die Erfassung von Protokollen mit mehreren Zeilen zuständig ist.

- In der Exportliste für den NFS-Server muss jedes Servermitglied in der VMware Cloud Director-Servergruppe über Lese-/Schreibzugriff auf den freigegebenen Speicherort verfügen, der in der Exportliste angegeben ist. Diese Funktion ermöglicht dem **vCloud**-Benutzer, Dateien in den freigegebenen Speicherort zu schreiben und Dateien daraus zu lesen.
- Der NFS-Server muss über das **root**-Systemkonto allen Servern in der VMware Cloud Director-Servergruppe Lese-/Schreibzugriff auf den freigegebenen Speicherort erteilen. Diese Funktion ermöglicht das gleichzeitige Erfassen der Protokolle aus allen Zellen in einem einzelnen Paket, indem das `vmware-vcd-support`-Skript mit den entsprechenden Optionen für Mehrfachzellen verwendet wird. Sie können diese Anforderung erfüllen, indem Sie `no_root_squash` in der NFS-Exportkonfiguration für diesen freigegebenen Speicherort verwenden.

Beispiel für Linux-NFS-Server

Wenn der Linux-NFS-Server ein Verzeichnis mit dem Namen „vCDspace“ als Übertragungsspeicher für die VMware Cloud Director-Servergruppe mit dem Speicherort `/nfs/vCDspace` verwendet, müssen Sie zum Exportieren dieses Verzeichnisses sicherstellen, dass der zugehörige Besitzer und die Berechtigungen auf **root:root** und **750** festgelegt sind. Die Methode `no_root_squash` wird zum Erteilen von Lese-/Schreibzugriff auf den freigegebenen Speicherort für drei Zellen mit den Namen „vCD-Cell1-IP“, „vCD-Cell2-IP“ und „vCD-Cell3-IP“ verwendet. Sie müssen der Datei `/etc/exports` die folgenden Zeilen hinzufügen.

```
/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)
```

In der Exportzeile darf zwischen der IP-Adresse jeder Zelle und der unmittelbar folgenden linken Klammer kein Leerzeichen vorhanden sein. Wenn der NFS-Server neu gestartet wird, während die Zellen Daten in den freigegebenen Speicherort schreiben, wird mit der Option `sync` in der Exportkonfiguration verhindert, dass die Daten im freigegebenen Speicherort beschädigt werden. Ein Unterverzeichnis eines Dateisystems wird zuverlässig exportiert, wenn Sie die Option `no_subtree_check` in der Exportkonfiguration verwenden.

Für jeden Server in der VMware Cloud Director-Servergruppe müssen Sie über einen entsprechenden Eintrag in der Datei `/etc/exports` des NFS-Servers verfügen, damit sie alle diese NFS-Freigabe mounten können. Führen Sie nach dem Ändern der Datei `/etc/exports` auf dem NFS-Server den Befehl `exportfs -a` aus, um die NFS-Freigaben erneut zu exportieren.

Installieren und Konfigurieren von NSX Data Center for vSphere für VMware Cloud Director

Wenn Sie Ihre VMware Cloud Director-Installation so planen, dass Netzwerkressourcen von NSX Data Center for vSphere verwendet werden, müssen Sie NSX Data Center for vSphere installieren und konfigurieren und eine eindeutige Instanz von NSX Manager jeder Instanz von vCenter Server zuordnen, die in der VMware Cloud Director-Installation enthalten sein soll.

NSX Manager ist im Download für NSX Data Center for vSphere enthalten. Die neuesten Informationen zur Kompatibilität zwischen VMware Cloud Director und anderen VMware-Produkten finden Sie in den *VMware-Produkt-Interoperabilitätstabellen* unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. Informationen zu den Netzwerkanforderungen finden Sie unter [Netzwerkkonfigurationsanforderungen für VMware Cloud Director](#).

Wichtig Dieses Verfahren ist nur anzuwenden, wenn Sie VMware Cloud Director neu installieren. Wenn Sie eine vorhandene Installation von VMware Cloud Director aktualisieren, lesen Sie die Informationen unter [Upgrade von VMware Cloud Director unter Linux](#).

Voraussetzungen

Überprüfen Sie, ob jedes Ihrer vCenter Server-Systeme die Anforderungen für die Installation von NSX Manager erfüllt.

Verfahren

- 1 Führen Sie die Installationsaufgabe für die virtuelle NSX Manager-Appliance durch.

Weitere Informationen dazu finden Sie im *Installationshandbuch für NSX*.

- 2 Melden Sie sich bei der virtuellen NSX Manager-Appliance, die Sie installiert haben, an und überprüfen Sie die Einstellungen, die Sie während der Installation angegeben haben.

- 3 Ordnen Sie die virtuelle NSX Manager-Appliance, die Sie zusammen mit dem vCenter Server-System installiert haben, das Sie zu VMware Cloud Director hinzufügen möchten, Ihrer geplanten VMware Cloud Director-Installation zu.

- 4 Konfigurieren Sie die VXLAN-Unterstützung in den zugehörigen NSX Manager-Instanzen.

VMware Cloud Director erstellt VXLAN-Netzwerkpools, um Netzwerkressourcen für Anbieter-VDCs bereitzustellen. Wenn die VXLAN-Unterstützung nicht im zugeordneten NSX Manager konfiguriert wurde, wird bei den Anbieter-VDCs ein Netzwerkpool-Fehler angezeigt, und Sie müssen einen anderen Typ von Netzwerkpool erstellen und ihn dem Anbieter-VDC zuordnen. Weitere Informationen zum Konfigurieren der VXLAN-Unterstützung finden Sie im *Administratorhandbuch für NSX*.

- 5 (Optional) Wenn Edge Gateways im System verteiltes Routing bereitstellen sollen, richten Sie einen NSX Controller-Cluster ein.

Weitere Informationen dazu finden Sie im *Administratorhandbuch für NSX*.

Installieren und Konfigurieren von NSX-T Data Center für VMware Cloud Director

Wenn in Ihrer VMware Cloud Director-Installation Netzwerkressourcen von NSX-T Data Center verwendet werden sollen, müssen Sie mindestens eine NSX-T Data Center-Instanz installieren und konfigurieren.

Wichtig Um die NSX-T Data Center-Objekte und -Tools zu konfigurieren, verwenden Sie die vereinfachte Richtlinien-Benutzeroberfläche und die Richtlinien-APIs, die der vereinfachten Benutzeroberfläche entsprechen. Weitere Informationen hierzu finden Sie in der Übersicht zu NSX-T Manager im *NSX-T Data Center-Verwaltungshandbuch*.

Die neuesten Informationen zur Kompatibilität zwischen VMware Cloud Director und anderen VMware-Produkten finden Sie in den [VMware-Produkt-Interoperabilitätstabellen](#).

Informationen zu den Netzwerkanforderungen finden Sie unter [Netzwerkkonfigurationsanforderungen für VMware Cloud Director](#).

Dieses Verfahren ist nur anzuwenden, wenn Sie VMware Cloud Director neu installieren. Wenn Sie eine vorhandene Installation von VMware Cloud Director aktualisieren, lesen Sie die Informationen unter [Upgrade von VMware Cloud Director unter Linux](#).

Voraussetzungen

Machen Sie sich mit NSX-T Data Center vertraut.

Verfahren

- 1 Stellen Sie die virtuellen NSX-T Manager-Appliances bereit und konfigurieren Sie sie.
Weitere Informationen zur NSX-T Manager-Bereitstellung finden Sie im *NSX-T Data Center-Installationshandbuch*.
- 2 Erstellen Sie Transportzonen basierend auf Ihren Netzwerkanforderungen.
Weitere Informationen zu Transportzonen finden Sie im *NSX-T Data Center-Installationshandbuch*.

Hinweis

- 3 Stellen Sie Edge-Knoten und einen Edge-Cluster bereit und konfigurieren Sie diese.
Weitere Informationen zur NSX Edge-Erstellung finden Sie im *NSX-T Data Center-Installationshandbuch*.
- 4 Konfigurieren Sie die ESXi-Host-Transportknoten.
Weitere Informationen zum Konfigurieren eines Transportknotens für verwaltete Hosts finden Sie im *NSX-T Data Center-Installationshandbuch*.
- 5 Erstellen Sie ein Tier-0-Gateway.
Weitere Informationen zur Tier-0-Erstellung finden Sie im *NSX-T Data Center-Verwaltungshandbuch*.

Nächste Schritte

Nach der Installation von VMware Cloud Director haben Sie folgende Möglichkeiten:

- 1 Registrieren der NSX-T Manager-Instanz bei Ihrer Cloud
Informationen zur Registrierung einer NSX-T Manager-Instanz finden Sie im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.
- 2 Erstellen eines Netzwerkpools, der von einer NSX-T Data Center-Transportzone gestützt wird
Weitere Informationen zum Erstellen eines Netzwerkpools, der von einer NSX-T Data Center-Transportzone gestützt wird, finden Sie im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.
- 3 Importieren des Tier-0-Gateways als externes Netzwerk

Weitere Informationen zum Hinzufügen eines externen Netzwerks, das von einem logischen NSX-T Data Center-Tier-0-Router gestützt wird, finden Sie im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance

Sie können eine VMware Cloud Director-Servergruppe erstellen, indem Sie eine oder mehrere Instanzen der VMware Cloud Director-Appliance bereitstellen. Bereitstellen der VMware Cloud Director-Appliance unter Verwendung des vSphere Client oder des VMware OVF Tools.

Wichtig Gemischte VMware Cloud Director-Installationen unter Linux und VMware Cloud Director-Appliance-Bereitstellungen in einer Servergruppe werden nicht unterstützt.

Die VMware Cloud Director-Appliance ist eine vorkonfigurierte virtuelle Maschine, die für die Verwendung der VMware Cloud Director-Dienste optimiert ist.

Die Appliance wird mit einem Namen im Format `VMware Cloud Director-v` bereitgestellt. `v.v.v-nnnnn_OVF10.ova`, wobei `v.v.v` die Produktversion und `nnnnn` die Build-Nummer darstellt. Beispiel: `VMware Cloud Director-9.7.0.0-9229800_OVA10.ova`.

Das VMware Cloud Director-Appliance-Paket enthält die folgende Software:

- VMware Photon™ OS
- Die VMware Cloud Director-Gruppe der Dienste
- PostgreSQL 10

Die Größen „Primär-klein“ und „Standby-klein“ der VMware Cloud Director-Appliance sind für Lab- oder Testsysteme geeignet. Die Größen „Primär-groß“ und „Standby-groß“ erfüllen die Mindestgrößenanforderungen für Produktionssysteme. Je nach Arbeitslast müssen Sie möglicherweise weitere Ressourcen hinzufügen.

Wichtig Das Installieren von Drittanbieterkomponenten auf der VMware Cloud Director-Appliance wird nicht unterstützt. Sie können nur unterstützte VMware-Komponenten gemäß den [VMware-Produktinteroperabilitätstabellen](#) installieren. Beispielsweise können Sie eine unterstützte Version eines VMware vRealize® Operations Manager™ oder VMware vRealize® Log Insight™-Überwachungs-Agent installieren.

Appliance-Datenbankkonfiguration

Ab Version 9.7 enthält die VMware Cloud Director-Appliance eine eingebettete PostgreSQL-Datenbank mit einer Hochverfügbarkeitsfunktion (HA). Um eine Appliance-Bereitstellung mit einem Datenbank-HA-Cluster zu erstellen, müssen Sie eine Instanz der VMware Cloud Director-Appliance als primäre Zelle und zwei Instanzen als Standby-Zellen bereitstellen. Sie können zusätzliche Instanzen der VMware Cloud Director-Appliance in der Servergruppe als vCD-

Anwendungszellen bereitstellen, die nur die VMware Cloud Director-Gruppe von Diensten ohne die eingebettete Datenbank ausführen. vCD-Anwendungszellen stellen eine Verbindung mit der Datenbank in der primären Zelle her. Weitere Informationen finden Sie unter [Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration](#).

Standardmäßig verwendet die VMware Cloud Director-Appliance TLS anstatt des veralteten SSL für Datenbankverbindungen einschließlich Replizierung. Diese Funktion wird unmittelbar nach der Bereitstellung mit einem selbstsignierten PostgreSQL-Zertifikat aktiviert. Informationen zur Verwendung eines signierten Zertifikats von einer Zertifizierungsstelle (CA) finden Sie unter [Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und VMware Cloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats](#).

Hinweis Die VMware Cloud Director-Appliance unterstützt keine externen Datenbanken.

Appliance-Netzwerkconfiguration

Ab Version 9.7 wird die VMware Cloud Director-Appliance mit zwei Netzwerken (`eth0` und `eth1`) bereitgestellt, damit Sie den HTTP-Datenverkehr vom Datenbankdatenverkehr isolieren können. Verschiedene Dienste überwachen eine oder beide der entsprechenden Netzwerkschnittstellen.

Hinweis Die Netzwerke `eth0` und `eth1` müssen in separaten Subnetzen platziert werden.

Dienst	Port auf eth0	Port auf eth1
SSH	22	22
HTTP	80	n. v.
HTTPS	443	n. v.
PostgreSQL	n. v.	5432
Verwaltungsbenutzeroberfläche	5480	5480
Konsolen-Proxy	8443	n. v.
JMX	8998, 8999	n. v.
JMS/ActiveMQ	61616	n. v.

Nach der Erstellung der VMware Cloud Director-Appliance können Sie die Netzwerkfunktionen von vSphere verwenden, um eine neue Netzwerkschnittstellenkarte (NIC) hinzuzufügen. Weitere Informationen finden Sie unter [Hinzufügen eines Netzwerkadapters zu einer virtuellen Maschine](#) im *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Die VMware Cloud Director-Appliance unterstützt die Benutzeranpassung von Firewallregeln mithilfe von `iptables`. Um benutzerdefinierte `iptables`-Regeln hinzuzufügen, können Sie Ihre eigenen Konfigurationsdaten am Ende der Datei `/etc/systemd/scripts/iptables` hinzufügen.

Ab Version 10.1 können Dienstanbieter und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Verweigerungsliste interner Hosts, die für Mandanten, die die VMware

Cloud Director-API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Verweigerungsliste, nachdem Sie die Installation oder das Upgrade von VMware Cloud Director durchgeführt haben und bevor Sie Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie im [Konfigurieren einer Negativliste für Testverbindungen](#).

Größenrichtlinien für die VMware Cloud Director-Appliance

Je nach Ihren Anforderungen können Sie verschiedene Konfigurationen Ihrer VMware Cloud Director-Appliance-basierten Servergruppe und verschiedene Größen der virtuellen VMware Cloud Director-Appliance-Instanzen haben.

Übersicht

Um sicherzustellen, dass der Cluster ein automatisiertes Failover unterstützen kann, wenn ein Fehler in einer primären Zelle auftritt, muss die minimale VMware Cloud Director-Bereitstellung aus einer primären und zwei Standby-Zellen bestehen. Die Umgebung bleibt in jedem Fehlerszenario verfügbar, bei dem eine der Zellen aus irgendeinem Grund offline geschaltet wird. Wenn ein Standby-Fehler auftritt, erfolgt der Betrieb des Cluster bis zur erneuten Bereitstellung der ausgefallenen Zelle in einem voll funktionsfähigen Zustand mit einigen Leistungsbeeinträchtigungen. Weitere Informationen finden Sie im [Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration](#).

Die VMware Cloud Director-Appliance weist vier Größen auf, die Sie während der Bereitstellung auswählen können: Klein, Mittel, Groß und Extragroß (VVD). Die Appliance-Größe „Klein“ ist für Lab-Testzwecke geeignet, und in diesem Dokument wird die Appliance-Konfiguration „Klein“ nicht näher erläutert. Die Tabelle mit den Größenoptionen enthält die Spezifikationen für die verbleibenden Optionen und die am besten geeigneten Anwendungsfälle für eine Produktionsumgebung. Die Konfiguration „Extragroß“ stimmt mit dem Skalierungsprofil unter [VMware Validated Designs \(VVD\) for Cloud Providers](#) überein.

Um größere benutzerdefinierte Größen zu erstellen, können **Systemadministratoren** die Größe der bereitgestellten Zellen anpassen.

Die kleinste empfohlene Konfiguration für Produktionsbereitstellungen ist eine Drei-Knoten-Bereitstellung mit virtuellen Appliances mittlerer Größe.

Hinweis Sie können einen VMware Cloud Director-Cluster mit einer primären Zelle und ohne Standby-Zellen oder Anwendungszellen bereitstellen. VMware bietet keinen Support für Bereitstellungen mit einer einzelnen Zelle in einer Produktionsumgebung, da sie aus Datenbanksicht eine einzelne Fehlerquelle sind. Bereitstellungen mit einer Zelle erhalten keinen Support für Probleme im Zusammenhang mit der Leistung oder Stabilität.

Größenoptionen für die VMware Cloud Director-Appliance

Sie können den folgenden Entscheidungsleitfaden verwenden, um eine Schätzung der Appliance-Größe für Ihre Umgebung vorzunehmen.

	Mittel	Groß	Extragroß (VVD)
Empfohlene Anwendungsfälle	Lab- oder kleine Produktionsumgebungen	Produktionsumgebung	Produktion mit API-Integrationen und Überwachung
vRealize Operations Management Pack-Bereitstellung in der VMware Cloud Director-Umgebung	Nein	Nein	Ja
Aktivierung von Cassandra-VM-Metriken in VMware Cloud Director	Nein	Nein	Ja
Ungefähre Anzahl gleichzeitiger Benutzer oder Clients, die über einen Zeitraum von 30 Minuten maximal auf die API zugreifen.	< 50	< 100	< 100
Verwaltete VMs	5.000	5.000	15000

Konfigurationsdefinitionen

Hinweis primary-large- und standby-large-Appliances von VMware Cloud Director 9.7 und höher verfügen standardmäßig nicht über die 16 vCPUs, die für eine große HA-Clusterkonfiguration erforderlich sind. Wenn Sie eine große VMware Cloud Director-Appliance-Konfiguration verwenden möchten, müssen Sie nach der Bereitstellung die vCPUs der primären und Standby-Zellen manuell in 16 ändern.

	Mittel	Groß	Extragroß (VVD)
HA-Clusterkonfiguration	1 primäre Zelle + 2 Standby-Zellen	1 primäre Zelle + 2 Standby-Zellen + 1 Anwendungszelle	1 primäre Zelle + 2 Standby-Zellen + 2 Anwendungszellen
vCPUs der primären oder Standby-Zelle	8	16	24
vCPUs der Anwendungszelle	Nicht verfügbar	8	8
RAM der primären oder Standby-Zelle	16 GB	24 GB	32 GB
RAM der Anwendungszelle	Nicht verfügbar	8	8

	Mittel	Groß	Extragroß (VVD)
Verhältnis von vCPU zu physischem Kern	1:1	1:1	1:1
PostgreSQL-Anpassung in primären und Standby-Zellen	<pre>shared_buffers = '3GB'; effective_cache_size = '9GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '8';</pre>	<pre>shared_buffers = '5GB'; effective_cache_size = '15GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '16';</pre>	<pre>shared_buffers = '7GB'; effective_cache_size = '21GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '24';</pre>

So erkennen Sie, ob Ihr System unterdimensioniert ist

In einer VMware Cloud Director-Zelle wächst der CPU- oder Arbeitsspeicherverbrauch an und bleibt dauerhaft auf einem hohen Niveau, d. h. einem Niveau nahe der Kapazitätsgrenze. Die VMware Cloud Director-Zelle verliert möglicherweise auch die Verbindung zur Datenbank.

So erkennen Sie, ob die Anzahl der Zellen in Ihrem System nicht ausreicht

In den Dateien `vcloud-container-debug.log` und `cell-runtime.log` einer beliebigen der VMware Cloud Director-Zellen sehen Sie Einträge ähnlich dem folgenden: `org.apache.tomcat.jdbc.pool.PoolExhaustedException: [pool-jetty-XXXXX] Zeitüberschreitung: Pool leer. Abrufen einer Verbindung nicht möglich in 20 Sekunden, keine verfügbar.` Die VMware Cloud Director-Zelle verliert möglicherweise auch die Verbindung zur Datenbank.

Hinweis Basierend auf der standardmäßigen Datenbankverbindungskonfiguration sind alle Konfigurationen auf maximal 6 Zellen des primären, Standby- und Anwendungstyps beschränkt.

So passen Sie die Appliance-Größe an

Um die Größe der VMware Cloud Director-Appliance an eine der unterstützten Konfigurationen anzupassen, müssen Sie nach dem Ausführen der VMware Cloud Director-Appliance-Bereitstellungsfunktion das folgende Verfahren für alle Zellen ausführen.

- 1 Stellen Sie sicher, dass Sie über die erforderliche Anzahl an Zellen für die ausgewählte Konfiguration verfügen.
- 2 Passen Sie den Arbeitsspeicher und die vCPU aller Zellen an eine der unterstützten Konfigurationen an, die Sie benötigen.

Wichtig Die Menge an RAM und vCPU muss für alle primären und Standby-Zellen identisch sein.

- 3 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem der primären Appliance als **root** an.

4 Ändern Sie den Benutzer in **postgres**.

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

5 Aktualisieren Sie die Konfigurationsdatei `postgresql.auto.conf`, indem Sie die folgenden Befehle ausführen.

Konfigurationstyp	Beschreibung
Mittel	<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>
Groß	<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>
Besonders groß	<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 Kehren Sie zum **root**-Benutzer zurück, indem Sie den Befehl `exit` ausführen.

7 Starten Sie den `vpostgres`-Prozess neu.

```
systemctl restart vpostgres
```

8 Ändern Sie den Benutzer erneut in **postgres**.

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

- 9 Kopieren Sie für jeden Standby-Knoten die Datei `postgresql.auto.conf` auf den Knoten und starten Sie den `vpostgres`-Prozess neu.
 - a Kopieren Sie `postgresql.auto.conf` vom primären Knoten auf den Standby-Knoten.

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

- b Starten Sie den `vpostgres`-Prozess neu.

```
systemctl restart vpostgres
```

Um die Größe der VMware Cloud Director-Appliance an eine benutzerdefinierte Konfiguration anzupassen, müssen Sie nach dem Ausführen der VMware Cloud Director-Appliance-Bereitstellungsfunktion das folgende Verfahren für alle Zellen ausführen.

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem der primären Appliance als **root** an.
- 2 Um die vCPU-Informationen anzuzeigen und zu notieren, führen Sie den folgenden Befehl aus.

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

- 3 Um die RAM-Informationen anzuzeigen und zu notieren, führen Sie den folgenden Befehl aus. Der unten angegebene RAM ist in KB angegeben, und Sie müssen in GB konvertieren, indem Sie ihn durch 1.024.000 teilen.

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

- 4 Berechnen Sie den Wert für `shared_buffers` so, dass er ein Viertel des gesamten RAM minus 4 GB beträgt.

$$\text{shared_buffers} = 0,25 * (\text{gesamter RAM} - 4 \text{ GB})$$
 - 5 Berechnen Sie den Wert für `effective_cache_size` so, dass er drei Viertel des gesamten RAM minus 4 GB beträgt.

$$\text{effective_cache_size} = 0,75 * (\text{gesamter RAM} - 4 \text{ GB})$$
 - 6 Berechnen Sie den Wert für `max_worker_processes` so, dass er gleich der Anzahl an vCPUs ist.
 - 7 Ändern Sie den Benutzer in **postgres**.

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

- 8 Aktualisieren Sie die Konfigurationsdatei `postgresql.auto.conf`, indem Sie die folgenden Befehle ausführen und die berechneten Werte einsetzen.

```
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 Kehren Sie zum **root**-Benutzer zurück, indem Sie den Befehl `exit` ausführen.
- 10 Starten Sie den `vpostgres`-Prozess neu.

```
systemctl restart vpostgres
```

- 11 Ändern Sie den Benutzer erneut in **postgres**.

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

- 12 Kopieren Sie für jeden Standby-Knoten die Datei `postgresql.auto.conf` auf den Knoten und starten Sie den `vpostgres`-Prozess neu.

- a Kopieren Sie `postgresql.auto.conf` vom primären Knoten auf den Standby-Knoten.

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

- b Starten Sie den `vpostgres`-Prozess neu.

```
systemctl restart vpostgres
```

Voraussetzungen für die Bereitstellung der VMware Cloud Director-Appliance

Um eine erfolgreiche Bereitstellung der VMware Cloud Director-Appliance sicherzustellen, müssen Sie vor dem Starten der Bereitstellung einige Aufgaben und Vorabprüfungen durchführen.

- Überprüfen Sie, ob Sie Zugriff auf die VMware Cloud Director `.ova`-Datei haben.
- Bevor Sie die primäre Appliance bereitstellen, bereiten Sie einen gemeinsam genutzten NFS-Übertragungsdienstspeicher vor. Weitere Informationen finden Sie unter [Vorbereiten des Übertragungsserverspeichers für VMware Cloud Director unter Linux](#).

Hinweis Der gemeinsam genutzte Übertragungsdienstspeicher darf weder eine Datei `response.properties` noch ein Verzeichnis `appliance-nodes` enthalten.

- [Installieren und Konfigurieren einer RabbitMQ AMQP Broker-Instanz](#).

Methoden für die VMware Cloud Director-Appliance-Bereitstellung

- [Bereitstellen der VMware Cloud Director-Appliance unter Verwendung des vSphere Clients](#)
- [Bereitstellen der VMware Cloud Director-Appliance mit dem VMware OVF Tool](#)
- [Bereitstellen der VMware Cloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation](#)

Bereitstellen der VMware Cloud Director-Appliance unter Verwendung des vSphere Clients

Sie können die VMware Cloud Director-Appliance mit dem vSphere Client (HTML5) als OVF-Vorlage bereitstellen. Nach der Bereitstellung der OVF-Vorlage müssen Sie die Konfiguration in der Appliance Management-Benutzerschnittstelle abschließen.

Sie müssen das erste Mitglied einer VMware Cloud Director-Servergruppe als primäre Zelle bereitstellen. Sie können ein nachfolgendes Mitglied einer VMware Cloud Director-Servergruppe als Standby- oder VMware Cloud Director-Anwendungszelle bereitstellen. Weitere Informationen finden Sie unter [Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration](#).

Wichtig Gemischte VMware Cloud Director-Installationen unter Linux und VMware Cloud Director-Appliance-Bereitstellungen in einer Servergruppe werden nicht unterstützt.

Wenn Sie einem Datenbankcluster zusätzliche oder Ersatz-Appliances hinzufügen, müssen vCPU und RAM mit denen der vorhandenen primären und Standby-Zellen im Cluster übereinstimmen.

Die OVA-Version der neu bereitgestellten Standby-Appliance muss mit derjenigen der vorhandenen Appliances im Cluster identisch sein. Informationen zum Anzeigen der Version der ausgeführten Appliances finden Sie unter „Info über“ in der Appliance-Verwaltungsbenutzeroberfläche. Die Appliance wird mit einem Namen im Format `VMware Cloud Director-v bereitgestellt.v.v.v-nnnnnn_OVF10.ova`, wobei *v.v.v.v* die Produktversion und *nnnnnn* die Build-Nummer darstellt. Beispiel: `VMware Cloud Director-10.2.0.0-9229800_OVA10.ova`.

Informationen zum Bereitstellen von OVF-Vorlagen in vSphere finden Sie im Abschnitt *Verwaltung virtueller vSphere-Maschinen*.

Alternativ können Sie die Appliance mithilfe des VMware OVF Tool bereitstellen. Weitere Informationen finden Sie unter [Bereitstellen der VMware Cloud Director-Appliance mit dem VMware OVF Tool](#).

Hinweis Die Bereitstellung der VMware Cloud Director-Appliance in VMware Cloud Director wird nicht unterstützt.

Voraussetzungen

Weitere Informationen finden Sie unter [Voraussetzungen für die Bereitstellung der VMware Cloud Director-Appliance](#).

Verfahren

1 Starten der Bereitstellung der VMware Cloud Director-Appliance

Um die Appliance-Bereitstellung zu starten, öffnen Sie den Bereitstellungsassistenten über den vSphere Web Client (Flex) oder den vSphere Client (HTML5) und stellen Sie die OVF-Vorlage bereit.

2 Konfigurieren der primären VMware Cloud Director-Appliance

Nach der Bereitstellung der OVF-Vorlage für die primäre Appliance müssen Sie in der Appliance Management-Benutzerschnittstelle der primären VMware Cloud Director-Appliance-Instanz mit der Konfigurationsphase fortfahren.

3 Konfigurieren der Standby- und Anwendungszellen in VMware Cloud Director

Nach der Bereitstellung der OVF-Vorlage für die Standby- oder Anwendungszelle müssen Sie in der Appliance Management-Benutzerschnittstelle der bereitzustellenden Instanz mit der Konfigurationsphase fortfahren.

Nächste Schritte

- Konfigurieren Sie die öffentliche Konsolen-Proxy-Adresse, da die VMware Cloud Director-Appliance ihre `eth0`-NIC mit dem benutzerdefinierten Port 8443 für den Konsolen-Proxy-Dienst verwendet. Weitere Informationen finden Sie unter [Anpassen öffentlicher Adressbücher für VMware Cloud Director unter Linux](#).
- Um der VMware Cloud Director-Servergruppe Mitglieder hinzuzufügen, wiederholen Sie den Vorgang.
- Um den Lizenzschlüssel einzugeben, melden Sie sich beim VMware Cloud Director Service Provider Admin Portal an.
- Um das selbstsignierte Zertifikat zu ersetzen, das während des erstmaligen Starts der Appliance erstellt wird, können Sie die Schritte unter [Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores für VMware Cloud Director unter Linux](#) ausführen.

Starten der Bereitstellung der VMware Cloud Director-Appliance

Um die Appliance-Bereitstellung zu starten, öffnen Sie den Bereitstellungsassistenten über den vSphere Web Client (Flex) oder den vSphere Client (HTML5) und stellen Sie die OVF-Vorlage bereit.

Verfahren

- 1 Klicken Sie im vSphere Web Client oder dem vSphere Client mit der rechten Maustaste auf ein Bestandslistenobjekt und klicken Sie dann auf **OVF-Vorlage bereitstellen**.

- 2 Geben Sie den Pfad zur VMware Cloud Director .ova-Datei ein und klicken Sie auf **Weiter**.
- 3 Geben Sie einen Namen für die virtuelle Maschine ein und durchsuchen Sie das vCenter Server-Repository, um ein Datacenter oder einen Ordner für die Bereitstellung der Appliance auszuwählen. Klicken Sie anschließend auf **Weiter**.
- 4 Wählen Sie einen ESXi-Host oder -Cluster aus, auf bzw. in dem die Appliance bereitgestellt werden soll, und klicken Sie auf **Weiter**.
- 5 Überprüfen Sie Details der OVF-Vorlage und klicken Sie auf **Weiter**.
- 6 Lesen und akzeptieren Sie die Lizenzvereinbarungen und klicken Sie auf **Weiter**.
- 7 Wählen Sie den Bereitstellungstyp und die -größe aus und klicken Sie auf **Weiter**.

Die Größen „Primär-klein“ und „Standby-klein“ der VMware Cloud Director-Appliance sind für Lab- oder Testsysteme geeignet. Die Größen „Primär-groß“ und „Standby-groß“ erfüllen die Mindestgrößenanforderungen für Produktionssysteme. Je nach Arbeitslast müssen Sie möglicherweise weitere Ressourcen hinzufügen.

Option	Beschreibung
Primär-klein	<p>Stellt die Appliance mit 12 GB RAM und 2 vCPUs als erstes Mitglied in einer VMware Cloud Director-Servergruppe bereit.</p> <p>Die eingebettete Datenbank in der primären Zelle ist als VMware Cloud Director-Datenbank konfiguriert. Der Datenbankname lautet <code>vcloud</code>, und der Datenbankbenutzer ist <code>vcloud</code>.</p>
Primär-groß	<ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 und höhere Versionen stellen die Appliance mit 24 GB RAM und 8 vCPUs als erstes Mitglied in einer VMware Cloud Director-Servergruppe bereit. ■ VMware Cloud Director 10.2 stellt die Appliance mit 24 GB RAM und 4 vCPUs als erstes Mitglied in einer VMware Cloud Director-Servergruppe bereit. <p>Die eingebettete Datenbank in der primären Zelle ist als VMware Cloud Director-Datenbank konfiguriert. Der Datenbankname lautet <code>vcloud</code>, und der Datenbankbenutzer ist <code>vcloud</code>.</p>
Standby-klein	<p>Wird verwendet, um einer primär-kleinen Zelle in einem Datenbank-HA-Cluster beizutreten.</p> <p>Stellt die Appliance mit 12 GB RAM und 2 vCPUs als zweites oder drittes Mitglied in einer VMware Cloud Director-Servergruppe mit einer Datenbank-Hochverfügbarkeitskonfiguration bereit.</p> <p>Die eingebettete Datenbank in einer Standby-Zelle wird in einem Replizierungsmodus mit der primären Datenbank konfiguriert.</p>

Option	Beschreibung
Standby-groß	<p>Wird verwendet, um einer primär-großen Zelle in einem Datenbank-HA-Cluster beizutreten.</p> <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 und höhere Versionen stellen die Appliance mit 24 GB RAM und 8 vCPUs als zweites oder drittes Mitglied in einer VMware Cloud Director-Servergruppe mit einer Datenbank-Hochverfügbarkeitskonfiguration bereit. ■ VMware Cloud Director 10.2 stellt die Appliance mit 24 GB RAM und 4 vCPUs als zweites oder drittes Mitglied in einer VMware Cloud Director-Servergruppe mit einer Datenbank-Hochverfügbarkeitskonfiguration bereit. <p>Die eingebettete Datenbank in einer Standby-Appliance wird in einem Replizierungsmodus mit der primären Datenbank konfiguriert.</p>
Cloud Director-Zellenanwendung	<ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 und höhere Versionen stellen die Appliance mit 8 GB RAM und 4 vCPUs als nachfolgendes Mitglied in einer VMware Cloud Director-Servergruppe bereit. ■ VMware Cloud Director 10.2 stellt die Appliance mit 8 GB RAM und 2 vCPUs als nachfolgendes Mitglied in einer VMware Cloud Director-Servergruppe bereit. <p>Die eingebettete Datenbank in einer vCD-Anwendungszelle wird nicht verwendet. Die vCD-Anwendungszelle stellt eine Verbindung mit der primären Datenbank her.</p>

Wichtig Die primäre und die Standby-Zelle in einer VMware Cloud Director-Servergruppe müssen dieselbe Größe aufweisen. Ein Datenbank-HA-Cluster kann aus einer primär-kleinen und zwei Standby-kleinen Zellen oder aus einer primär-großen und zwei Standby-großen Zellen bestehen.

Nach der Bereitstellung können Sie die Größe der Appliance neu konfigurieren.

- 8 Wählen Sie das Festplattenformat und den Datenspeicher für die Konfigurationsdateien und virtuellen Festplatten der virtuellen Maschine aus und klicken Sie auf **Weiter**.

Thick-Formate verbessern die Leistung, und Thin-Formate sparen Speicherplatz.

- 9 Wählen Sie in den Dropdown-Menüs in den **Zielnetzwerk**-Zellen die Zielnetzwerke für die Netzwerkkarten `eth1` und `eth0` der Appliance aus.

Die Quellnetzwerke in der Liste können in umgekehrter Reihenfolge angegeben werden. Stellen Sie sicher, dass Sie für jedes Quellnetzwerk das richtige Zielnetzwerk auswählen.

Wichtig Die beiden Zielnetzwerke müssen unterschiedlich sein.

- 10 Wählen Sie in den Dropdown-Menüs unter **IP-Zuweisungseinstellungen** die Option **Statisch – Manuell** für die IP-Zuweisung und **IPv4** als Protokoll aus.

- 11 Klicken Sie auf **Weiter**.

Sie werden an die Seite **Vorlage anpassen** des Assistenten umgeleitet, auf der Sie die Details für VMware Cloud Director konfigurieren.

12 Konfigurieren Sie im Abschnitt **VCD-Appliance-Einstellungen** die Appliance-Details.

Einstellung	Beschreibung
NTP-Server	Der Hostname oder die IP-Adresse des zu verwendenden NTP-Servers.
Anfängliches Root-Kennwort	<p>Das anfängliche Root-Kennwort für die Appliance. Es muss mindestens acht Zeichen, einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.</p> <p>Wichtig Das anfängliche Root-Kennwort wird zum Keystore-Kennwort. Für die Cluster-Bereitstellung müssen alle Zellen während der anfänglichen Bereitstellung über dasselbe Root-Kennwort verfügen. Nachdem der Startvorgang abgeschlossen ist, können Sie das Root-Kennwort in jeder gewünschten Zelle ändern.</p> <p>Wenn Sie den FIPS-Modus verwenden möchten, muss das root-Kennwort für die Appliance 14 oder mehr Zeichen enthalten.</p> <p>Hinweis Der OVF-Bereitstellungsassistent validiert das anfängliche Root-Kennwort nicht anhand von Kennwortkriterien.</p>
Root-Kennwort läuft bei der ersten Anmeldung ab	Wenn Sie das anfängliche Kennwort nach der ersten Anmeldung weiterhin verwenden möchten, müssen Sie sicherstellen, dass das anfängliche Kennwort die Kriterien für das Root-Kennwort erfüllt. Um das anfängliche Root-Kennwort nach der ersten Anmeldung weiter zu verwenden, deaktivieren Sie diese Option.
SSH-Root-Anmeldung aktivieren	Standardmäßig deaktiviert.

Hinweis Informationen zum Ändern von Datum, Uhrzeit oder Zeitzone der Appliance finden Sie unter <https://kb.vmware.com/kb/59674>.

13 (Optional) Wenn Ihre Netzwerktopologie dies erfordert, geben Sie im Abschnitt **Zusätzliche Netzwerkeigenschaften** die statischen Routen für die Netzwerkschnittstellen `eth0` und `eth1` ein und klicken Sie auf **Weiter**.

Wenn Sie Hosts über eine nicht standardmäßige Gateway-Route erreichen möchten, müssen Sie möglicherweise statische Routen bereitstellen. Beispielsweise kann nur über die `eth1`-Schnittstelle auf die Managementinfrastruktur zugegriffen werden, während sich das Standard-Gateway auf `eth0` befindet. In den meisten Fällen kann diese Einstellung leer bleiben.

Die statischen Routen müssen sich in einer kommasetrennten Liste mit Routenspezifikationen befinden. Eine Routenspezifikation muss aus der IP-Adresse des Ziel-Gateways und optional aus einer CIDR-Netzwerkspezifikation (Classless Inter-Domain Routing) bestehen. Beispiel: `172.16.100.253 172.16.100.0/19, 172.16.200.253`.

14 Geben Sie im Abschnitt **Netzwerkeigenschaften** die Netzwerkdetails für die Netzwerkkarten `eth0` und `eth1` ein und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Standard-Gateway	Die IP-Adresse des Standard-Gateways für die Appliance.
Domänenname	Die DNS-Suchdomäne, z. B. <code>mydomain.com</code> .

Einstellung	Beschreibung
Domänensuchpfad	Eine durch Kommas oder Leerzeichen getrennte Liste von Domänennamen für die Suche nach dem Appliance-Hostnamen, z. B. <i>subdomain.example.com</i> . Hinweis Der Domänenname, den Sie im Textfeld „Domänenname“ eingegeben haben, ist das erste Element in der Liste der Domänensuchpfade.
Domänennamenserver	Die IP-Adresse des Domänennamenservers für die Appliance.
eth0-Netzwerk-IP-Adresse	Die IP-Adresse für die eth0-Schnittstelle.
eth0-Netzwerkmaske	Die Netzmaske oder das Präfix für die eth0-Schnittstelle.
eth1-Netzwerk-IP-Adresse	Die IP-Adresse für die eth1-Schnittstelle.
eth1-Netzwerkmaske	Die Netzmaske oder das Präfix für die eth1-Schnittstelle.

- Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Konfigurationseinstellungen für die VMware Cloud Director-Appliance und klicken Sie auf **Beenden**, um die Bereitstellung abzuschließen.

Nächste Schritte

- Schalten Sie die neu erstellte virtuelle Maschine ein.
- [Konfigurieren der primären VMware Cloud Director-Appliance](#) oder [Konfigurieren der Standby- und Anwendungszellen in VMware Cloud Director](#).

Konfigurieren der primären VMware Cloud Director-Appliance

Nach der Bereitstellung der OVF-Vorlage für die primäre Appliance müssen Sie in der Appliance Management-Benutzerschnittstelle der primären VMware Cloud Director-Appliance-Instanz mit der Konfigurationsphase fortfahren.

Voraussetzungen

- [Starten der Bereitstellung der VMware Cloud Director-Appliance](#).
- Schalten Sie die neu erstellte virtuelle Maschine ein.
- Machen Sie sich mit dem Thema [Vorbereiten des Übertragungsserverspeichers für die VMware Cloud Director-Appliance](#) vertraut.

Verfahren

- Öffnen Sie einen Webbrowser und navigieren Sie zu `https://Primary-Appliance-eth1-IP-Address:5480`.
- Melden Sie sich bei der Appliance Management-Benutzerschnittstelle der primären Appliance-Instanz an.

Die Seite **Systeminstallation der primären Appliance** wird angezeigt.

- 3 Konfigurieren Sie im Abschnitt **Appliance-Einstellungen** die Appliance-Details und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Mounten von NFS für Übertragungsdateispeicherort	Der Speicherort des freigegebenen NFS-Übertragungsservers. VMware Cloud Director überprüft den Speicherort und zeigt ein grünes Häkchen an, wenn der NFS-Mount validiert wird.
DB-Kennwort für den Benutzer vcloud	Das Kennwort für den PostgreSQL-Datenbankbenutzer vcloud .
DB-Kennwort bestätigen	Bestätigung des Kennworts für den PostgreSQL-Datenbankbenutzer vcloud .
Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit	Aktiviert oder deaktiviert die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit von VMware.

- 4 Konfigurieren Sie im Abschnitt **Administratorkonto** die Details des Systemadministrators und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Benutzername	Der Benutzername für das Systemadministrator -Konto. Standardmäßig <code>administrator</code> .
Kennwort	Das Kennwort für das Systemadministrator -Konto. Das Kennwort muss zwischen 6 und 128 Zeichen lang sein.
Kennwort bestätigen	Bestätigen Sie das Kennwort für das Konto Systemadministrator .
Vollständiger Name	Der vollständige Name des Systemadministrators . Standardmäßig <code>vCD Admin</code> .
Mail-Adresse	Die E-Mail-Adresse des Systemadministrators .

- 5 Konfigurieren Sie im Abschnitt **VMware Cloud Director-Einstellungen** die Installation dieser Instanz.

Einstellung	Beschreibung
Systemname	Der Name des vCenter Server-Ordners, der für diese VMware Cloud Director-Installation erstellt werden soll.
Installations-ID	Die ID für diese VMware Cloud Director-Installation, die bei der Erstellung von MAC-Adressen für virtuelle Netzwerkkarten verwendet werden soll. Standardmäßig <code>1</code> . Wenn Sie ausgeweitete Netzwerke für VMware Cloud Director-Installationen in Multisite-Bereitstellungen erstellen möchten, richten Sie eine eindeutige Installations-ID für jede VMware Cloud Director-Installation ein.

- 6 Klicken Sie nach Abschluss der Systeminstallation auf **Senden** und dann auf **OK**.

Ergebnisse

Wenn die Bereitstellung erfolgreich verläuft, werden die Registerkarten **Verfügbarkeit der eingebetteten Datenbank** und **Dienste** angezeigt.

Nächste Schritte

- [Ändern der VMware Cloud Director-Appliance-Zeitzone](#)
- Stellen Sie eine Standby- oder Anwendungszelle bereit. Weitere Informationen finden Sie unter [Starten der Bereitstellung der VMware Cloud Director-Appliance](#).
- [Konfigurieren der Standby- und Anwendungszellen in VMware Cloud Director](#)

Konfigurieren der Standby- und Anwendungszellen in VMware Cloud Director

Nach der Bereitstellung der OVF-Vorlage für die Standby- oder Anwendungszelle müssen Sie in der Appliance Management-Benutzerschnittstelle der bereitzustellenden Instanz mit der Konfigurationsphase fortfahren.

Voraussetzungen

- 1 Stellen Sie eine Standby- oder Anwendungszelle bereit. Weitere Informationen finden Sie im [Starten der Bereitstellung der VMware Cloud Director-Appliance](#).
- 2 Weitere Informationen finden Sie im [Vorbereiten des Übertragungsserverspeichers für die VMware Cloud Director-Appliance](#).
- 3 Schalten Sie die neu erstellte virtuelle Maschine ein.

Verfahren

- 1 Öffnen Sie einen Webbrowser und navigieren Sie zu `https://Cell-eth1-IP-Address:5480`.
- 2 Melden Sie sich bei der Appliance Management-Benutzerschnittstelle der Standby- oder Anwendungszelle an.
Die Seite **Systeminstallation** wird angezeigt.
- 3 Geben Sie den NFS-Mount für den Speicherort der Übertragungsdatei ein.
- 4 Klicken Sie nach Abschluss der Systeminstallation auf **Senden** und dann auf **OK**.

Nächste Schritte

[Ändern der VMware Cloud Director-Appliance-Zeitzone](#)

Bereitstellen der VMware Cloud Director-Appliance mit dem VMware OVF Tool

Sie können die VMware Cloud Director-Appliance mit dem vSphere OVF Tool als OVF-Vorlage bereitstellen.

Sie müssen das erste Mitglied einer VMware Cloud Director-Servergruppe als primäre Zelle bereitstellen. Sie können ein nachfolgendes Mitglied einer VMware Cloud Director-Servergruppe als Standby- oder VMware Cloud Director-Anwendungszelle bereitstellen. Weitere Informationen finden Sie unter [Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration](#).

Informationen zum Installieren des OVF-Tools finden Sie im Dokument mit den *Versionshinweisen für das VMware OVF Tool*.

Informationen zur Verwendung des OVF-Tools finden Sie im *Benutzerhandbuch für das OVF-Tool*.

Wichtig Gemischte VMware Cloud Director-Installationen unter Linux und VMware Cloud Director-Appliance-Bereitstellungen in einer Servergruppe werden nicht unterstützt.

Wenn Sie einem Datenbankcluster zusätzliche oder Ersatz-Appliances hinzufügen, müssen vCPU und RAM mit denen der vorhandenen primären und Standby-Zellen im Cluster übereinstimmen.

Die OVA-Version der neu bereitgestellten Standby-Appliance muss mit derjenigen der vorhandenen Appliances im Cluster identisch sein. Informationen zum Anzeigen der Version der ausgeführten Appliances finden Sie unter „Info über“ in der Appliance-Verwaltungsbenutzeroberfläche. Die Appliance wird mit einem Namen im Format `VMware Cloud Director-v bereitgestellt.v.v.v-nnnnnn_OVF10.ova`, wobei *v.v.v.v* die Produktversion und *nnnnnn* die Build-Nummer darstellt. Beispiel: `VMware Cloud Director-10.2.0.0-9229800_OVA10.ova`.

Informationen zum Bereitstellen von OVF-Vorlagen in vSphere finden Sie im Abschnitt *Verwaltung virtueller vSphere-Maschinen*.

Alternativ können Sie die Appliance mithilfe des vSphere Clients bereitstellen. Weitere Informationen finden Sie im [Bereitstellen der VMware Cloud Director-Appliance unter Verwendung des vSphere Clients](#).

Bevor Sie den Bereitstellungsbeefehl ausführen, finden Sie weitere Informationen unter [Voraussetzungen für die Bereitstellung der VMware Cloud Director-Appliance](#).

Ab VMware Cloud Director 10.2 müssen Sie den Parameter `--X:enableHiddenProperties` zum Bereitstellen der VMware Cloud Director-Appliance einschließen.

Hinweis Zum Abschließen der Konfiguration nach der Bereitstellung haben Sie die Auswahl zwischen der Angabe der optionalen OVF-Konfigurationsoptionen während der Bereitstellung der primären Appliance oder der Ausführung der Appliance-Verwaltungsbenutzeroberfläche.

ovftool-Befehlsoptionen und -Eigenschaften für die Bereitstellung der VMware Cloud Director-Appliance

Option	Wert	Beschreibung
<code>--noSSLVerify</code>	n. v.	Überspringt die SSL-Überprüfung für vSphere-Verbindungen.
<code>--acceptAllEulas</code>	n. v.	Akzeptiert alle Endbenutzer-Lizenzvereinbarungen (EULAs).
<code>--X:enableHiddenProperties</code>	n. v.	Zeigt alle Eigenschaften für die Konfiguration der Appliance an.

Option	Wert	Beschreibung
--datastore	<i>target_vc_datastore</i>	Der Name des Zieldatenspeichers, auf dem die Konfigurationsdateien und virtuellen Festplatten der virtuellen Maschine gespeichert werden sollen.
--allowAllExtraConfig	n. v.	Konvertiert alle zusätzlichen Konfigurationsoptionen in das Format VMX.
--net:"eth0 Network"	<i>portgroup_on_vc_for_eth0</i>	Das Zielnetzwerk für das eth0-Netzwerk der Appliance. Wichtig Muss sich vom eth1-Zielnetzwerk unterscheiden.
--net:"eth1 Network"	<i>portgroup_on_vc_for_eth1</i>	Das Zielnetzwerk für das eth1-Netzwerk der Appliance. Wichtig Muss sich vom eth0-Zielnetzwerk unterscheiden.
--name	<i>vm_name_on_vc</i>	Der VM-Name für die Appliance.
--diskMode	thin oder thick	Das Festplattenformat für die Konfigurationsdateien und virtuellen Festplatten der virtuellen Maschine.
--prop:"vami.ip0.VMware_vCloud_Director"	<i>eth0_ip_address</i>	IP-Adresse von eth0. Wird für den Zugriff auf die Benutzeroberfläche und die API verwendet. Bei dieser Adresse bestimmt der DNS-Reverse-Lookup den Hostnamen der Appliance und legt diesen fest.
--prop:"vami.ip1.VMware_vCloud_Director"	<i>eth1_ip_address</i>	IP-Adresse von eth1. Wird für den Zugriff auf interne Dienste verwendet, einschließlich des eingebetteten PostgreSQL-Datenbankdiensts.
--prop:"vami.DNS.VMware_vCloud_Director"	<i>dns_ip_address</i>	Die IP-Adresse des Domänennamenservers für die Appliance.
--prop:"vami.domain.VMware_vCloud_Director"	<i>dns_name</i>	Die DNS-Suchdomäne. Wird als erstes Element im Suchpfad angezeigt.
--prop:"vami.gateway.VMware_vCloud_Director"	<i>gateway_ip_address</i>	Die IP-Adresse des Standard-Gateways für die Appliance.
--prop:"vami.netmask0.VMware_vCloud_Director"	<i>netmask</i>	Die Netzmaske oder das Präfix für die eth0-Schnittstelle.
--prop:"vami.netmask1.VMware_vCloud_Director"	<i>netmask</i>	Die Netzmaske oder das Präfix für die eth1-Schnittstelle.

Option	Wert	Beschreibung
<code>--prop:"vami.searchpath.VMware_vCloud_Director_domain_names"</code>	<code>vmami.searchpath.VMware_vCloud_Director_domain_names</code>	Der Domänensuchpfad der Appliance. Eine komma- oder leerzeichengetrennte Liste von Domännennamen.
<code>--prop:"vcloudconf.ceip_enabled.VMware_vCloud_Director"</code>	<code>vmami.ceip_enabled.VMware_vCloud_Director</code>	Aktiviert oder deaktiviert die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit von VMware. Der Standardwert ist „Wahr“. Optional, wenn Sie die Appliance-Verwaltungsbenutzeroberfläche ausführen möchten, um die Konfiguration der primären Appliance nach der Bereitstellung abzuschließen.
<code>--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"</code>	<code>vmami.enable_ssh.VMware_vCloud_Director</code>	Aktiviert oder deaktiviert den SSH- root -Zugriff auf die Appliance.
<code>--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"</code>	<code>vmami.expire_root_password.VMware_vCloud_Director</code>	Legt fest, ob das anfängliche Kennwort nach der ersten Anmeldung weiter verwendet werden soll oder nicht.
<code>--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director":nfs_mount_path</code>	<code>vmami.nfs_mount.VMware_vCloud_Director:nfs_mount_path</code>	Die IP-Adresse und der Exportpfad des externen NFS-Servers. Wird nur für eine primäre Zelle verwendet.
<code>--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"address</code>	<code>vmami.ntp-server.VMware_vCloud_Director:address</code>	Die IP-Adresse des Zeitservers.
<code>--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"</code>	<code>vmami.varoot-password.VMware_vCloud_Director</code>	Das anfängliche Root-Kennwort für die Appliance. Es muss mindestens acht Zeichen, einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten. Wichtig Das anfängliche Root-Kennwort wird zum Keystore-Kennwort. Für die Cluster-Bereitstellung müssen alle Zellen während der anfänglichen Bereitstellung über dasselbe Root-Kennwort verfügen. Nachdem der Startvorgang abgeschlossen ist, können Sie das Root-Kennwort in jeder gewünschten Zelle ändern.
<code>--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"</code>	<code>vmami.db_pwd.VMware_vCloud_Director</code>	Das Datenbankkennwort des cloud -Benutzers. Wird nur für eine primäre Zelle verwendet. Optional, wenn Sie die Appliance-Verwaltungsbenutzeroberfläche ausführen möchten, um die Konfiguration der primären Appliance nach der Bereitstellung abzuschließen.

Option	Wert	Beschreibung
<code>--prop:"vcloudconf.admin_email.VMware_vCloud_Director"address</code>	<code>vcloudconf.admin_email.VMware_vCloud_Director</code>	<p>Die E-Mail-Adresse für das Systemadministrator-Konto.</p> <p>Wird nur für eine primäre Zelle verwendet.</p> <p>Optional, wenn Sie die Appliance-Verwaltungsbenutzeroberfläche ausführen möchten, um die Konfiguration der primären Appliance nach der Bereitstellung abzuschließen.</p>
<code>--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"</code>	<code>vcloudconf.admin_fname.VMware_vCloud_Director</code>	<p>Der Name für das Systemadministrator-Konto.</p> <p>Wird nur für eine primäre Zelle verwendet.</p> <p>Optional, wenn Sie die Appliance-Verwaltungsbenutzeroberfläche ausführen möchten, um die Konfiguration der primären Appliance nach der Bereitstellung abzuschließen.</p>
<code>--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"password</code>	<code>vcloudconf.admin_pwd.VMware_vCloud_Director</code>	<p>Das Kennwort für das Systemadministrator-Konto.</p> <p>Wird nur für eine primäre Zelle verwendet.</p> <p>Optional, wenn Sie die Appliance-Verwaltungsbenutzeroberfläche ausführen möchten, um die Konfiguration der primären Appliance nach der Bereitstellung abzuschließen.</p>
<code>--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"uname</code>	<code>vcloudconf.admin_uname.VMware_vCloud_Director</code>	<p>Der Benutzername für das Systemadministrator-Konto.</p> <p>Wird nur für eine primäre Zelle verwendet.</p> <p>Optional, wenn Sie die Appliance-Verwaltungsbenutzeroberfläche ausführen möchten, um die Konfiguration der primären Appliance nach der Bereitstellung abzuschließen.</p>
<code>--prop:"vcloudconf.inst_id.VMware_vCloud_Director"ID</code>	<code>vcloudconf.inst_id.VMware_vCloud_Director</code>	<p>Die Installations-ID für VMware Cloud Director</p> <p>Wird nur für eine primäre Zelle verwendet.</p> <p>Optional, wenn Sie die Appliance-Verwaltungsbenutzeroberfläche ausführen möchten, um die Konfiguration der primären Appliance nach der Bereitstellung abzuschließen.</p>

Option	Wert	Beschreibung
<pre>--prop:"vcloudconf.sys_name.VMware_vCloudSystemName"</pre>		<p>Der Name des vCenter Server-Ordners, der für diese VMware Cloud Director-Installation erstellt werden soll.</p> <p>Optional, wenn Sie die Appliance-Verwaltungsbenutzeroberfläche ausführen möchten, um die Konfiguration der primären Appliance nach der Bereitstellung abzuschließen.</p>
<pre>--prop:"vcloudnet.routes0.VMware_vCloudNetwork" cidr, ip_address1, ip_address2, ...</pre>		<p>Optional. Statische Routen für die eth0-Schnittstelle. Es muss sich um eine kommasetrennte Liste mit Routenspezifikationen handeln. Eine Routenspezifikation muss aus einer Gateway-IP-Adresse und optional einer CIDR-Netzwerkspezifikation (Classless Inter-Domain Routing) (Präfix/Bits) bestehen. Beispiel: 172.16.100.253 172.16.100/19, 172.16.200.253.</p>
<pre>--prop:"vcloudnet.routes1.VMware_vCloudNetwork" cidr, ip_address1, ip_address2, ...</pre>		<p>Optional. Statische Routen für die eth1-Schnittstelle. Es muss sich um eine kommasetrennte Liste mit Routenspezifikationen handeln. Eine Routenspezifikation muss aus einer Gateway-IP-Adresse und optional einer CIDR-Netzwerkspezifikation (Classless Inter-Domain Routing) (Präfix/Bits) bestehen. Beispiel: 172.16.100.253 172.16.100/19, 172.16.200.253.</p>

Option	Wert	Beschreibung
--deploymentOption	primary-small, primary-large, standby-small, standby-large oder cell	<p>Der Typ und die Größe der Appliance, die Sie bereitstellen möchten.</p> <p>Die Größen „Primär-klein“ und „Standby-klein“ der VMware Cloud Director-Appliance sind für Lab- oder Testsysteme geeignet. Die Größen „Primär-groß“ und „Standby-groß“ erfüllen die Mindestgrößenanforderungen für Produktionssysteme. Je nach Arbeitslast müssen Sie möglicherweise weitere Ressourcen hinzufügen.</p> <ul style="list-style-type: none"> ■ primary-small stellt die Appliance mit 12 GB RAM und 2 vCPUs als erstes Mitglied in einer VMware Cloud Director-Servergruppe bereit. Die eingebettete Datenbank in der primären Zelle ist als VMware Cloud Director-Datenbank konfiguriert. Der Datenbankname lautet <code>vcloud</code> und der Datenbankbenutzer ist <code>vcloud</code>. ■ primary-large: <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 und höhere Versionen stellen die Appliance mit 24 GB RAM und 8 vCPUs als erstes Mitglied in einer VMware Cloud Director-Servergruppe bereit. ■ VMware Cloud Director 10.2 stellt die Appliance mit 24 GB RAM und 4 vCPUs als erstes Mitglied in einer VMware Cloud Director-Servergruppe bereit. <p>Die eingebettete Datenbank in der primären Zelle ist als VMware Cloud Director-Datenbank konfiguriert. Der Datenbankname lautet <code>vcloud</code>, und der Datenbankbenutzer ist <code>vcloud</code>.</p> ■ standby-small stellt die Appliance mit 12 GB RAM und 2 vCPUs als zweites oder drittes Mitglied in einer VMware Cloud Director-Servergruppe mit einer Datenbank-Hochverfügbarkeitskonfiguration bereit. Die eingebettete Datenbank in einer Standby-Zelle wird in einem Replizierungsmodus mit der primären Datenbank konfiguriert.

Option	Wert	Beschreibung
		<ul style="list-style-type: none"> ■ standby-large: <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 und höhere Versionen stellen die Appliance mit 24 GB RAM und 8 vCPUs als zweites oder drittes Mitglied in einer VMware Cloud Director-Servergruppe mit einer Datenbank-Hochverfügbarkeitskonfiguration bereit. ■ VMware Cloud Director 10.2 stellt die Appliance mit 24 GB RAM und 4 vCPUs als zweites oder drittes Mitglied in einer VMware Cloud Director-Servergruppe mit einer Datenbank-Hochverfügbarkeitskonfiguration bereit. <p>Die eingebettete Datenbank in einer Standby-Zelle wird in einem Replizierungsmodus mit der primären Datenbank konfiguriert.</p> ■ cell: <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 und höhere Versionen stellen die Appliance mit 8 GB RAM und 4 vCPUs als nachfolgendes Mitglied in einer VMware Cloud Director-Servergruppe bereit. ■ VMware Cloud Director 10.2 stellt die Appliance mit 8 GB RAM und 2 vCPUs als nachfolgendes Mitglied in einer VMware Cloud Director-Servergruppe bereit. <p>Die eingebettete Datenbank in einer vCD-Anwendungszelle</p>

Option	Wert	Beschreibung
		wird nicht verwendet. Die vCD-Anwendungszelle stellt eine Verbindung mit der primären Datenbank her.
		Wichtig Die primäre und die Standby-Zelle in einer VMware Cloud Director-Servergruppe müssen dieselbe Größe aufweisen. Ein Datenbank-HA-Cluster kann aus einer primär-kleinen und zwei Standby-kleinen Zellen oder aus einer primär-großen und zwei Standby-großen Zellen bestehen. Nach der Bereitstellung können Sie die Größe der Appliance neu konfigurieren.
--powerOn	<i>path_to_ova</i>	Schaltet die virtuelle Maschine nach der Bereitstellung manuell ein.

Ein Beispielbefehl für die Bereitstellung der primären VMware Cloud Director-Appliance zu Produktionszwecken

Wichtig Bevor Sie den Befehl VMware OVF Tool ausführen, ersetzen Sie die Kennwörter `vcloudapp.varoot-passwordVMware_vCloud_Director`, `vcloudconf.db_pwdVMware_vCloud_Director` und `vcloudconf.admin_pwd.VMware_vCloud_Director` durch Ihre eigenen sicheren Kennwörter.

```
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
```

Ein Beispielbefehl für die Bereitstellung der VMware Cloud Director-Standby-Appliance zu Produktionszwecken

Wichtig Bevor Sie den Befehl VMware OVF Tool ausführen, ersetzen Sie das Kennwort `vcloudapp.varoot-password.VMware_vCloud_Director` durch Ihr eigenes sicheres Kennwort.

```
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
```

Nach der Bereitstellung der VMware Cloud Director-Appliance

Nachdem Sie die Appliance bereitgestellt haben, prüfen Sie die Warn- oder Fehlermeldungen in der `firstboot`-Protokolldatei. Weitere Informationen finden Sie unter [Prüfen der Protokolldateien in der VMware Cloud Director-Appliance](#).

Verwenden Sie die Appliance-Verwaltungsbenutzeroberfläche, um die primäre Appliance zu konfigurieren. Weitere Informationen finden Sie im [Konfigurieren der primären VMware Cloud Director-Appliance](#).

Verwenden Sie die Appliance-Verwaltungsbenutzeroberfläche, um die Standby- und Anwendungszellen zu konfigurieren. Weitere Informationen finden Sie im [Konfigurieren der Standby- und Anwendungszellen in VMware Cloud Director](#).

Bereitstellen der VMware Cloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation

Sie können die VMware Cloud Director-Appliance mit signierten Platzhalterzertifikaten bereitstellen. Sie können diese Zertifikate verwenden, um eine unbegrenzte Anzahl von Servern zu sichern, die Unterdomänen des im Zertifikat aufgeführten Domänennamens sind.

Bei der Bereitstellung von VMware Cloud Director-Appliances generiert VMware Cloud Director standardmäßig selbstsignierte Zertifikate und verwendet sie zum Konfigurieren der VMware Cloud Director-Zelle für die HTTPS- und die Konsolenproxy-Kommunikation.

Wenn Sie eine primäre Appliance erfolgreich bereitstellen, kopiert die Konfigurationslogik der Appliance die Datei `responses.properties` von der primären Appliance in den gemeinsamen Speicher des gemeinsam genutzten NFS-Übertragungsdienst unter `/opt/vmware/vcloud-director/data/transfer`. Andere für diese VMware Cloud Director-Servergruppe bereitgestellte Appliances verwenden diese Datei, um sich automatisch selbst zu konfigurieren. Die Datei `responses.properties` enthält einen Pfad zum SSL-Zertifikat-Keystore, der die automatisch generierten selbstsignierten Zertifikate von `user.keystore.path` enthält. Standardmäßig ist dies ein Pfad zu einer Keystore-Datei, die für jede Appliance lokal ist.

Nachdem Sie die primäre Appliance bereitgestellt haben, können Sie sie für die Verwendung signierter Zertifikate neu konfigurieren. Weitere Informationen zum Erstellen des Keystores mit signierten Zertifikaten finden Sie unter [Erstellen und Importieren der von einer Zertifizierungsstelle signierten SSL-Zertifikate in die VMware Cloud Director-Appliance](#).

Wenn es sich bei den signierten Zertifikaten, die Sie für die primäre VMware Cloud Director-Appliance verwenden, um signierte Platzhalterzertifikate handelt, können diese Zertifikate auf alle anderen Appliances in der VMware Cloud Director-Servergruppe, d. h. Standby-Zellen und VMware Cloud Director-Anwendungszellen, angewendet werden. Sie können die Bereitstellung der Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation verwenden, um die zusätzlichen Zellen mit den signierten Platzhalter-SSL-Zertifikaten zu konfigurieren.

Voraussetzungen

- Vergewissern Sie sich, dass der Keystore, der die signierten SSL-Platzhalterzertifikate für die HTTPS- und Konsolenproxy-Aliase enthält, auf der primären Appliance verfügbar ist, d. h. unter `/opt/vmware/vcloud-director/certificates.ks`.
- Wenn Sie Schlüsselpaare erstellen und von einer Zertifizierungsstelle signierte Zertifikatsdateien importieren müssen, finden Sie weitere Informationen unter [Erstellen und Importieren der von einer Zertifizierungsstelle signierten SSL-Zertifikate in die VMware Cloud Director-Appliance](#).
- Wenn Sie bereits über einen eigenen privaten Schlüssel und eine von einer Zertifizierungsstelle signierte Zertifikatsdatei verfügen, finden Sie weitere Informationen unter [Importieren von privaten Schlüsseln und den von einer Zertifizierungsstelle signierten SSL-Zertifikaten in die VMware Cloud Director-Appliance](#).
- Wenn JCEKS als Keystore-Typ des Keystores mit den signierten SSL-Platzhalterzertifikaten verwendet wird, stellen Sie sicher, dass das private Kennwort für die Schlüssel innerhalb des Keystores mit dem Kennwort des Keystores übereinstimmt. Das Keystore-Kennwort muss mit dem anfänglichen Root-Kennwort übereinstimmen, das bei der Bereitstellung aller Appliances verwendet wird.

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

Verfahren

- 1 Kopieren Sie die neue `certificates.ks`-Datei mit den ordnungsgemäß signierten Zertifikaten von der primären Appliance in der Übertragungsfreigabe unter `/opt/vmware/vcloud-director/data/transfer/`.

- 2 Ändern Sie die Besitzer- und die Gruppenberechtigungen in der Keystore-Datei in **vcloud**.

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

- 3 Stellen Sie sicher, dass der Besitzer der Keystore-Datei über Lese- und Schreibberechtigungen verfügt.

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

- 4 Führen Sie auf der primären Appliance den Befehl zum Importieren der neuen signierten Zertifikate in die VMware Cloud Director-Instanz aus.

Dieser Befehl aktualisiert auch die Datei `responses.properties` in der Übertragungsfreigabe, indem die Variable `user.keystore.path` so geändert wird, dass sie auf die Keystore-Datei in der Übertragungsfreigabe verweist.

```
/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 Damit die neuen signierten Zertifikate wirksam werden, starten Sie den `vmware-vcd`-Dienst auf der primären Appliance neu.

- a Führen Sie den Befehl aus, um den Dienst anzuhalten.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid cell) -s
```

- b Führen Sie den Befehl aus, um den Dienst zu starten.

```
systemctl start vmware-vcd
```

- 6 Stellen Sie die Appliances der Standby-Zelle und der Anwendungs-Zelle unter Verwendung des anfänglichen Root-Kennworts bereit, das mit dem Keystore-Kennwort übereinstimmt.

Ergebnisse

Alle neu bereitgestellten Appliances, die denselben Speicher des gemeinsam genutzten NFS-Übertragungsdiensts verwenden, sind mit denselben signierten SSL-Platzhalterzertifikaten konfiguriert, die von der primären Appliance verwendet werden.

Erstellen und Importieren der von einer Zertifizierungsstelle signierten SSL-Zertifikate in die VMware Cloud Director-Appliance

Das Erstellen und Importieren der von einer Zertifizierungsstelle signierten Zertifikate bietet die höchste Vertrauensebene für die SSL-Kommunikation und hilft Ihnen, die Verbindungen innerhalb Ihrer Cloud zu sichern.

Jeder VMware Cloud Director-Server benötigt zwei SSL-Zertifikate, um die Kommunikation zwischen Clients und Servern zu sichern. Jeder VMware Cloud Director-Server muss zwei unterschiedliche SSL-Endpoints unterstützen – für die HTTPS- und die Konsolen-Proxy-Kommunikation.

In der VMware Cloud Director-Appliance nutzen diese beiden Endpoints dieselbe IP-Adresse oder denselben Hostnamen, verwenden jedoch zwei unterschiedliche Ports: 443 für die HTTPS-Kommunikation und 8443 für die Konsolen-Proxy-Kommunikation. Jeder Endpoint muss über ein eigenes SSL-Zertifikat verfügen. Sie können dasselbe Zertifikat für beide Endpoints verwenden, z. B. mithilfe eines Platzhalterzertifikats.

Bei den Zertifikaten für beide Endpoints müssen sowohl ein definierter X.500-Name als auch eine X.509 Subject Alternative Name-Erweiterung angegeben werden.

Wenn Sie bereits über einen eigenen privaten Schlüssel und eine von einer Zertifizierungsstelle signierte Zertifikatsdatei verfügen, befolgen Sie die in [Importieren von privaten Schlüsseln und den von einer Zertifizierungsstelle signierten SSL-Zertifikaten in die VMware Cloud Director-Appliance](#) beschriebenen Schritte.

Wichtig Bei der Bereitstellung generiert die VMware Cloud Director-Appliance selbstsignierte Zertifikate mit einer Schlüsselgröße von 2.048 Bit. Sie müssen die Sicherheitsanforderungen Ihrer Installation überprüfen, bevor Sie eine geeignete Schlüsselgröße auswählen. Schlüssel mit einer Länge von weniger als 1024 Bit werden entsprechend NIST Special Publication 800-131A nicht mehr unterstützt.

Das in diesem Verfahren verwendete Keystore-Kennwort ist das **root**-Benutzerkennwort und wird als *root_password* dargestellt.

Voraussetzungen

Machen Sie sich mit dem Befehl `keytool` vertraut. Sie verwenden `keytool`, um die von einer Zertifizierungsstelle signierten SSL-Zertifikate in die VMware Cloud Director-Appliance zu importieren. VMware Cloud Director speichert eine Kopie von `keytool` unter `/opt/vmware/vcloud-director/jre/bin/keytool`.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der VMware Cloud Director-Appliance als **root** an.
- 2 Je nach den Anforderungen Ihrer Umgebung wählen Sie eine der folgenden Optionen aus.

Wenn Sie die VMware Cloud Director-Appliance bereitstellen, generiert VMware Cloud Director automatisch selbstsignierte Zertifikate mit einer Schlüsselgröße von 2048 Bit für den HTTPS- und den Konsolen-Proxy-Dienst.

 - Wenn Ihre Zertifizierungsstelle die Zertifikate signieren soll, die bei der Bereitstellung generiert werden, fahren Sie mit [Schritt 5](#) fort.
 - Wenn Sie neue Zertifikate mit benutzerdefinierten Optionen generieren möchten, z. B. eine größere Schlüsselgröße, fahren Sie mit [Schritt 3](#) fort.
- 3 Führen Sie den Befehl aus, um die vorhandene Datei `certificates.ks` zu sichern.

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

- 4 Führen Sie den Befehl zum Erstellen von Schlüsselpaaren aus einem öffentlichen und einem privaten Schlüssel für den HTTPS- und den Konsolen-Proxy-Dienst aus.

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

Der Befehl erstellt oder aktualisiert einen Keystore unter `certificates.ks` mit dem von Ihnen angegebenen Kennwort. Zertifikate werden mithilfe der Standardwerte des Befehls erstellt. Je nach DNS-Konfiguration Ihrer Umgebung ist der CN (Common Name, Allgemeiner Name) des Ausstellers für jeden Dienst entweder auf die IP-Adresse oder den FQDN festgelegt. Für das Zertifikat wird die Standardschlüssellänge von 2048-Bit verwendet und das Zertifikat läuft ein Jahr nach der Erstellung ab.

Wichtig Aufgrund von Konfigurationsbeschränkungen in der VMware Cloud Director-Appliance müssen Sie den Speicherort `/opt/vmware/vcloud-director/certificates.ks` für den Zertifikat-Keystore verwenden.

Hinweis Sie verwenden das **root**-Kennwort der Appliance als Keystore-Kennwort.

- 5 Erstellen Sie eine Zertifikatsignieranforderung (CSR) für den HTTPS-Dienst und für den Konsolen-Proxy-Dienst.

Wichtig Die VMware Cloud Director-Appliance nutzt dieselbe IP-Adresse und denselben Hostnamen für den HTTPS-Dienst und den Konsolen-Proxy-Dienst. Aus diesem Grund müssen die CSR-Erstellungsbefehle denselben DNS und dieselben IP-Adressen für das SAN (Subject Alternative Name)-Erweiterungsargument aufweisen.

- a Erstellen Sie eine Zertifikatsignieranforderung in der Datei `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 Erstellen Sie eine Zertifikatsignieranforderung in der Datei `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 Senden Sie die Zertifikatsignieranforderungen an die Zertifizierungsstelle.

Wenn Ihre Zertifizierungsstelle die Angabe eines Webservertyps verlangt, geben Sie Jakarta Tomcat an.

Sie erhalten die von der Zertifizierungsstelle signierten Zertifikate.

- 7 Kopieren Sie die von der Zertifizierungsstelle signierten Zertifikate, das Stammzertifikat der Zertifizierungsstelle und alle Zwischenzertifikate auf die VMware Cloud Director-Appliance.

8 Führen Sie die Befehle aus, um die signierten Zertifikate in den PKCS12-Keystore zu importieren.

- a Importieren Sie das Stammzertifikat der Zertifizierungsstelle aus der Datei `root.cer` in die Keystore-Datei `certificates.ks`.

```
keytool -import -storetype PKCS12 -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias root -file root_certificate_file
```

- b Wenn Sie Zwischenzertifikate erhalten haben, importieren Sie sie aus der Datei `intermediate.cer` in die Keystore-Datei `certificates.ks`.

```
keytool -import -storetype PKCS12 -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias intermediate -file intermediate_certificate_file
```

- c Importieren Sie das Zertifikat des HTTPS-Diensts.

```
keytool -import -storetype PKCS12 -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias http -file http_certificate_file
```

- d Importieren Sie das Konsolen-Proxy-Dienstzertifikat.

```
keytool -import -storetype PKCS12 -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias consoleproxy -file console_proxy_certificate_file
```

Die Befehle überschreiben die Datei `certificates.ks` mit den neu erworbenen, von der Zertifizierungsstelle signierten Versionen der Zertifikate.

9 Um zu überprüfen, ob die Zertifikate importiert wurden, führen Sie den Befehl aus, um den Inhalt der Keystore-Datei aufzulisten.

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

10 Führen Sie den Befehl aus, um die Zertifikate in die VMware Cloud Director-Instanz zu importieren.

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

- 11 Damit die neuen signierten Zertifikate wirksam werden, starten Sie den `vmware-vcd`-Dienst auf der VMware Cloud Director-Appliance neu.
 - a Führen Sie den Befehl aus, um den Dienst anzuhalten.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid cell) -s
```

- b Führen Sie den Befehl aus, um den Dienst zu starten.

```
systemctl start vmware-vcd
```

Nächste Schritte

- Wenn Sie Platzhalterzertifikate verwenden, finden Sie weitere Informationen unter [Bereitstellen der VMware Cloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation](#).
- Wenn Sie keine Platzhalterzertifikate verwenden, wiederholen Sie diesen Vorgang auf allen VMware Cloud Director-Servern in der Servergruppe.
- Weitere Informationen zum Ersetzen der Zertifikate für die eingebettete PostgreSQL-Datenbank und die Verwaltungsschnittstelle der VMware Cloud Director-Appliance finden Sie unter [Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und VMware Cloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats](#).

Importieren von privaten Schlüsseln und den von einer Zertifizierungsstelle signierten SSL-Zertifikaten in die VMware Cloud Director-Appliance

Wenn Sie über einen eigenen privaten Schlüssel und von einer Zertifizierungsstelle signierte Zertifikatsdateien verfügen, müssen Sie vor dem Import der Keystores in Ihre VMware Cloud Director-Umgebung Keystore-Dateien erstellen, in die die Zertifikate und die privaten Schlüssel für den HTTPS- und den Konsolen-Proxy-Dienst importiert werden.

Voraussetzungen

- Machen Sie sich mit dem Befehl `keytool` vertraut. Sie verwenden `keytool`, um die von einer Zertifizierungsstelle signierten SSL-Zertifikate in die VMware Cloud Director-Appliance zu importieren. VMware Cloud Director speichert eine Kopie von `keytool` unter `/opt/vmware/vcloud-director/jre/bin/keytool`.
- Kopieren Sie Ihre Zwischenzertifikate, das Root-CA-Zertifikat, den von der Zertifizierungsstelle signierten HTTPS-Dienst und die privaten Schlüssel und Zertifikate des Konsolen-Proxy-Diensts auf die Appliance.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der VMware Cloud Director-Appliance als `root` an.

- 2 Wenn Sie über Zwischenzertifikate verfügen, führen Sie den Befehl aus, um das von der Zertifizierungsstelle signierte Root-Zertifikat mit den Zwischenzertifikaten zu kombinieren und eine Zertifikatskette zu erstellen.

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

- 3 Verwenden Sie OpenSSL, um für den HTTPS- und den Konsolen-Proxy-Dienst Keystore-Zwischendateien mit dem privaten Schlüssel, der Zertifikatskette und dem entsprechenden Alias zu erstellen, und geben Sie ein Kennwort für jede Keystore-Datei an.

- a Erstellen Sie die Keystore-Datei für den HTTPS-Dienst.

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.p12 -chain
```

- b Erstellen Sie die Keystore-Datei für den Konsolen-Proxy-Dienst.

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.p12 -chain
```

- 4 Führen Sie den Befehl aus, um die vorhandene Datei `certificates.ks` zu sichern.

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

- 5 Verwenden Sie den Befehl `keytool`, um die PKCS12-Keystores in den Keystore `certificates.ks` zu importieren.

- a Importieren Sie den PKCS12-Keystore für den HTTPS-Dienst.

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

- b Importieren Sie den PKCS12-Keystore für den Konsolen-Proxy-Dienst.

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

- 6 Stellen Sie sicher, dass der Import der Zertifikate erfolgreich ist.

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

- 7 Führen Sie den Befehl aus, um die signierten Zertifikate in die VMware Cloud Director-Instanz zu importieren.

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

- 8 Damit die von einer Zertifizierungsstelle signierten Zertifikate wirksam werden, starten Sie den `vmware-vcd`-Dienst auf der VMware Cloud Director-Appliance neu.

```
service vmware-vcd restart
```

Nächste Schritte

- Wenn Sie Platzhalterzertifikate verwenden, finden Sie weitere Informationen unter [Bereitstellen der VMware Cloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation](#).
- Wenn Sie keine Platzhalterzertifikate verwenden, wiederholen Sie diesen Vorgang in allen Zellen der VMware Cloud Director-Appliance in der Servergruppe.
- Weitere Informationen zum Ersetzen der Zertifikate für die eingebettete PostgreSQL-Datenbank und die Verwaltungsschnittstelle der VMware Cloud Director-Appliance finden Sie unter [Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und VMware Cloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats](#).

Nach der Bereitstellung der VMware Cloud Director-Appliance

Nach dem Erstellen der VMware Cloud Director-Servergruppe können Sie Microsoft Sysprep-Dateien und die Cassandra-Datenbank installieren. Wenn Sie eine PostgreSQL-Datenbank verwenden, können Sie SSL konfigurieren und einige Parameter in der Datenbank anpassen.

Nach der Erstellung der VMware Cloud Director-Appliance können Sie die Netzwerkfunktionen von vSphere verwenden, um eine neue Netzwerkschnittstellenkarte (NIC) hinzuzufügen. Weitere Informationen finden Sie unter [Hinzufügen eines Netzwerkadapters zu einer virtuellen Maschine](#) im *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Hinweis Wenn Ihr Cluster für automatisches Failover konfiguriert ist, müssen Sie nach der Bereitstellung einer zusätzlichen oder mehrerer zusätzlicher Zellen die Appliance-API verwenden, um den Failover-Modus auf `Automatic` zurückzusetzen. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API](#). Der standardmäßige Failover-Modus für neue Zellen lautet `Manual`. Wenn der Failover-Modus für die Knoten des Clusters inkonsistent ist, lautet der Failover-Modus des Clusters `Indeterminate`. Der Modus `Indeterminate` kann zwischen den Knoten und den einer alten primären Zelle folgenden Knoten zu inkonsistenten Clusterzuständen führen. Informationen zum Anzeigen des Failover-Modus des Clusters finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

Ab Version 10.1 können Dienstanbieter und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Verweigerungsliste interner Hosts, die für Mandanten, die die VMware Cloud Director-API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Verweigerungsliste, nachdem Sie die Installation oder das Upgrade von VMware Cloud Director durchgeführt haben und bevor Sie Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie im [Konfigurieren einer Negativliste für Testverbindungen](#).

Ändern der VMware Cloud Director-Appliance-Zeitzone

Nachdem Sie die VMware Cloud Director-Appliance erfolgreich bereitgestellt haben, können Sie die Systemzeitzone der Appliance ändern. Alle VMware Cloud Director-Appliance-Instanzen in der Servergruppe und der Übertragungsserverspeicher müssen dieselben Einstellungen verwenden.

Voraussetzungen

- Bereitstellen der VMware Cloud Director-Appliance. Weitere Informationen finden Sie im [Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance](#).
- Ändern Sie die Zeitzone des Übertragungsserverspeichers in die neue Zeitzone der primären VMware Cloud Director-Appliance.

Verfahren

- 1 Wenn Sie eine Webkonsole oder eine Remote-Konsole für den primären Knoten verwenden, wählen Sie unten links im Konsolenfenster **Zeitzone festlegen** aus.
- 2 Wählen Sie einen Standort, ein Land und eine Region für die Zeitzone aus.
Die neu ausgewählte Zeitzone wird unten links im Konsolenfenster angezeigt.
- 3 Melden Sie sich bei der Konsole der VMware Cloud Director-Appliance als **root**-Benutzer an.
- 4 Um sicherzustellen, dass die VMware Cloud Director-Appliance die neue Zeitzone verwendet, starten Sie den Dienst `vmware-vcd neu`.
- 5 Wiederholen Sie [Schritt 1](#) bis [Schritt 4](#) für alle Standby- und Anwendungszellen in Ihrer VMware Cloud Director-Bereitstellung.

Anpassen öffentlicher Adressen für die VMware Cloud Director-Appliance

Zum Erfüllen der Anforderungen des Lastausgleichsdiensts oder Proxys können Sie die Webadressen des Standard-Endpoints für das VMware Cloud Director-Webportal, die VMware Cloud Director-API und den Konsolen-Proxy ändern.

Sie müssen die Adresse des öffentlichen VMware Cloud Director-Konsolen-Proxys konfigurieren, da die Appliance eine einzelne IP-Adresse mit dem benutzerdefinierten Port 8443 für den Konsolen-Proxy-Dienst verwendet. Weitere Informationen finden Sie unter [6](#).

Voraussetzungen

Stellen Sie sicher, dass Sie sich als **Systemadministrator** angemeldet haben. Nur ein **Systemadministrator** kann öffentliche Endpoints anpassen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste des Service Provider Admin Portal **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Einstellungen** auf **Öffentliche Adressen**.
- 3 Um die öffentlichen Endpoints anzupassen, klicken Sie auf **Bearbeiten**.

- 4 Bearbeiten Sie zum Anpassen der VMware Cloud Director-URLs die **Webportal**-Endpoints.
 - a Geben Sie eine benutzerdefinierte öffentliche VMware Cloud Director-URL für (sichere) HTTPS-Verbindungen ein und klicken Sie auf **Hochladen**, um die Zertifikate hochzuladen, die die Vertrauenskette für diesen Endpoint bilden.

Die Zertifikatskette muss mit dem vom Dienst-Endpoint verwendeten Zertifikat übereinstimmen. Hierbei handelt es sich um das Zertifikat, das auf alle VMware Cloud Director-Zellen-Keystores mit dem Alias `consoleproxy` hochgeladen wurde. SSL-Terminierung der Konsolen-Proxy-Verbindungen auf einem Lastausgleichsdienst wird nicht unterstützt. Die Zertifikatskette muss ein Endpoint-Zertifikat, Zwischenzertifikate und ein Stammzertifikat im PEM-Format ohne einen privaten Schlüssel enthalten.

- 5 (Optional) Um die Cloud Director REST API- und die OpenAPI-URLs anzupassen, deaktivieren Sie die Option **Webportaleinstellungen verwenden**.

- a Geben Sie eine benutzerdefinierte HTTP-Basis-URL ein.

Wenn Sie die HTTP-Basis-URL beispielsweise auf `http://vcloud.example.com` setzen, können Sie auf die VMware Cloud Director-API unter `http://vcloud.example.com/api` und auf VMware Cloud Director OpenAPI unter `http://vcloud.example.com/cloudapi` zugreifen.

- b Geben Sie eine benutzerdefinierte HTTPS REST API-Basis-URL ein und klicken Sie auf **Hochladen**, um die Zertifikate hochzuladen, die die Vertrauenskette für diesen Endpoint bilden.

Wenn Sie die Basis-URL der HTTPS-REST API beispielsweise auf `https://vcloud.example.com` setzen, können Sie auf die VMware Cloud Director-API unter `https://vcloud.example.com/api` und auf VMware Cloud Director OpenAPI unter `https://vcloud.example.com/cloudapi` zugreifen.

Die Zertifikatskette muss mit dem vom Dienst-Endpoint verwendeten Zertifikat übereinstimmen. Hierbei handelt es sich entweder um das Zertifikat, das auf alle VMware Cloud Director-Zellen-Keystores mit dem Alias `http` hochgeladen wurde, oder um das VIP-Zertifikat des Lastausgleichsdiensts, wenn SSL-Terminierung verwendet wird. Die Zertifikatskette muss ein Endpoint-Zertifikat, Zwischenzertifikate und ein Stammzertifikat im PEM-Format ohne einen privaten Schlüssel enthalten.

- 6 Geben Sie die Adresse eines benutzerdefinierten öffentlichen VMware Cloud Director-Konsolen-Proxys ein.

Diese Adresse ist der vollqualifizierte Domänenname (FQDN) der `eth0`-Netzwerkkarte der VMware Cloud Director-Appliance, die entweder durch dem FQDN oder die IP-Adresse mit dem benutzerdefinierten Port 8443 für den Konsolen-Proxy-Dienst angegeben wird.

Geben Sie für eine VMware Cloud Director-Appliance-Instanz mit dem FQDN `vcloud.example.com` beispielsweise `vcloud.example.com:8443` ein.

VMware Cloud Director verwendet die Konsolen-Proxy-Adresse beim Öffnen eines Remote-Konsolenfensters auf einer VM.

7 Klicken Sie zum Speichern der Änderungen auf **Speichern**.

Installieren und Konfigurieren einer Cassandra-Datenbank zum Speichern von historischen Metrikdaten

VMware Cloud Director kann Metriken erfassen, die aktuelle und historische Informationen über die Leistung und den Ressourcenverbrauch der virtuellen Maschinen in Ihrer Cloud zur Verfügung stellen. Daten für historische Metriken werden in einem Cassandra-Cluster gespeichert.

Cassandra ist eine Open Source-Datenbank, die Sie verwenden können, um den zugrunde liegenden Speicher für eine skalierbare, leistungsfähige Lösung zur Erfassung von Zeitreihendaten (z. B. Metriken für virtuelle Maschinen) bereitzustellen. Wenn VMware Cloud Director das Abrufen von historischen Metriken aus virtuellen Maschinen unterstützen soll, müssen Sie einen Cassandra-Cluster installieren und konfigurieren und das Dienstprogramm `cell-management-tool` zum Herstellen einer Verbindung zwischen dem Cluster und VMware Cloud Director verwenden. Für das Abrufen aktueller Metriken ist keine optionale Datenbanksoftware erforderlich.

Voraussetzungen

- Bevor Sie die optionale Datenbanksoftware konfigurieren, stellen Sie sicher, dass VMware Cloud Director installiert ist und ausgeführt wird.
- Wenn Sie noch nicht mit Cassandra vertraut sind, lesen Sie die Informationen unter <http://cassandra.apache.org/>.
- Eine Liste der Cassandra-Versionen, die zur Verwendung als Metrikdatenbank unterstützt werden, finden Sie in den *VMware Cloud Director-Versionshinweise*. Sie können Cassandra unter <http://cassandra.apache.org/download/> herunterladen.
- Installieren und konfigurieren Sie den Cassandra-Cluster:
 - Der Cassandra-Cluster muss mindestens vier virtuelle Maschinen enthalten, die auf zwei oder mehr Hosts bereitgestellt werden.
 - Zwei Cassandra-Seed-Knoten sind erforderlich.
 - Aktivieren Sie Client-zu-Knoten-Verschlüsselung mit Cassandra. Weitere Informationen finden Sie unter <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html>.
 - Aktivieren Sie Cassandra-Benutzerauthentifizierung. Weitere Informationen finden Sie unter <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html>.
 - Aktivieren Sie Java Native Access (JNA) Version 3.2.7 oder höher auf jedem Cassandra-Cluster.
 - Knoten-zu-Knoten-Verschlüsselung mit Cassandra ist optional.

- Verwendung von SSL mit Cassandra ist optional. Wenn Sie sich gegen die Aktivierung von SSL für Cassandra entscheiden, müssen Sie den Konfigurationsparameter `cassandra.use.ssl` in der Datei `global.properties` in jeder Zelle auf 0 setzen (`$VCLLOUD_HOME/etc/global.properties`)

Verfahren

- 1 Verwenden Sie das Dienstprogramm `cell-management-tool`, um eine Verbindung zwischen VMware Cloud Director und den Knoten im Cassandra-Cluster herzustellen.

Im folgenden Beispielbefehl sind `node1-ip`, `node2-ip`, `node3-ip` und `node4-ip` die IP-Adressen der Mitglieder des Cassandra-Clusters. Es wird der Standardport (9042) verwendet. Metrikdaten werden 15 Tage lang aufbewahrt.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --configure
--create-schema \ --cluster-nodes node1-ip,node2-ip,node3-ip, node4-ip \ --username admin
--password 'P@55w0rd' --ttl 15
```

Informationen zur Verwendung des Zellenverwaltungstools finden Sie unter [Kapitel 5 Überblick über das Zellenverwaltungstool](#).

- 2 (Optional) Wenn Sie ein Upgrade von VMware Cloud Director von Version 9.1 durchführen, verwenden Sie das Dienstprogramm `cell-management-tool`, um die Metrikdatenbank zum Speichern von mehrstufigen Metriken zu konfigurieren.

Führen Sie einen Befehl ähnlich dem folgenden Beispiel aus:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --add-
rollup \ --username admin --password 'P@55w0rd'
```

- 3 Starten Sie jede VMware Cloud Director-Zelle neu.

Installieren und Konfigurieren einer RabbitMQ AMQP Broker-Instanz

Wenn Sie blockierende Aufgaben, Benachrichtigungen oder VMware Cloud Director-API-Erweiterungen wie Container Service Extension (CSE) und VMware Cloud Director App Launchpad verwenden möchten, müssen Sie einen RabbitMQ AMQP Broker installieren und konfigurieren.

Advanced Message Queuing Protocol (AMQP) ist ein offener Standard für Nachrichtenwarteschlangen, der flexible Messaging-Funktionen für Unternehmenssysteme unterstützt. VMware Cloud Director verwendet RabbitMQ AMQP Broker zum Bereitstellen des Nachrichtenbuses, der von Erweiterungsdiensten, Objekterweiterungen und Benachrichtigungen verwendet wird.

Bei VMware Cloud Director kann beim Konfigurieren von Benachrichtigungen die Verwendung eines MQTT-Clients eine Alternative zu RabbitMQ AMQP Broker sein. Weitere Informationen finden Sie im [Abonnieren von Ereignissen, Aufgaben und Metriken mithilfe eines MQTT-Clients](#).

Verfahren

- 1 Laden Sie den RabbitMQ-Server von <https://www.rabbitmq.com/download.html> herunter.
Die Liste der unterstützten RabbitMQ-Versionen finden Sie in den *VMware Cloud Director-Versionshinweise*.
- 2 Befolgen Sie die Installationsanweisungen für RabbitMQ und installieren Sie die Software auf einem geeigneten Host.
Der RabbitMQ-Serverhost muss für jede VMware Cloud Director-Zelle im Netzwerk erreichbar sein.
- 3 Notieren Sie sich während der RabbitMQ-Installation folgende Werte, die Sie später beim Konfigurieren von VMware Cloud Director für die Zusammenarbeit mit dieser RabbitMQ-Installation bereitstellen müssen:
 - Den vollqualifizierten Domännennamen des RabbitMQ-Serverhosts, z. B. *amqp.example.com*.
 - Eine zur Authentifizierung mit RabbitMQ gültige Kombination aus Benutzername und Kennwort.
 - Den Port, über den der Broker Nachrichten empfängt. Der Standardwert lautet 5672 für nicht Nicht-SSL. Der Standardport für SSL/TLS lautet 5671.
 - Das Kommunikationsprotokoll ist TCP.
 - Den virtuellen RabbitMQ-Host. Der Standardwert ist "/".

Nächste Schritte

Der AMQP-Dienst von VMware Cloud Director versendet standardmäßig unverschlüsselte Nachrichten. Sie können den AMQP-Dienst so konfigurieren, dass diese Nachrichten mit SSL verschlüsselt werden. Sie können den Dienst auch so konfigurieren, dass er das Broker-Zertifikat überprüft, indem Sie den standardmäßigen JCEKS Trust Store der Java-Laufzeitumgebung auf der VMware Cloud Director-Zelle verwenden, normalerweise unter `$VCLLOUD_HOME/jre/lib/security/cacerts`.

Informationen zum Aktivieren von SSL mit dem AMQP-Dienst von VMware Cloud Director finden Sie unter [Konfigurieren eines AMQP Brokers](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Ändern des Root-Kennworts der VMware Cloud Director-Appliance

Wenn Sie das Root-Kennwort für eine VMware Cloud Director-Appliance ändern, müssen Sie auch den Zertifikat-Keystore der Appliance aktualisieren, um das neue Kennwort verwenden zu können.

Voraussetzungen

- Machen Sie sich mit dem Befehl `keytool` vertraut. VMware Cloud Director speichert eine Kopie von „keytool“ unter `/opt/vmware/vcloud-director/jre/bin/keytool`.

- Wenn Sie Platzhalterzertifikate verwenden und diese im gemeinsam genutzten NFS-Übertragungsspeicher speichern, befolgen Sie das unter [Bereitstellen der VMware Cloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation](#) beschriebene Verfahren, um sicherzustellen, dass sie aktualisiert werden.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der VMware Cloud Director-Appliance als **root** an.
- 2 Führen Sie den Befehl `passwd` aus und ändern Sie das Kennwort für den **root**-Benutzer.

```
passwd root
```

Hinweis Wenn der FIPS-Modus aktiviert ist, muss das **root**-Kennwort der Appliance mindestens 14 Zeichen enthalten.

Hinweis Wenn das Root-Kennwort bereits abgelaufen ist, werden Sie von VMware Cloud Director dazu aufgefordert, es beim ersten Anmelden bei der VMware Cloud Director-Appliance-Konsole als **root** festzulegen.

- 3 Führen Sie den Befehl aus, um die vorhandene Keystore-Datei für Zertifikate zu sichern.

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

- 4 Führen Sie zum Generieren eines neuen Zertifikats-Keystore den Befehl `keytool` aus.

```
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
```

Hinweis Ab VMware Cloud Director 10.2 lautet der standardmäßige Keystore-Typ für Zertifikate für die VMware Cloud Director-Appliance PKCS12. Wenn Sie eine Version der Appliance verwenden, die auf Version 10.2 aktualisiert wurde, verwenden Sie JCEKS als `-srcstoretype` und `-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 Führen Sie den Befehl aus, um die alte Keystore-Datei für Zertifikate mit der neuen zu ersetzen.

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

- 6 Führen Sie den Befehl `chown` aus, um Benutzer- und Gruppenbesitz der keystore-Datei zu überprüfen.

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

- 7 Um das neue Kennwort für den Keystore zu verwenden, aktualisieren Sie die Konfiguration des VMware Cloud Director-Servers:

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

Nächste Schritte

Wiederholen Sie dieses Verfahren für jede Appliance im Cluster.

Wichtig Für alle Appliances muss dasselbe Root-Kennwort verwendet werden. Für jede neu bereitgestellte Appliance muss das neue Root-Kennwort verwendet werden.

Upgrade und Migration der VMware Cloud Director-Appliance

Ab Version 9.7 enthält die VMware Cloud Director-Appliance eine eingebettete PostgreSQL-Datenbank mit einer Hochverfügbarkeitsfunktion. Sie können ein Upgrade der VMware Cloud Director-Appliance auf eine höhere Version durchführen. Sie können Ihre vorhandene frühere Version von VMware Cloud Director mit einer externen PostgreSQL-Datenbank auf eine VMware Cloud Director-Umgebung migrieren, die aus Bereitstellungen der VMware Cloud Director-Appliance der Version 10.0 oder höher besteht.

Upgrade der VMware Cloud Director-Appliance

Informationen zum Upgrade der Version 9.7 der VMware Cloud Director-Appliance auf Version 10.2 finden Sie unter [Upgrade der VMware Cloud Director-Appliance mithilfe eines Update-Pakets](#).

Ab VMware Cloud Director 10.0 werden Microsoft SQL Server-Datenbanken nicht mehr unterstützt.

Wenn Sie ein Upgrade von VMware Cloud Director durchführen, muss die neue Version mit den folgenden Komponenten Ihrer vorhandenen Installation kompatibel sein:

- Mit der Datenbanksoftware, die Sie derzeit für die VMware Cloud Director-Datenbank verwenden. Weitere Informationen finden Sie in der Tabelle „Upgrade- und Migrationspfade“.
- Mit der derzeit verwendeten VMware vSphere® -Version.
- Mit der derzeit verwendeten VMware NSX®-Version.
- Alle Drittanbieterkomponenten, die direkt mit VMware Cloud Director interagieren.

Informationen zur Kompatibilität von VMware Cloud Director mit anderen VMware-Produkten und mit Datenbanken von Drittanbietern finden Sie in den *VMware-Produkt-Interoperabilitätstabellen* unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. Wenn Sie vSphere- oder NSX-Komponenten als Teil des VMware Cloud Director-Upgrades aktualisieren möchten, müssen Sie diese Upgrades nach dem Upgrade von VMware Cloud Director durchführen. Weitere Informationen finden Sie unter [Nach dem Upgrade von VMware Cloud Director](#).

Nach dem Upgrade mindestens eines VMware Cloud Director-Servers können Sie die VMware Cloud Director-Datenbank aktualisieren. In der Datenbank werden Informationen über den Laufzeitstatus des Servers gespeichert. Dazu gehören auch die Status aller VMware Cloud Director-Aufgaben, die auf ihm ausgeführt werden. Um sicherzustellen, dass nach einem Upgrade keine ungültigen Aufgabeninformationen in der Datenbank verbleiben, müssen Sie sich vergewissern, dass auf keinem Server Aufgaben aktiv sind, bevor Sie mit dem Upgrade beginnen.

Das Upgrade behält die folgenden Artefakte bei, die nicht in der VMware Cloud Director-Datenbank gespeichert sind:

- Lokale und globale Eigenschaftendateien werden in die neue Installation kopiert.
- Zur Unterstützung der Gastanpassung verwendete Microsoft-Sysprep-Dateien werden in die neue Installation kopiert.

Damit alle Server in der Servergruppe und die Datenbank aktualisiert werden können, muss VMware Cloud Director für eine gewisse Zeit heruntergefahren werden. Wenn Sie einen Lastausgleichsdienst verwenden, kann dieser so konfiguriert werden, dass eine Meldung mit folgendem oder ähnlichem Inhalt angezeigt wird: `Das System steht wegen eines Upgrades nicht zur Verfügung.`

Ab Version 10.1 können Dienstanbieter und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Verweigerungsliste interner Hosts, die für Mandanten, die die VMware

Cloud Director-API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Verweigerungsliste, nachdem Sie die Installation oder das Upgrade von VMware Cloud Director durchgeführt haben und bevor Sie Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie im [Konfigurieren einer Negativliste für Testverbindungen](#).

Wichtig Nach dem Upgrade auf Version 10.1 und höher überprüft VMware Cloud Director immer die Zertifikate für alle mit ihm verbundenen Infrastruktur-Endpoints. Der Grund hierfür besteht darin, dass die Verwaltung von SSL-Zertifikaten durch VMware Cloud Director geändert wurde. Wenn Sie die Zertifikate vor dem Upgrade nicht in VMware Cloud Director importieren, kommt es in vCenter Server- und NSX-Verbindungen aufgrund von Problemen bei der SSL-Überprüfung möglicherweise zu fehlgeschlagenen Verbindungen. In diesem Fall haben Sie nach dem Upgrade zwei Möglichkeiten:

- 1 Führen Sie den Befehl `trust-infra-certs` des Zellenverwaltungstools aus, um automatisch alle Zertifikate in den zentralisierten Zertifikatspeicher zu importieren. Weitere Informationen finden Sie unter [Importieren von Endpoint-Zertifikaten aus vSphere-Ressourcen](#).
- 2 Wählen Sie in der Service Provider Admin Portal-Benutzeroberfläche jede vCenter Server- und NSX-Instanz aus und geben Sie die Anmeldedaten beim Akzeptieren des Zertifikats erneut ein.

Migrieren der VMware Cloud Director-Appliance

Wenn Ihre vorhandene VMware Cloud Director-Servergruppe aus Bereitstellungen der VMware Cloud Director 9.5-Appliance besteht, können Sie Ihre Umgebung nur auf eine neuere Version der VMware Cloud Director-Appliance migrieren. Verwenden Sie das VMware Cloud Director-Installationsprogramm für Linux, um die vorhandene Umgebung ausschließlich als Teil des Migrations-Workflows zu aktualisieren. Weitere Informationen finden Sie unter [Migrieren auf die vCloud Director-Appliance](#).

Wenn in Ihrer VMware Cloud Director-Umgebung eine externe Oracle- oder Microsoft SQL-Datenbank verwendet wird, müssen Sie vor dem Upgrade auf VMware Cloud Director 10.2 eine Migration auf eine PostgreSQL-Datenbank durchführen. Informationen zu Upgrade-Pfaden finden Sie unter [Upgrade von VMware Cloud Director unter Linux](#).

Upgrade- und Migrationspfade und -Workflows

Quellumgebung	Zielumgebung
	VMware Cloud Director-Appliance 10.2 mit einer eingebetteten PostgreSQL-Datenbank
<p>VMware Cloud Director 9.7 unter Linux mit einer externen Microsoft SQL Server-Datenbank</p>	<ol style="list-style-type: none"> <li data-bbox="810 380 1423 537">1 Führen Sie eine Migration auf die VMware Cloud Director-Appliance 9.7 durch. Weitere Informationen finden Sie unter Migrieren von vCloud Director mit einer externen Microsoft SQL-Datenbank auf die vCloud Director-Appliance. <li data-bbox="810 537 1423 678">2 Führen Sie ein Upgrade Ihrer Umgebung auf die VMware Cloud Director-Appliance 10.2 durch. Siehe Upgrade der VMware Cloud Director-Appliance mithilfe eines Update-Pakets.
<p>VMware Cloud Director 9.7 unter Linux mit einer externen PostgreSQL-Datenbank</p>	<ol style="list-style-type: none"> <li data-bbox="810 688 1423 846">1 Führen Sie eine Migration auf die VMware Cloud Director-Appliance 9.7 durch. Weitere Informationen finden Sie unter Migrieren von vCloud Director mit einer externen PostgreSQL-Datenbank auf die vCloud Director-Appliance. <li data-bbox="810 846 1423 987">2 Führen Sie ein Upgrade Ihrer Umgebung auf die VMware Cloud Director-Appliance 10.2 durch. Siehe Upgrade der VMware Cloud Director-Appliance mithilfe eines Update-Pakets.
<p>VMware Cloud Director 10.0 unter Linux mit einer externen PostgreSQL-Datenbank</p>	<ol style="list-style-type: none"> <li data-bbox="810 997 1423 1155">1 Führen Sie eine Migration auf die VMware Cloud Director-Appliance 10.0 durch. Weitere Informationen finden Sie unter Migrieren von vCloud Director mit einer externen PostgreSQL-Datenbank auf die vCloud Director-Appliance. <li data-bbox="810 1155 1423 1295">2 Führen Sie ein Upgrade Ihrer Umgebung auf die VMware Cloud Director-Appliance 10.2 durch. Siehe Upgrade der VMware Cloud Director-Appliance mithilfe eines Update-Pakets.
<p>VMware Cloud Director 10.1 unter Linux mit einer externen PostgreSQL-Datenbank</p>	<ol style="list-style-type: none"> <li data-bbox="810 1306 1423 1463">1 Führen Sie eine Migration auf die VMware Cloud Director-Appliance 10.1 durch. Weitere Informationen finden Sie unter Migrieren von VMware Cloud Director mit einer externen PostgreSQL-Datenbank auf die VMware Cloud Director-Appliance. <li data-bbox="810 1463 1423 1604">2 Führen Sie ein Upgrade Ihrer Umgebung auf die VMware Cloud Director-Appliance 10.2 durch. Siehe Upgrade der VMware Cloud Director-Appliance mithilfe eines Update-Pakets.
<p>VMware Cloud Director-Appliance 9.7, 10.0 oder 10.1 mit einer eingebetteten PostgreSQL-Datenbank</p>	<p>Führen Sie ein Upgrade Ihrer Umgebung auf die VMware Cloud Director-Appliance 10.2 durch. Siehe Upgrade der VMware Cloud Director-Appliance mithilfe eines Update-Pakets.</p>

Upgrade der VMware Cloud Director-Appliance mithilfe eines Update-Pakets

Sie können die VMware Cloud Director-Appliance mithilfe eines Update-Pakets auf die neueste Version aktualisieren oder Patches auf die VMware Cloud Director-Appliance anwenden.

Während die Bereitstellung der VMware Cloud Director-Appliance aktualisiert wird, funktioniert der VMware Cloud Director-Dienst nicht mehr und es kann zu einem Ausfall kommen. Die Dauer des Ausfalls richtet sich nach dem Zeitraum, den Sie zum Aktualisieren aller VMware Cloud Director-Appliances und Ausführen des Upgrade-Skripts der VMware Cloud Director-Datenbank benötigen. Die Anzahl der funktionierenden Zellen in der VMware Cloud Director-Servergruppe wird reduziert, bis Sie den VMware Cloud Director-Dienst auf der letzten VMware Cloud Director-Appliance beenden. Ein ordnungsgemäß konfigurierter Lastausgleichsdienst vor den VMware Cloud Director-HTTP-Endpoints sollte das Routing des Datenverkehrs zu den beendeten Zellen stoppen.

Nachdem Sie das Upgrade auf jede VMware Cloud Director-Appliance angewendet haben und das Datenbank-Upgrade abgeschlossen ist, müssen Sie jede VMware Cloud Director-Appliance neu starten.

Voraussetzungen

Erstellen Sie einen Snapshot der primären VMware Cloud Director-Appliance.

- 1 Wenn bei einem Upgrade von Version 10.1 oder höher bzw. beim Anwenden von Patches das automatische Failover im Falle eines Ausfalls des primären Datenbankdienstes aktiviert ist, ändern Sie den Failover-Modus während des Upgrades in `Manual`. Nach dem Upgrade können Sie den Failover-Modus auf `Automatic` festlegen. Weitere Informationen finden Sie im [Automatisches Failover der VMware Cloud Director-Appliance](#).
- 2 Melden Sie sich bei der vCenter Server-Instanz an, auf der sich die primäre VMware Cloud Director-Appliance Ihres Hochverfügbarkeits-Clusters der Datenbank befindet.
- 3 Navigieren Sie zur primären VMware Cloud Director-Appliance, klicken Sie mit der rechten Maustaste darauf und klicken Sie auf **Stromversorgung > Gastbetriebssystem herunterfahren**.
- 4 Klicken Sie mit der rechten Maustaste auf die Appliance und klicken Sie auf **Snapshots > Snapshot erstellen**. Geben Sie einen Namen und optional eine Beschreibung für den neuen Snapshot ein und klicken Sie auf **OK**.
- 5 Klicken Sie mit der rechten Maustaste auf die VMware Cloud Director-Appliance und klicken Sie auf **Stromversorgung > Einschalten**.
- 6 Vergewissern Sie sich, dass sich alle Knoten in der Hochverfügbarkeitskonfiguration Ihrer Datenbank in einem ordnungsgemäßen Zustand befinden. Weitere Informationen finden Sie im [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

Verfahren

- 1 Melden Sie sich in einem Webbrowser bei der Appliance-Verwaltungsbenutzeroberfläche einer VMware Cloud Director-Appliance-Instanz an, um die primäre Appliance, `https://appliance_ip_address: 5480` zu identifizieren.

Notieren Sie sich den Namen der primären Appliance. Sie müssen das Upgrade der primären Appliance durchführen, bevor Sie die Upgrades für die Standby- und Anwendungszellen durchführen. Sie müssen beim Sichern der Datenbank den Namen der primären Appliance verwenden.

- 2 Laden Sie das Update-Paket in die Appliance herunter, für die Sie das Upgrade durchführen.

Hinweis Sie müssen zuerst das Upgrade der primären Appliance durchführen.

VMware Cloud Director wird als ausführbare Datei mit einem Namen im Format `VMware_Cloud_Director_v.v.v.v-nnnnnnnn_update.tar.gz` verteilt, wobei `v.v.v.v` die Produktversion und `nnnnnnnn` die Build-Nummer darstellt. Beispiel: `VMware_Cloud_Director_10.1.0.4424-14420378_update.tar.gz`.

- 3 Erstellen Sie das Verzeichnis `local-update-package`, in dem das Updatepaket extrahiert werden soll.

```
mkdir /tmp/local-update-package
```

- 4 Extrahieren Sie das Updatepaket in das neu erstellte Verzeichnis.

```
tar -zxvf VMware_Cloud_Director_v.v.v.v-nnnnnnnn_update.tar.gz \
-C /tmp/local-update-package
```

- 5 Legen Sie das Verzeichnis `local-update-package` als Update-Repository fest.

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

- 6 Suchen Sie nach Updates, um sicherzustellen, dass Sie das Repository ordnungsgemäß eingerichtet haben.

```
vamicli update --check
```

Die Upgrade-Version wird als verfügbares Update angezeigt.

- 7 Fahren Sie VMware Cloud Director herunter, indem Sie den folgenden Befehl ausführen:

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

- 8 Wenden Sie das verfügbare Upgrade an.

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

- 9 Wiederholen Sie 2 bis 8 für die verbleibenden Standby- und Anwendungszellen.

- 10 Sichern Sie von der primären Appliance aus die eingebettete Datenbank der VMware Cloud Director-Appliance.

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

- 11 Führen Sie von jeder Appliance aus das VMware Cloud Director-Datenbank-upgrade-Dienstprogramm aus.

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

- 12 Starten Sie die VMware Cloud Director-Appliance neu.

```
shutdown -r now
```

Nächste Schritte

- Wenn das Upgrade erfolgreich durchgeführt wurde, können Sie den Snapshot der VMware Cloud Director-Appliance löschen.
- Wenn das Upgrade nicht erfolgreich ist, können Sie die VMware Cloud Director-Appliance auf den Snapshot zurücksetzen, den Sie vor dem Upgrade erstellt haben. Weitere Informationen finden Sie im [Rollback einer VMware Cloud Director-Appliance, wenn ein Upgrade fehlschlägt](#).

Upgrade der VMware Cloud Director-Appliance mit dem VMware Update Repository

Sie können das VMware Update Repository verwenden, um ein Upgrade der VMware Cloud Director-Appliance von Version 9.7 auf Version 10.0 und höher durchzuführen oder Patches anzuwenden.

Hinweis Sie können das VMware Update Repository nur zum Upgrade von VMware Cloud Director auf die neueste VMware Cloud Director-Version verwenden. Nur die neueste Version ist im VMware Update Repository verfügbar. Wenn Sie ein Upgrade von VMware Cloud Director auf eine andere Version durchführen möchten, finden Sie weitere Informationen unter [Upgrade der VMware Cloud Director-Appliance mithilfe eines Update-Pakets](#).

Während die Bereitstellung der VMware Cloud Director-Appliance aktualisiert wird, funktioniert der VMware Cloud Director-Dienst nicht mehr und es kann zu einem Ausfall kommen. Die Dauer des Ausfalls richtet sich nach dem Zeitraum, den Sie zum Aktualisieren aller VMware Cloud Director-Appliances und Ausführen des Upgrade-Skripts der VMware Cloud Director-Datenbank benötigen. Die Anzahl der funktionierenden Zellen in der VMware Cloud Director-Servergruppe wird reduziert, bis Sie den VMware Cloud Director-Dienst auf der letzten VMware Cloud Director-Appliance beenden. Ein ordnungsgemäß konfigurierter Lastausgleichsdienst vor den VMware Cloud Director-HTTP-Endpoints sollte das Routing des Datenverkehrs zu den beendeten Zellen stoppen.

Nachdem Sie das Upgrade auf jede VMware Cloud Director-Appliance angewendet haben und das Datenbank-Upgrade abgeschlossen ist, müssen Sie jede VMware Cloud Director-Appliance neu starten.

Voraussetzungen

- Erstellen Sie einen Snapshot der primären VMware Cloud Director-Appliance.
 - a Wenn bei einem Upgrade von Version 10.1 oder höher bzw. beim Anwenden von Patches das automatische Failover im Falle eines Ausfalls des primären Datenbankdienstes aktiviert ist, ändern Sie den Failover-Modus für die Dauer des Upgrades in `Manual`. Nach dem Upgrade können Sie den Failover-Modus auf `Automatic` festlegen. Weitere Informationen finden Sie im [Automatisches Failover der VMware Cloud Director-Appliance](#).
 - b Melden Sie sich bei der vCenter Server-Instanz an, auf der sich die primäre VMware Cloud Director-Appliance Ihres Hochverfügbarkeits-Clusters der Datenbank befindet.
 - c Navigieren Sie zur primären VMware Cloud Director-Appliance, klicken Sie mit der rechten Maustaste darauf und klicken Sie auf **Stromversorgung > Gastbetriebssystem herunterfahren**.
 - d Klicken Sie mit der rechten Maustaste auf die Appliance und klicken Sie auf **Snapshots > Snapshot erstellen**. Geben Sie einen Namen und optional eine Beschreibung für den neuen Snapshot ein und klicken Sie auf **OK**.
 - e Klicken Sie mit der rechten Maustaste auf die VMware Cloud Director-Appliance und klicken Sie auf **Stromversorgung > Einschalten**.
 - f Vergewissern Sie sich, dass sich alle Knoten in der Hochverfügbarkeitskonfiguration Ihrer Datenbank in einem ordnungsgemäßen Zustand befinden. Weitere Informationen finden Sie im [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).
- Vergewissern Sie sich, dass die VMware Cloud Director-Appliance Zugriff auf `https://vapp-updates.vmware.com` hat.

Verfahren

- 1 Melden Sie sich in einem Webbrowser bei der Appliance-Verwaltungsbenuzoberfläche einer VMware Cloud Director-Appliance-Instanz an, um die primäre Appliance, `https://appliance_ip_address: 5480` zu identifizieren.

Notieren Sie sich den Namen der primären Appliance. Sie müssen beim Sichern der Datenbank den Namen der primären Appliance verwenden.
- 2 Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der primären Appliance als **root** an.

- 3 Setzen Sie das Update-Repository so zurück, dass es auf das VMware Update Repository verweist.

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

- 4 Suchen Sie nach Updates, um sicherzustellen, dass das VMware Update Repository das gewünschte Upgrade aufweist.

Standardmäßig verweist der Befehl `vamicli` auf das VMware Update Repository.

```
vamicli update --check
```

Die Upgrade-Version wird als verfügbares Update angezeigt.

- 5 Fahren Sie VMware Cloud Director herunter, indem Sie den folgenden Befehl ausführen:

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

- 6 Sichern Sie ausgehend von der primären Appliance die eingebettete Datenbank der VMware Cloud Director-Appliance.

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

Hinweis Sie müssen die Appliance nur einmal sichern. Sichern Sie die Appliance nicht, nachdem Sie das verfügbare Upgrade angewendet haben.

- 7 Wenden Sie das verfügbare Upgrade an.

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

- 8 Melden Sie sich bei den verbleibenden Standby- und Anwendungszellen an und wiederholen Sie die Schritte 3, 4, 5 und 7 für jede Appliance.

- 9 Führen Sie von jeder Appliance aus das VMware Cloud Director-Datenbank-upgrade-Dienstprogramm aus.

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

- 10 Starten Sie die VMware Cloud Director-Appliance neu.

```
shutdown -r now
```

Nächste Schritte

- Wenn das Upgrade erfolgreich durchgeführt wurde, können Sie den Snapshot der VMware Cloud Director-Appliance löschen.
- Wenn das Upgrade nicht erfolgreich ist, können Sie die VMware Cloud Director-Appliance auf den Snapshot zurücksetzen, den Sie vor dem Upgrade erstellt haben. Weitere Informationen finden Sie im [Rollback einer VMware Cloud Director-Appliance, wenn ein Upgrade fehlschlägt](#).

- Wenn beim Befehl `vamicli update --install latest` ein Fehler auftritt, finden Sie weitere Informationen unter [Installieren des neuesten Updates von VMware Cloud Director schlägt fehl](#).

Rollback einer VMware Cloud Director-Appliance, wenn ein Upgrade fehlschlägt

Wenn das Upgrade einer VMware Cloud Director-Appliance fehlschlägt, können Sie den vor dem Update erstellten Snapshot der Appliance verwenden und ein Rollback der VMware Cloud Director-Appliance durchführen.

Bevor Sie mit dem Rollback beginnen, notieren Sie sich mithilfe der VMware Cloud Director-Appliance-API die Knoten-IDs der Standby-Knoten im Cluster. Weitere Informationen finden Sie in der *API-Schema-Referenz für VMware Cloud Director-Appliance* unter <http://code.vmware.com>.

- 1 Setzen Sie die primäre VMware Cloud Director-Appliance auf den Snapshot zurück, den Sie vor dem Start des Upgrades erstellt haben.

Lesen Sie mehr über das Wiederherstellen von Snapshots virtueller Maschinen mithilfe der Wiederherstellungsoptionen. Weitere Informationen finden Sie unter [Wiederherstellen von VM-Snapshots durch Zurücksetzen](#) in der *vSphere-Administratorhandbuch für virtuelle Maschinen*.

- 2 Schalten Sie die Zelle der primären VMware Cloud Director-Appliance ein.
- 3 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem jeder Zelle der primären VMware Cloud Director-Appliance an. Sie müssen sich als **root**-Benutzer anmelden.
- 4 Beenden Sie die VMware Cloud Director-Dienste auf allen Appliance-Zellen.

```
service vmware-vcd stop
```

- 5 Verwenden Sie die primäre VMware Cloud Director-Zelle, um die Registrierung der sekundären Knoten im Cluster aufzuheben.
 - a Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem der primären Zelle als **root** an.
 - b Ändern Sie den Benutzer in **postgres**.

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

- c Führen Sie den Befehl aus, um die Registrierung einer Standby-Appliance-Zelle aufzuheben.

Um die Registrierung eines inaktiven Standby-Knotens aufzuheben, müssen Sie die Knoten-ID angeben.

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister --node-id=Knoten-ID  
-f /opt/vmware/vpostgres/current/etc/repmgr.conf
```

- d Wiederholen Sie [5.c](#), um die Registrierung der anderen Standby-Appliance-Zelle aufzuheben.
- 6 Fahren Sie im vSphere Client alle Standby-Appliances herunter und löschen Sie sie.
- a Wechseln Sie im vSphere Client zu den Standby-Appliances.
 - b Klicken Sie mit der rechten Maustaste auf eine Standby-Appliance und klicken Sie auf **Stromversorgung > Gastbetriebssystem herunterfahren**.
 - c Klicken Sie mit der rechten Maustaste auf die Appliance und klicken Sie auf **Von Festplatte löschen**.
 - d Wiederholen Sie [6.a](#) bis [6.c](#) für die andere Standby-Appliance-Zelle.
- 7 Stellen Sie sicher, dass die Tool Suite `repmgr` und die eingebettete PostgreSQL-Datenbank der Zelle der primären VMware Cloud Director-Appliance ordnungsgemäß funktionieren.
- a Ändern Sie den Benutzer in **postgres**.

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

- b Führen Sie den Befehl aus, um den Cluster-Status zu überprüfen.

```
/opt/vmware/vpostgres/current/bin/repmgr cluster show
```

In der Konsolenausgabe werden Informationen zum einzigen Knoten im Cluster angezeigt.

```

      ID | Name      | Role      | Status      | Upstream | Location | Connection
string
-----+-----+-----+-----+-----+-----+-----
+-----+-----+-----+-----+-----+-----+-----
Node 1 | Knotenname | primary |
*running |           | default | host=Host-IP-Adresse user=repmgr dbname=repmgr

```

- 8 Stellen Sie die sekundären Appliances erneut bereit. Weitere Informationen finden Sie im [Bereitstellen der VMware Cloud Director-Appliance unter Verwendung des vSphere Clients](#).
- 9 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem jeder Zelle der primären VMware Cloud Director-Appliance an. Sie müssen sich als **root**-Benutzer anmelden.
- 10 Starten Sie die VMware Cloud Director-Dienste.

```
service vmware-vcd start
```

Migrieren von VMware Cloud Director mit einer externen PostgreSQL-Datenbank auf eine VMware Cloud Director-Appliance

Wenn Ihre aktuelle VMware Cloud Director-Umgebung eine externe PostgreSQL-Datenbank verwendet, können Sie in eine neue VMware Cloud Director-Umgebung migrieren, die aus Bereitstellungen der VMware Cloud Director-Appliance besteht. Ihre aktuelle VMware Cloud Director-Umgebung kann aus VMware Cloud Director-Installationen auf Linux oder aus

Bereitstellungen der VMware Cloud Director-Appliance bestehen. Die neue VMware Cloud Director-Umgebung kann die eingebetteten PostgreSQL-Datenbanken der Appliance in einem Hochverfügbarkeitsmodus verwenden.

Der Migrations-Workflow umfasst vier Hauptphasen.

- Aktualisieren der vorhandenen VMware Cloud Director-Umgebung
- Erstellen der neuen VMware Cloud Director-Servergruppe durch Bereitstellen einer oder mehrerer Instanzen der VMware Cloud Director-Appliance
- Migrieren der externen Datenbank auf die eingebettete Datenbank
- Kopieren der gemeinsam genutzten Übertragungsdienst- und Zertifikatsdaten.

Vorgehensweise

- 1 Wenn die aktuelle externe PostgreSQL-Datenbank Version 9.x aufweist, führen Sie ein Upgrade der externen PostgreSQL-Datenbank auf Version 10 oder höher durch.
- 2 Aktualisieren Sie die aktuelle VMware Cloud Director-Umgebung auf Version 10.2.
Weitere Informationen finden Sie unter [Upgrade von VMware Cloud Director unter Linux](#).
- 3 Vergewissern Sie sich, dass der Neustart von VMware Cloud Director der Migrationsquelle erfolgreich ist.
- 4 Führen Sie in jeder Zelle der aktualisierten VMware Cloud Director-Umgebung den Befehl zum Beenden des VMware Cloud Director-Diensts aus.

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

- 5 Sichern Sie die aktuelle Datenbank in der externen PostgreSQL-Datenbank.

```
sudo -u postgres path_to_pg_dump -Fc db_name > /tmp/db_dump_name
```

Wenn nicht genügend freier Speicherplatz im Ordner `/tmp` vorhanden ist, verwenden Sie einen anderen Speicherort zum Speichern der Speicherabbilddatei.

- 6 Wenn sich der Datenbankbesitzer und der Datenbankname von `vcloud` unterscheiden, notieren Sie sich den Benutzernamen und den Datenbanknamen.

Sie müssen diesen Benutzer in der neuen Umgebung erstellen und die Datenbank in [Schritt 13](#) umbenennen.

- 7 Wenn die neue VMware Cloud Director-Umgebung die IP-Adressen der vorhandenen Umgebung verwenden soll, müssen Sie die Eigenschaften und die Zertifikatsdateien an einen Speicherort in der externen PostgreSQL-Datenbank kopieren und die Zellen ausschalten.
 - a Kopieren Sie die Dateien `global.properties`, `responses.properties`, `certificates`, `proxycertificates` und `truststore`, die sich unter `/opt/vmware/vcloud-director/etc/` befinden, in das Verzeichnis `/tmp` oder in einen beliebigen bevorzugten Speicherort auf der externen PostgreSQL-Datenbank.

- b Schalten Sie die Zellen in der vorhandenen Umgebung aus.
- 8 Wenn die neue VMware Cloud Director-Umgebung den NFS-Server der vorhandenen Umgebung verwenden soll, erstellen Sie ein neues Verzeichnis auf diesem NFS-Server und exportieren Sie es als neuen freigegebenen NFS-Mount-Punkt.

Sie können den vorhandenen Mount-Punkt nicht wieder verwenden, da die Benutzer- und Gruppen-IDs (UID/GID) der Benutzer im alten NFS möglicherweise nicht mit den Benutzer- und Gruppen-IDs im neuen NFS übereinstimmen.

- 9 Erstellen Sie die neue Servergruppe durch Bereitstellen einer oder mehrerer Instanzen der VMware Cloud Director-Appliance.
- Wenn Sie die Hochverfügbarkeitsfunktion der Datenbank verwenden möchten, stellen Sie eine primäre und zwei Standby-Zellen und optional eine oder mehrere vCD-Anwendungszellen bereit.
 - Wenn Sie die Zellen in der vorhandenen Umgebung ausgeschaltet haben, können Sie die ursprünglichen IP-Adressen für die neuen Zellen verwenden.
 - Wenn Sie einen neuen Pfad auf den vorhandenen NFS-Server exportiert haben, können Sie diesen neuen freigegebenen Mount-Punkt für die neue Umgebung verwenden.

Weitere Informationen finden Sie unter [Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance](#).

- 10 Führen Sie in jeder neu bereitgestellten Zelle den Befehl zum Beenden des VMware Cloud Director-Diensts aus.

```
service vmware-vcd stop
```

- 11 Kopieren Sie die Speicherabbilddatei aus dem Ordner `/tmp` in der externen PostgreSQL-Datenbank in den Ordner `/tmp` in der primären Zelle der neuen Umgebung.

Siehe [Schritt 5](#).

- 12 Ändern Sie die Berechtigungen in der Speicherabbilddatei.

```
chmod a+r /tmp/db_dump_name
```

- 13 Melden Sie sich als **root** bei der Konsole der neu bereitgestellten primären Zelle an und übertragen Sie die VMware Cloud Director-Datenbank aus der externen in die eingebettete Datenbank.

- a Ändern Sie den Benutzer in `postgres`, stellen Sie eine Verbindung zum `psql`-Datenbankterminal her und führen Sie die Anweisung aus, um die `vcloud`-Datenbank zu löschen.

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

- b Wenn sich der Datenbankbesitzer der vorhandenen externen Datenbank von `vcloud` unterscheidet, erstellen Sie einen Benutzer mit dem Namen, den Sie in [Schritt 6](#) notiert haben.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'CREATE USER
<db_owner_external_pg>;'
```

- c Führen Sie den Befehl `pg_restore` aus.

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

- d Wenn sich der Datenbankname der vorhandenen externen Datenbank von `vcloud` unterscheidet, ändern Sie ihn in `vcloud`, indem Sie den Namen verwenden, den Sie in [Schritt 6](#) notiert haben.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE
<db_name_external_pg> RENAME TO vcloud;'
```

- e Wenn sich der Datenbankbesitzer der vorhandenen VMware Cloud Director-Umgebung von `vcloud` unterscheidet, ändern Sie den Datenbankbesitzer in `vcloud` und weisen Sie die Tabellen erneut `vcloud` zu.

```
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 Sichern und ersetzen Sie die Konfigurationsdaten in jeder neu bereitgestellten Zelle, konfigurieren Sie den VMware Cloud Director-Dienst neu und starten Sie ihn.
- a Sichern Sie die Eigenschaften, den Truststore und die Zertifikatsdateien, kopieren Sie diese Dateien und ersetzen Sie sie am Speicherort in der externen PostgreSQL-Datenbank der Migrationsquelle, in die Sie die Dateien in [Schritt 7 a](#) kopiert haben.

Die Dateien `global.properties`, `responses.properties`, `truststore`, `certificates` und `proxycertificates` befinden sich unter `/opt/vmware/vcloud-director/etc/`.

- b Sichern Sie die Keystore-Datei, die sich unter `/opt/vmware/vcloud-director/certificates.ks` befindet.

Kopieren und ersetzen Sie sie nicht durch die Keystore-Datei aus der Migrationsquelle.

- c Führen Sie den Befehl aus, um den VMware Cloud Director-Dienst neu zu konfigurieren.

```
/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 --uid --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
```

Dabei gilt:

- Der Wert `--keystore-password` entspricht dem anfänglichen **root**-Kennwort dieser Appliance.
- Der Wert `--database-password` stimmt mit dem Datenbankkennwort überein, das Sie während der Bereitstellung der Appliance festgelegt haben.
- Der Wert `--database-host` stimmt mit der `eth1`-Netzwerk-IP-Adresse der primären Appliance überein.
- Der Wert `--primary-ip` entspricht der `eth0`-Netzwerk-IP-Adresse der Appliance.
- Der Wert `--console-proxy-ip` entspricht der `eth0`-Netzwerk-IP-Adresse der Appliance.
- Der Wert `--console-proxy-port` entspricht dem Proxy-Port 8443 der Appliance-Konsole.

Informationen zur Fehlerbehebung finden Sie unter [Neukonfigurieren des VMware Cloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der VMware Cloud Director-Appliance fehl](#).

- d Führen Sie den Befehl aus, um den VMware Cloud Director-Dienst zu starten.

```
service vmware-vcd start
```

Sie können den Fortschritt des Zellenstarts unter `/opt/vmware/vcloud-director/logs/cell.log` überwachen.

- 15 Ändern Sie die Konfiguration des Lastausgleichsdiensts dahingehend, dass alle IPs der neuen Appliance `eth0` in die Lastausgleichspools für HTTP-, HTTPS- und TCP-Datenverkehr aufgenommen und die alten IPs der Linux-VMware Cloud Director-Zellen aus diesen Pools entfernt werden.
- 16 Nachdem alle Zellen der neuen Servergruppe gestartet wurden, stellen Sie sicher, dass die Migration Ihrer VMware Cloud Director-Umgebung erfolgreich verlaufen ist.
 - a Öffnen Sie das Service Provider Admin Portal mithilfe der `eth0` Netzwerk-IP-Adresse einer beliebigen Zelle aus der neuen Servergruppe, `https://eth0_IP_new_cell/provider`.
 - b Melden Sie sich beim Service Provider Admin Portal mit Ihren vorhandenen Anmeldedaten für **Systemadministratoren** aus der Migrationsquelle an.
 - c Stellen Sie sicher, dass Ihre vSphere- und Cloud-Ressourcen in der neuen Umgebung zur Verfügung stehen.

- 17 Verwenden Sie nach erfolgreicher Überprüfung der VMware Cloud Director-Migration die Service Provider Admin Portal, um die getrennten Zellen zu löschen, die zur alten VMware Cloud Director-Umgebung gehören.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Cloud-Zellen**.
 - c Wählen Sie eine inaktive Zelle aus und klicken Sie auf **Registrierung aufheben**.

Sie können die VMware Cloud Director-Appliance bereitstellen, um Mitglieder zur Servergruppe der migrierten Umgebung hinzuzufügen.

Weitere Schritte

In der neuen Umgebung der migrierten VMware Cloud Director-Appliance werden selbstsignierte Zertifikate verwendet. Zur Verwendung der ordnungsgemäß signierten Zertifikate aus der alten Umgebung in jeder Zelle der neuen Umgebung führen Sie die folgenden Schritte aus:

- 1 Kopieren und ersetzen Sie die Keystore-Datei aus der alten Zelle in `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.
- 2 Führen Sie den Befehl des Zellenverwaltungstools aus, um die Zertifikate zu ersetzen.

Stellen Sie sicher, dass `vcloud.vcloud` der Besitzer dieser Datei ist.

```
/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 Starten Sie den VMware Cloud Director-Dienst neu.

```
service vmware-vcd restart
```

Wenn Sie dieser Servergruppe neue Mitglieder hinzufügen, werden die Zellen der neuen Appliance mit diesen ordnungsgemäß signierten Zertifikaten bereitgestellt.

Nach dem Upgrade von VMware Cloud Director

Nach dem Upgrade aller VMware Cloud Director-Server und der gemeinsam genutzten Datenbank können Sie die NSX Manager-Instanzen aktualisieren, die Netzwerkdienste für Ihre Cloud bereitstellen. Danach können Sie die ESXi-Hosts und die vCenter Server-Instanzen aktualisieren, die bei Ihrer VMware Cloud Director-Installation registriert sind.

Wichtig VMware Cloud Director unterstützt nur erweiterte Edge-Gateways. Sie müssen jedes ältere, nicht erweiterte Edge-Gateway in ein erweitertes Gateway konvertieren. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/66767>.

Ab Version 10.1 können Dienstleister und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Verweigerungsliste interner Hosts, die für Mandanten, die die VMware Cloud Director-API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Verweigerungsliste, nachdem Sie die Installation oder das Upgrade von VMware Cloud Director durchgeführt haben und bevor Sie Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie im [Konfigurieren einer Negativliste für Testverbindungen](#).

Wichtig Nach dem Upgrade auf Version 10.1 und höher überprüft VMware Cloud Director immer die Zertifikate für alle mit ihm verbundenen Infrastruktur-Endpoints. Der Grund hierfür besteht darin, dass die Verwaltung von SSL-Zertifikaten durch VMware Cloud Director geändert wurde. Wenn Sie die Zertifikate vor dem Upgrade nicht in VMware Cloud Director importieren, kommt es in vCenter Server- und NSX-Verbindungen aufgrund von Problemen bei der SSL-Überprüfung möglicherweise zu fehlgeschlagenen Verbindungen. In diesem Fall haben Sie nach dem Upgrade zwei Möglichkeiten:

- 1 Führen Sie den Befehl `trust-infra-certs` des Zellenverwaltungstools aus, um automatisch alle Zertifikate in den zentralisierten Zertifikatspeicher zu importieren. Weitere Informationen finden Sie unter [Importieren von Endpoint-Zertifikaten aus vSphere-Ressourcen](#).
- 2 Wählen Sie in der Service Provider Admin Portal-Benutzeroberfläche jede vCenter Server- und NSX-Instanz aus und geben Sie die Anmeldedaten beim Akzeptieren des Zertifikats erneut ein.

Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist

Bevor Sie ein Upgrade eines vCenter Server- und ESXi-Hosts durchführen, die bei VMware Cloud Director registriert sind, müssen Sie ein Upgrade einer jeden NSX Manager-Instanz durchführen, die mit diesem vCenter Server verbunden ist.

Durch das Durchführen eines Upgrades von NSX Manager wird der Zugriff auf administrative NSX-Funktionen unterbrochen, es werden jedoch keine Netzwerkdienste unterbrochen. Sie können ein Upgrade von NSX Manager durchführen, bevor oder nachdem Sie ein Upgrade von VMware Cloud Director durchgeführt haben. Dies ist unabhängig davon, ob VMware Cloud Director-Zellen ausgeführt werden.

Informationen zum Durchführen eines Upgrades von NSX finden Sie in der NSX for vSphere-Dokumentation unter <https://docs.vmware.com>.

Verfahren

- 1 Führen Sie ein Upgrade des NSX Manager durch, der mit jedem vCenter Server verknüpft ist, der bei der VMware Cloud Director-Installation registriert ist.
- 2 Nach dem Upgrade aller NSX Manager können Sie ein Upgrade der registrierten vCenter Server-Systeme und ESXi-Hosts durchführen.

Upgrade von vCenter Server-Systemen, ESXi-Hosts und NSX Edges

Nach dem Upgrade von VMware Cloud Director und NSX Manager müssen Sie das Upgrade der vCenter Server-Systeme und ESXi-Hosts durchführen, die bei VMware Cloud Director registriert sind. Nach dem Upgrade aller verbundenen vCenter Server-Systeme und ESXi-Hosts können Sie das Upgrade der NSX Edges durchführen.

Voraussetzungen

Stellen Sie sicher, dass Sie bereits ein Upgrade eines jeden NSX Manager durchgeführt haben, der den mit Ihrer Cloud verbundenen vCenter Server-Systemen zugeordnet ist. Weitere Informationen finden Sie unter [Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist](#).

Verfahren

- 1 Deaktivieren Sie die vCenter Server-Instanz.
 - a Wählen Sie in der oberen Navigationsleiste des VMware Cloud Director Service Provider Admin Portal unter **Ressourcen** die Option **vSphere-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **vCenter Server-Instanzen**.
 - c Wählen Sie das Optionsfeld neben der vCenter Server-Instanz aus, die Sie deaktivieren möchten, und klicken Sie auf **Deaktivieren**.
 - d Klicken Sie auf **OK**.
- 2 Führen Sie ein Upgrade des vCenter Server-Systems durch.

Informationen dazu finden Sie unter *Upgrade von vCenter Server*.
- 3 Verifizieren Sie alle öffentlichen VMware Cloud Director-URLs und Zertifikatsketten.
 - a Wählen Sie in der oberen Navigationsleiste **Administration** aus.
 - b Klicken Sie im linken Bereich unter **Einstellungen** auf **Öffentliche Adressen**.
 - c Überprüfen Sie alle öffentlichen Adressen.
- 4 Aktualisieren Sie die Registrierung von vCenter Server bei VMware Cloud Director.
 - a Wählen Sie in der oberen Navigationsleiste des VMware Cloud Director Service Provider Admin Portal unter **Ressourcen** die Option **vSphere-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **vCenter Server-Instanzen**.
 - c Wählen Sie das Optionsfeld neben dem gewünschten vCenter Server und klicken Sie auf **Erneut verbinden**.
 - d Klicken Sie auf **OK**.

- 5 Führen Sie ein Upgrade jedes ESXi-Hosts durch, den das aktualisierte vCenter Server-System unterstützt.

Weitere Informationen finden Sie unter *VMware ESXi-Upgrade*.

Wichtig Um sicherzustellen, dass Sie über ausreichend Hostkapazität zur Unterstützung der virtuellen Maschinen in Ihrer Cloud verfügen, aktualisieren Sie die Hosts jeweils in kleinen Gruppen. Bei diesem Vorgehen kann die Aktualisierung der Hostagenten rechtzeitig abgeschlossen werden, um eine Migration der virtuellen Maschinen zurück zum aktualisierten Host zu ermöglichen.

- a Verwenden Sie das vCenter Server-System, um den Host in den Wartungsmodus zu versetzen und zu ermöglichen, dass alle virtuellen Maschinen auf diesem Host auf einen anderen Host migriert werden.
 - b Aktualisieren Sie den Host.
 - c Verwenden Sie das vCenter Server-System, um die Verbindung zum Host wiederherzustellen.
 - d Verwenden Sie das vCenter Server-System, um den Wartungsmodus für den Host zu beenden.
- 6 (Optional) Führen Sie ein Upgrade der NSX Edges durch, die vom vCenter Server Manager verwaltet werden, der mit dem aktualisierten NSX-System verbunden ist.

Aktualisierte NSX Edges bieten bessere Leistung und Integration. Sie können entweder NSX Manager oder VMware Cloud Director für das Upgrade von NSX Edges verwenden.

- Informationen zur Verwendung von NSX Manager für das Upgrade von NSX Edges finden Sie in der NSX für vSphere-Dokumentation unter <https://docs.vmware.com/de/>.
- Um VMware Cloud Director für das Upgrade eines NSX-Edge-Gateways zu verwenden, müssen Sie das durch das Edge unterstützte VMware Cloud Director-Netzwerkobjekt verwenden:
 - Ein entsprechendes Upgrade eines Edge-Gateways findet automatisch statt, wenn Sie entweder VMware Cloud Director oder die VMware Cloud Director-API zum Zurücksetzen eines vom Edge-Gateway unterstützten Netzwerks verwenden.
 - Durch das erneute Bereitstellen eines Edge-Gateways wird ein Upgrade der zugeordneten NSX Edge-Appliance durchgeführt.

Hinweis Die erneute Bereitstellung wird nur für NSX Data Center for vSphere-Edge-Gateways unterstützt.

- Durch das Zurücksetzen eines vApp-Netzwerks von innerhalb des Kontexts der vApp wird ein Upgrade der diesem Netzwerk zugeordneten NSX Edge-Appliance durchgeführt. Um ein vApp-Netzwerk innerhalb des Kontexts einer vApp zurückzusetzen, navigieren Sie zur Registerkarte **Netzwerke** für die vApp, zeigen Sie die Netzwerkdetails an, klicken Sie auf das Optionsfeld neben dem Namen des vApp-Netzwerks und klicken Sie auf **Zurücksetzen**.

Weitere Informationen zum erneuten Bereitstellen von Edge-Gateways und zum Zurücksetzen von vApp-Netzwerken finden Sie im *VMware Cloud Director API-Programmierhandbuch*.

Nächste Schritte

Wiederholen Sie diesen Vorgang für die anderen vCenter Server-Systeme, die bei Ihrer VMware Cloud Director-Installation registriert sind.

Verwaltung der VMware Cloud Director-Appliance

Sie können den Status der Zellen in einem HA-Datenbank-Cluster anzeigen, die eingebettete Datenbank sichern und wiederherstellen und die Appliance-Einstellungen neu konfigurieren.

Nachdem Sie die VMware Cloud Director-Appliance bereitgestellt haben, können Sie die IP-Adressen des `eth0`- und des `eth1`-Netzwerks oder den Hostnamen der Appliance nicht ändern. Wenn Sie für die VMware Cloud Director-Appliance andere Adressen oder einen anderen Hostnamen verwenden möchten, müssen Sie eine neue Appliance bereitstellen.

Wenn Sie die Wartung einer Appliance durchführen müssen, die das Herunterfahren des Hochverfügbarkeits-Clusters der Datenbank erfordert, müssen Sie zuerst die primäre Appliance und dann die Standby-Appliances herunterfahren, um Synchronisierungsprobleme zu vermeiden.

Hinweis Wenn Ihr Cluster für automatisches Failover konfiguriert ist, müssen Sie nach der Bereitstellung einer zusätzlichen oder mehrerer zusätzlicher Zellen die Appliance-API verwenden, um den Failover-Modus auf `Automatic` zurückzusetzen. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API](#). Der standardmäßige Failover-Modus für neue Zellen lautet `Manual`. Wenn der Failover-Modus für die Knoten des Clusters inkonsistent ist, lautet der Failover-Modus des Clusters `Indeterminate`. Der Modus `Indeterminate` kann zwischen den Knoten und den einer alten primären Zelle folgenden Knoten zu inkonsistenten Clusterzuständen führen. Informationen zum Anzeigen des Failover-Modus des Clusters finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

Sichern und Wiederherstellen der eingebetteten Datenbank der VMware Cloud Director-Appliance

Sie können die eingebettete PostgreSQL-Datenbank der VMware Cloud Director-Appliance sichern, mit deren Hilfe Sie die VMware Cloud Director-Umgebung nach einem Ausfall wiederherstellen können.

Sichern der eingebetteten Datenbank der VMware Cloud Director-Appliance

Wenn Ihre Umgebung aus Bereitstellungen der VMware Cloud Director-Appliance mit eingebetteten PostgreSQL-Datenbanken besteht, können Sie die VMware Cloud Director-Datenbank über die primäre Zelle sichern. Die resultierende `.tgz`-Datei wird im gemeinsam genutzten NFS-Übertragungsdienstspeicher gespeichert.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der primären Zelle als **root** an.
- 2 Sichern Sie die eingebettete Datenbank der VMware Cloud Director-Appliance, indem Sie den folgenden Befehl ausführen.

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

Ergebnisse

Im gemeinsam genutzten NFS-Übertragungsdienstspeicher wird im Verzeichnis `vcloudapp.nfs_mount.VMware_vCloud_Director/pgdb-backup/` die neu erstellte Datei `db-backup-date_time_format.tgz` angezeigt. Die `.tgz`-Datei enthält die Speicherabbilddatei der Datenbank sowie die Dateien `global.properties`, `responses.properties`, `certificates`, `proxycertificates` und `truststore` der primären Zelle.

Wiederherstellen einer VMware Cloud Director-Appliance 10.2.1- und früheren Umgebung mit einer High Availability-Datenbankkonfiguration

Wenn Sie die eingebettete PostgreSQL-Datenbank einer VMware Cloud Director-Appliance 10.2.1- und früheren Umgebung mit einer HA-Datenbankkonfiguration gesichert haben, können Sie einen neuen Appliance-Cluster bereitstellen und die darin enthaltene Appliance-Datenbank wiederherstellen.

Der Wiederherstellungs-Workflow umfasst drei Hauptphasen.

- Kopieren der eingebetteten Datenbanksicherungsdatei `.tar` aus dem freigegebenen NFS-Speicher des Übertragungsdiensts
- Wiederherstellen der Datenbank auf die primären und Standby-Zellen der eingebetteten Datenbank
- Bereitstellen aller erforderlichen Anwendungszellen

Voraussetzungen

- Stellen Sie sicher, dass Sie über eine Sicherungsdatei vom Typ `.tar` der eingebetteten PostgreSQL-Datenbank verfügen. Weitere Informationen finden Sie unter [Sichern der eingebetteten Datenbank der VMware Cloud Director-Appliance](#).
- Stellen Sie eine primäre und zwei Standby-Datenbankzellen bereit. Weitere Informationen finden Sie im [Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance](#).

- Wenn der neue Appliance-Cluster den NFS-Server der vorhandenen Umgebung verwenden soll, erstellen Sie ein neues Verzeichnis auf dem NFS-Server und exportieren Sie es als neue Freigabe. Der vorhandene Mount-Punkt kann nicht erneut verwendet werden.

Vorgehensweise

- 1 Melden Sie sich bei den primären und Standby-Zellen als **root** an und führen Sie den Befehl aus, um den VMware Cloud Director-Dienst zu beenden.

```
service vmware-vcd stop
```

- 2 Kopieren Sie in den primären und Standby-Zellen die `.tar`-Sicherungsdatei in den Ordner `/tmp`.

Wenn nicht genügend freier Speicherplatz im Ordner `/tmp` vorhanden ist, verwenden Sie einen anderen Speicherort zum Speichern der Datei vom Typ `.tar`.

- 3 Entpacken Sie in den primären und Standby-Zellen die Sicherungsdatei unter `/tmp`.

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

Im Ordner `/tmp` werden die extrahierten Dateien `global.properties`, `responses.properties`, `certificates`, `proxycertificates`, `truststore` sowie die Speicherabbilddatei der Datenbank mit der Bezeichnung `vcloud_date_time_format` angezeigt.

Hinweis Die Datei `truststore` steht nur für VMware Cloud Director Version 9.7.0.1 bis 10.2.1 zur Verfügung.

- 4 Melden Sie sich ausschließlich in der primären Zelle als **root** bei der Konsole an und führen Sie die folgenden Befehle aus.
 - a Löschen Sie die `vcloud`-Datenbank.

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

- b Führen Sie den Befehl `pg_restore` aus.

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

- 5 Speichern Sie in den primären und Standby-Zellen eine Kopie der Konfigurationsdatendateien und ersetzen Sie sie. Konfigurieren Sie den VMware Cloud Director-Dienst anschließend neu und starten Sie ihn.
 - a Sichern Sie die Eigenschaften, Zertifikate und Truststore-Dateien.

Die Dateien `global.properties`, `responses.properties`, `certificates`, `proxycertificates` und `truststore` befinden sich unter `/opt/vmware/vcloud-director/etc/`.

Hinweis Die Datei `truststore` steht nur für VMware Cloud Director Version 9.7.0.1 bis 10.2.1 zur Verfügung.

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

- b Kopieren und ersetzen Sie die Eigenschaften, Zertifikate und Truststore-Dateien anhand der Sicherungsdateien, die Sie in [Schritt 3](#) extrahiert haben.

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

Hinweis Die Datei `truststore` steht nur für VMware Cloud Director Version 9.7.0.1 bis 10.2.1 zur Verfügung.

- c Sichern Sie die Keystore-Datei, die sich unter `/opt/vmware/vcloud-director/certificates.ks` befindet.

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

- d Führen Sie die folgenden Befehle aus, um den VMware Cloud Director-Dienst neu zu konfigurieren.

```
/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
```

Dabei gilt:

- Die Option `--keystore-password` stimmt mit dem Keystore-Kennwort für die Zertifikate in der Appliance überein. Beim Keystore-Kennwort handelt es sich unter Umständen um das **root**-Kennwort, das Sie während der Bereitstellung der Appliance verwendet haben.

- Die Option `--database-password` stimmt mit dem Datenbankkennwort überein, das Sie während der Einrichtung der Appliance in der Verwaltungsbenutzeroberfläche der VMware Cloud Director-Appliance unter `https://appliance_eth0_ip:5480` festgelegt haben.
- Die Option `--database-host` entspricht der `eth1`-Netzwerk-IP-Adresse der primären Datenbank-Appliance.
- Der Wert `--primary-ip` entspricht der `eth0`-Netzwerk-IP-Adresse der wiederherzustellenden Appliance-Zelle. Hierbei handelt es sich nicht um die IP-Adresse der primären Datenbankzelle.
- Die Option `--console-proxy-ip` entspricht der `eth0`-Netzwerk-IP-Adresse der wiederherzustellenden Appliance.

Informationen zur Fehlerbehebung finden Sie unter [Neukonfigurieren des VMware Cloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der VMware Cloud Director-Appliance fehl](#).

- e Führen Sie den Befehl aus, um den VMware Cloud Director-Dienst zu starten.

```
service vmware-vcd start
```

Sie können den Fortschritt des Zellenstarts unter `/opt/vmware/vcloud-director/logs/cell.log` überwachen.

- 6 (Optional) Stellen Sie gegebenenfalls zusätzliche Anwendungszellen bereit. Weitere Informationen finden Sie im [Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance](#).
- 7 Wenn die neuen Appliances andere IPs als die ursprünglichen von Ihnen zu ersetzenden Appliances verwenden, müssen Sie die Konfiguration des Lastausgleichsdiensts aktualisieren, der der VMware Cloud Director-Servergruppe vorangestellt ist, um die IPs der neuen Appliances aufzunehmen.
- 8 Nachdem alle Zellen der Servergruppe gestartet wurden, stellen Sie sicher, dass die Wiederherstellung Ihrer VMware Cloud Director-Umgebung erfolgreich verlaufen ist.
 - a Öffnen Sie das VMware Cloud Director Service Provider Admin Portal mithilfe der `eth0`-Netzwerk-IP-Adresse einer beliebigen Zelle aus der neuen Servergruppe, `https://eth0_IP_new_cell/provider`.

Wenn Sie die Konfiguration des Lastausgleichsdiensts in Schritt 7 aktualisiert haben, müssen Sie die öffentliche Adresse der Servergruppe verwenden, um auf das Service Provider Admin Portal zuzugreifen.
 - b Melden Sie sich beim Service Provider Admin Portal mit den vorhandenen Anmeldedaten für **Systemadministratoren** an.
 - c Stellen Sie sicher, dass Ihre vSphere- und Cloud-Ressourcen in der neuen Umgebung zur Verfügung stehen.

- 9 Verwenden Sie nach erfolgreicher Überprüfung der Datenbankwiederherstellung die Service Provider Admin Portal, um die getrennten Zellen zu löschen, die zur alten VMware Cloud Director-Umgebung gehören.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Cloud-Zellen**.
 - c Wählen Sie eine inaktive Zelle aus und klicken Sie auf **Registrierung aufheben**.
- 10 Wenn der Failover-Modus vor der Wiederherstellung `Automatic` war, müssen Sie ihn mithilfe der VMware Cloud Director-Appliance-API erneut auf `Automatic` festlegen.

Wiederherstellen einer VMware Cloud Director-Appliance 10.2.2- und höheren Umgebung mit einer High Availability-Datenbankkonfiguration

Wenn Sie die eingebettete PostgreSQL-Datenbank einer VMware Cloud Director-Appliance 10.2.2- und höheren Umgebung mit einer High Availability-Datenbankkonfiguration gesichert haben, können Sie einen neuen Appliance-Cluster bereitstellen und die darin enthaltene Appliance-Datenbank wiederherstellen.

Der Wiederherstellungs-Workflow umfasst drei Hauptphasen.

- Kopieren der eingebetteten Datenbanksicherungsdatei `.tar` aus dem freigegebenen NFS-Speicher des Übertragungsdiensts
- Wiederherstellen der Datenbank auf die primären und Standby-Zellen der eingebetteten Datenbank
- Bereitstellen aller erforderlichen Anwendungszellen

Voraussetzungen

- Stellen Sie sicher, dass Sie über eine Sicherungsdatei vom Typ `.tar` der eingebetteten PostgreSQL-Datenbank verfügen. Weitere Informationen finden Sie unter [Sichern der eingebetteten Datenbank der VMware Cloud Director-Appliance](#).
- Stellen Sie eine primäre und zwei Standby-Datenbankzellen bereit. Weitere Informationen finden Sie im [Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance](#).
- Wenn der neue Appliance-Cluster den NFS-Server der vorhandenen Umgebung verwenden soll, erstellen Sie ein neues Verzeichnis auf dem NFS-Server und exportieren Sie es als neue Freigabe. Der vorhandene Mount-Punkt kann nicht erneut verwendet werden.

Vorgehensweise

- 1 Melden Sie sich bei den primären und Standby-Zellen als **root** an und führen Sie den Befehl aus, um den VMware Cloud Director-Dienst zu beenden.

```
service vmware-vcd stop
```

- 2 Kopieren Sie in den primären und Standby-Zellen die `.tar`-Sicherungsdatei in den Ordner `/tmp`.

Wenn nicht genügend freier Speicherplatz im Ordner `/tmp` vorhanden ist, verwenden Sie einen anderen Speicherort zum Speichern der Datei vom Typ `.tar`.

- 3 Entpacken Sie in den primären und Standby-Zellen die Sicherungsdatei unter `/tmp`.

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

Im Ordner `/tmp` werden die extrahierten Dateien `global.properties`, `responses.properties`, `certificates.pem`, `certificates.key`, `proxycertificates.pem`, `proxycertificates.key`, `truststore.pem` sowie die Speicherabbilddatei der Datenbank mit der Bezeichnung `vcloud_date_time_format` angezeigt.

Hinweis Die Datei `truststore.pem` steht nur für VMware Cloud Director 10.2.2 und höher zur Verfügung.

- 4 Melden Sie sich ausschließlich in der primären Zelle als **root** bei der Konsole an und führen Sie die folgenden Befehle aus.
 - a Löschen Sie die `vcloud`-Datenbank.

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

- b Führen Sie den Befehl `pg_restore` aus.

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

- 5 Speichern Sie in den primären und Standby-Zellen eine Kopie der Konfigurationsdatendateien und ersetzen Sie sie. Konfigurieren Sie den VMware Cloud Director-Dienst anschließend neu und starten Sie ihn.
 - a Sichern Sie die Eigenschaften, Zertifikate und Truststore-Dateien.

Die Dateien `global.properties`, `responses.properties`, `certificates.pem`, `certificates.key`, `proxycertificates.pem`, `proxycertificates.key` und `truststore.pem` befinden sich unter `/opt/vmware/vcloud-director/etc/`.

Hinweis Die Datei `truststore.pem` steht nur für VMware Cloud Director 10.2.2 und höher zur Verfügung.

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

- b Kopieren und ersetzen Sie die Eigenschaften, Zertifikate und Truststore-Dateien anhand der Sicherungsdateien, die Sie in [Schritt 3](#) extrahiert haben.

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

Hinweis Die Datei `truststore.pem` steht nur für VMware Cloud Director 10.2.2 und höher zur Verfügung.

- c Sichern Sie die Keystore-Datei, die sich unter `/opt/vmware/vcloud-director/certificates.ks` befindet.

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

- d Führen Sie die folgenden Befehle aus, um den VMware Cloud Director-Dienst neu zu konfigurieren.

```
/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
```

Dabei gilt:

- Die Option `--keystore-password` stimmt mit dem Keystore-Kennwort für die Zertifikate in der Appliance überein. Beim Keystore-Kennwort handelt es sich unter Umständen um das **root**-Kennwort, das Sie während der Bereitstellung der Appliance verwendet haben.
- Die Option `--database-password` stimmt mit dem Datenbankkennwort überein, das Sie während der Einrichtung der Appliance in der Verwaltungsbenuzoberfläche der VMware Cloud Director-Appliance unter `https://appliance_eth0_ip:5480` festgelegt haben.
- Die Option `--database-host` entspricht der `eth1`-Netzwerk-IP-Adresse der primären Datenbank-Appliance.
- Der Wert `--primary-ip` entspricht der `eth0`-Netzwerk-IP-Adresse der wiederherzustellenden Appliance-Zelle. Hierbei handelt es sich nicht um die IP-Adresse der primären Datenbankzelle.

- Die Option `--console-proxy-ip` entspricht der `eth0`-Netzwerk-IP-Adresse der wiederherzustellenden Appliance.

Informationen zur Fehlerbehebung finden Sie unter [Neukonfigurieren des VMware Cloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der VMware Cloud Director-Appliance fehl](#).

- e Führen Sie den Befehl aus, um den VMware Cloud Director-Dienst zu starten.

```
service vmware-vcd start
```

Sie können den Fortschritt des Zellenstarts unter `/opt/vmware/vcloud-director/logs/cell.log` überwachen.

- 6 (Optional) Stellen Sie gegebenenfalls zusätzliche Anwendungszellen bereit. Weitere Informationen finden Sie im [Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance](#).
- 7 Wenn die neuen Appliances andere IPs als die ursprünglichen von Ihnen zu ersetzenden Appliances verwenden, müssen Sie die Konfiguration des Lastausgleichsdiensts aktualisieren, der der VMware Cloud Director-Servergruppe vorangestellt ist, um die IPs der neuen Appliances aufzunehmen.
- 8 Nachdem alle Zellen der Servergruppe gestartet wurden, stellen Sie sicher, dass die Wiederherstellung Ihrer VMware Cloud Director-Umgebung erfolgreich verlaufen ist.
 - a Öffnen Sie das VMware Cloud Director Service Provider Admin Portal mithilfe der `eth0`-Netzwerk-IP-Adresse einer beliebigen Zelle aus der neuen Servergruppe, `https://eth0_IP_new_cell/provider`.

Wenn Sie die Konfiguration des Lastausgleichsdiensts in Schritt 7 aktualisiert haben, müssen Sie die öffentliche Adresse der Servergruppe verwenden, um auf das Service Provider Admin Portal zuzugreifen.
 - b Melden Sie sich beim Service Provider Admin Portal mit den vorhandenen Anmeldedaten für **Systemadministratoren** an.
 - c Stellen Sie sicher, dass Ihre vSphere- und Cloud-Ressourcen in der neuen Umgebung zur Verfügung stehen.
- 9 Verwenden Sie nach erfolgreicher Überprüfung der Datenbankwiederherstellung die Service Provider Admin Portal, um die getrennten Zellen zu löschen, die zur alten VMware Cloud Director-Umgebung gehören.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Cloud-Zellen**.
 - c Wählen Sie eine inaktive Zelle aus und klicken Sie auf **Registrierung aufheben**.
- 10 Wenn der Failover-Modus vor der Wiederherstellung `Automatic` war, müssen Sie ihn mithilfe der VMware Cloud Director-Appliance-API erneut auf `Automatic` festlegen.

- 11 Wenn der FIPS-Modus der VMware Cloud Director-Appliance vor der Wiederherstellung aktiviert war, müssen Sie ihn mithilfe der API der VMware Cloud Director-Appliance erneut festlegen.

Der FIPS-Modus der Zelle wird automatisch wiederhergestellt.

Ändern des Failover-Modus der VMware Cloud Director-Appliance

Standardmäßig befindet sich die VMware Cloud Director-Appliance im manuellen Failover-Modus, und wenn der primäre Datenbankdienst ausfällt, müssen Sie die Failover-Aktion initiieren. Sie können den Failover-Modus mithilfe der Appliance-API in „Automatisch“ ändern.

Ab VMware Cloud Director 10.1 können Sie bei Ausfall des primären Datenbankdiensts VMware Cloud Director aktivieren, um ein automatisches Failover auf eine neue primäre Zelle durchzuführen. Weitere Informationen finden Sie im [Automatisches Failover der VMware Cloud Director-Appliance](#).

Der Failover-Modus wird mithilfe der VMware Cloud Director-Appliance-API auf `automatic` oder `manual` festgelegt. Weitere Informationen hierzu finden Sie im Abschnitt *Failovermode* in der [Schemareferenz für die VMware Cloud Director-Appliance-API](#).

Bei Clustern, die mit automatischem Failover konfiguriert sind, müssen Sie nach der Bereitstellung einer oder mehrerer zusätzlicher Zellen den Failover-Modus des Clusters unter Verwendung der Appliance-API auf `automatic` zurücksetzen. Wenn Sie den Failover-Modus des Clusters nicht zurücksetzen, wird der Failover-Modus über die Knoten hinweg inkonsistent.

Konfigurieren des externen Zugriffs auf die VMware Cloud Director-Datenbank

Sie können den Zugriff von bestimmten externen IP-Adressen auf die VMware Cloud Director-Datenbank aktivieren, die in der primären-Appliance eingebettet ist.

Während einer Migration auf die VMware Cloud Director-Appliance oder wenn Sie die Datenbanksicherungslösung eines Drittanbieters verwenden möchten, können Sie den externen Zugriff auf die eingebettete VMware Cloud Director-Datenbank aktivieren.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der primären Zelle als **root** an.
- 2 Navigieren Sie zum Datenbankverzeichnis `/opt/vmware/appliance/etc/pg_hba.d/`.
- 3 Erstellen Sie eine Textdatei mit Einträgen für die externen Ziel-IP-Adressen ähnlich den folgenden:

```
#TYPE DATABASE USER ADDRESS METHOD
host vcloud vcloud CIDR_notation md5
```

Beispiel:

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

Ihre Einträge werden an die dynamisch aktualisierte Datei `pg_hba.conf` angehängt, die den Zugriff auf die primäre Datenbank im HA-Cluster steuert.

Aktivieren oder Deaktivieren des SSH-Zugriffs auf die VMware Cloud Director-Appliance

Während der Bereitstellung der Appliance können Sie den SSH-Zugriff auf die Appliance deaktiviert lassen oder aktivieren. Nach der Bereitstellung können Sie die SSH-Zugriffseinstellung ändern.

Der SSH-Daemon wird in der Appliance zur Verwendung durch die Datenbank-HA-Funktion und für Remote-**root**-Anmeldungen ausgeführt. Sie können den SSH-Zugriff für den **root**-Benutzer deaktivieren. Der SSH-Zugriff für die Datenbank-HA-Funktion bleibt unverändert.

Voraussetzungen

Um dauerhafte Änderungen an den OVF-Eigenschaften vorzunehmen, müssen Sie die vSphere-Benutzeroberfläche zum Ändern der Werte der OVF-Eigenschaft verwenden. Weitere Informationen finden Sie im Thema „Konfigurieren von vApp-Eigenschaften“ im Handbuch *Verwaltung virtueller vSphere-Maschinen*.

Verfahren

- 1 Wenn Sie zu Testzwecken vorübergehende Änderungen an der OVF-Eigenschaft vornehmen möchten, ändern Sie die Eigenschaft in VMware Cloud Director.
 - a Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der VMware Cloud Director-Appliance als **root** an.
 - b Führen Sie das Skript zum Aktivieren oder Deaktivieren des SSH-**root**-Zugriffs aus.
 - Um den SSH-**root**-Zugriff zu aktivieren, führen Sie das Skript `/opt/vmware/appliance/bin/enable_root_login.sh` aus.
 - Um den SSH-**root**-Zugriff zu deaktivieren, führen Sie das Skript `/opt/vmware/appliance/bin/disable_root_login.sh` aus.
- 2 Wenn Sie dauerhafte Änderungen an der OVF-Eigenschaft vornehmen möchten, verwenden Sie die vSphere-Benutzeroberfläche zum Festlegen des Werts der Eigenschaft `vcloudapp.enable_ssh.VMware_vCloud_Director`.

Hinweis Sie müssen die VM ausschalten, um den Wert der Eigenschaft in vSphere zu ändern.

- Zum Aktivieren von SSH setzen Sie den Wert von `vcloudapp.enable_ssh.VMware_vCloud_Director` auf **True**.

- Zum Deaktivieren von SSH setzen Sie den Wert von `vcloudapp.enable_ssh.VMware_vCloud_Director` auf **False**.

Aktivieren oder Deaktivieren des FIPS-Modus auf der VMware Cloud Director-Appliance

Ab Version 10.2.2 können Sie die VMware Cloud Director-Appliance so konfigurieren, dass FIPS 140-2-validierte kryptografische Module verwendet und im FIPS-konformen Modus ausgeführt werden.

FIPS 140-2 (Federal Information Processing Standard) ist ein US- und kanadischer Behördenstandard, der Sicherheitsanforderungen für kryptografische Module spezifiziert. Das NIST Cryptographic Module Validation Program (CMVP) überprüft die kryptografischen Module, die mit den FIPS 140-2-Standards konform sind.

Mit VMware Cloud Director FIPS-Unterstützung sollen Konformitäts- und Sicherheitsaktivitäten in verschiedenen regulierten Umgebungen erleichtert werden. Weitere Informationen über die Unterstützung für FIPS 140-2 in VMware-Produkten finden Sie unter <https://www.vmware.com/security/certifications/fips.html>.

In VMware Cloud Director ist FIPS-validierte Kryptografie standardmäßig deaktiviert. Durch Aktivierung des FIPS-Modus konfigurieren Sie die VMware Cloud Director-Appliance so, dass FIPS 140-2-validierte kryptografische Module verwendet und im FIPS-konformen Modus ausgeführt werden.

Hinweis Durch Aktivierung des FIPS-Modus wird auch Reverse-Lookup von Hostnamen aktiviert.

Wichtig Wenn Sie den FIPS-Modus aktivieren, funktioniert die Integration in vRealize Orchestrator nicht.

In VMware Cloud Director 10.2.2 können Sie SAML-Assertionen nicht verschlüsseln, wenn der FIPS-Modus aktiviert ist. Wenn der FIPS-Modus nicht verwendet wird, liegen keine Beschränkungen bei der Assertion-Verschlüsselung vor.

VMware Cloud Director verwendet die folgenden FIPS 140-2-validierten kryptografischen Module:

- VMware BC-FJA (Bouncy Castle FIPS Java API) Version 1.0.2.1: [Zertifikat #3673](#)
- VMware OpenSSL FIPS Object Module Version 2.0.20-vmw: [Zertifikat #3857](#)

VMware Cloud Director befindet sich in einem Paket mit dem Zellenverwaltungstool (CMT). Das Zellenverwaltungstool ist jedoch nicht FIPS-konform.

Bei Verwendung der VMware Cloud Director-Appliance müssen Sie sowohl den FIPS-Modus der Appliance als auch den FIPS-Modus der Zelle verwalten, um die Appliance im FIPS-konformen Modus auszuführen.

- Beim FIPS-Modus der Appliance handelt es sich um den Modus des zugrunde liegenden Betriebssystems, der eingebetteten Datenbank und verschiedener Systembibliotheken.

- Beim FIPS-Modus der Zelle handelt es sich um den Modus der VMware Cloud Director-Zelle, die auf jeder Appliance ausgeführt wird.

Informationen zum Aktivieren und Deaktivieren des FIPS-Modus auf VMware Cloud Director unter Linux finden Sie unter [Aktivieren des FIPS-Modus für die Zellen in der Servergruppe](#).

Voraussetzungen

- Wenn die Metrikerfassung aktiviert ist, stellen Sie sicher, dass die Cassandra-Zertifikate dem X.509 v3-Zertifikatstandard entsprechen und alle erforderlichen Erweiterungen enthalten. Sie müssen Cassandra mit denselben Verschlüsselungssammlungen konfigurieren, die von VMware Cloud Director verwendet werden. Informationen zu den zulässigen SSL-Verschlüsselungen finden Sie unter [Verwalten der Liste der zulässigen SSL-Verschlüsselungen](#).
- Heben Sie die Registrierung von VMware Cloud Director beim vCenter Lookup Service auf. Informationen hierzu finden Sie unter [Konfigurieren der vSphere-Dienste](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste des Service Provider Admin Portal **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Einstellungen** auf **SSL**.
- 3 Klicken Sie auf **Aktivieren**.
- 4 Um zu bestätigen, dass Sie den Vorgang starten möchten, klicken Sie auf **Aktivieren**.

Nach Abschluss der Konfiguration zeigt VMware Cloud Director eine Meldung vom Typ `Aktivieren läuft (Auf Neustart der Zellen wird gewartet)` an, und Sie können mit Schritt 5 fortfahren. Wenn Sie den API-Befehl in Schritt 5 ausführen, startet VMware Cloud Director-Appliance die Zellen automatisch neu.

- 5 Um den FIPS-Modus der Appliance zu aktivieren oder zu deaktivieren, verwenden Sie die API der VMware Cloud Director-Appliance, um eine `PUT`-Anforderung an die `fips/{node_name}`-URL zu senden. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API](#).

Hinweis Sie müssen den `{node_name}` der Maschine verwenden, die die `PUT`-Anforderung verarbeitet.

Beispiel: Aktivieren des FIPS-Modus

Anfrage:

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

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

- 6 Wiederholen Sie Schritt 5 für jede Appliance, wie z. B. primäre Appliance, Standby-Appliance und Anwendungstypen.

Nächste Schritte

Um den Status der Zellen zu bestätigen, können Sie die Verwaltungsbenutzeroberfläche der VMware Cloud Director-Appliance verwenden. Weitere Informationen finden Sie im [Anzeigen des FIPS-Modus der VMware Cloud Director-Appliance](#).

Anzeigen des FIPS-Modus der VMware Cloud Director-Appliance

Ab Version 10.2.2 kann die VMware Cloud Director-Appliance im FIPS-konformen Modus ausgeführt werden. Sie können den FIPS-Modus der Appliance und der Zelle anzeigen.

Bei Verwendung der VMware Cloud Director-Appliance müssen Sie sowohl den FIPS-Modus der Appliance als auch den FIPS-Modus der Zelle verwalten, um die VMware Cloud Director-Appliance im FIPS-konformen Modus auszuführen.

- Beim FIPS-Modus der Appliance handelt es sich um den Modus des zugrunde liegenden Betriebssystems, der eingebetteten Datenbank und verschiedener Systembibliotheken.
- Beim FIPS-Modus der Zelle handelt es sich um den Modus der VMware Cloud Director-Zelle, die auf jeder Appliance ausgeführt wird.

Tabelle 3-1. Status des FIPS-Modus

Gesundheit	Beschreibung
	Die FIPS-Modi der Appliance und Zelle sind identisch. Beide Modi sind entweder ein- oder ausgeschaltet.
	Der FIPS-Modus der Zelle befindet sich im Status <i>Ausstehender Neustart</i> . Verwenden Sie die Appliance-API, um den FIPS-Modus der Appliance zu aktivieren oder zu deaktivieren. Durch Ändern des FIPS-Modus der Appliance wird der Dienst der VMware Cloud Director-Zelle automatisch neu gestartet.
	Die VMware Cloud Director-Appliance kann den FIPS-Modus der Zelle nicht bestimmen. Wenn der VMware Cloud Director-Dienst auf der Appliance fehlschlägt, kann der FIPS-Modus der Zelle nicht bestimmt werden.

Voraussetzungen

[Aktivieren oder Deaktivieren des FIPS-Modus auf der VMware Cloud Director-Appliance](#)

Verfahren

- 1 Melden Sie sich als **root** bei der Verwaltungsschnittstelle der Appliance unter `https://primary_eth1_ip_address:5480` an.
- 2 Wählen Sie **Systemkonfiguration** im linken Fensterbereich aus.
- 3 Zeigen Sie den Status des FIPS-Modus der Appliance und der Zelle auf jedem Knoten an.

Konfigurieren des SNMP-Agenten der VMware Cloud Director-Appliance

Ab VMware Cloud Director 10.2.2 können Sie den SNMP-Agenten der VMware Cloud Director-Appliance zur Überwachung von Abfrageanforderungen konfigurieren.

SNMP (Simple Network Management Protocol) ist ein Anwendungsschichtprotokoll für die Verwaltung und Überwachung von Netzwerkelementen. Die VMware Cloud Director-Appliance enthält einen SNMP-Agenten, der `GET`-, `GETBULK`- und `GETNEXT`-Anforderungen empfangen und auf diese reagieren kann. Der SNMP-Agent der VMware Cloud Director-Appliance ist mit allen SNMP-Verwaltungsdiensten kompatibel, die mit den SNMP-Standards konform sind. Sie können den Agenten für SNMP v1, v2c oder v3 konfigurieren. Allerdings bietet nur SNMP v3 verbesserte Sicherheit, einschließlich kryptografischer Authentifizierung und Verschlüsselung.

Wenn ein Net-SNMP-Agent vorhanden ist, beachten Sie vor der Konfiguration Folgendes:

- Während des Upgrades auf Version 10.2.2 oder höher löscht und ersetzt VMware Cloud Director Net-SNMP durch VMware-SNMP.
- Sie müssen alle vorhandenen Firewallregeln entfernen, die mit Net-SNMP zusammenarbeiten, da VMware-SNMP den Abrufport beim Starten und Beenden des `snmpd`-Dienstes aktiviert und deaktiviert.

VMware-SNMP für die VMware Cloud Director-Appliance bietet Unterstützung für standardmäßige Linux OS-MIBs (Management Information Bases), die über die folgenden branchenüblichen MIBs verfügen.

- 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

Konfigurieren eines benutzerdefinierten Ports für den SNMP-Agenten

Wenn Sie ab VMware Cloud Director 10.2.2 den VMware Cloud Director-SNMP-Agenten zum Abfragen konfigurieren, kann er Anforderungen von Clientsystemen für die SNMP-Verwaltung, wie z. B. GET-, GETNEXT- und GETBULK-Anforderungen, überwachen und darauf reagieren.

Der eingebettete SNMP-Agent überwacht standardmäßig den UDP-Port 161 für Abfrageanforderungen von Verwaltungssystemen. Sie können den Befehl `vicfg-snmp --port` zum Konfigurieren eines alternativen Ports verwenden. Zur Vermeidung von Konflikten zwischen dem SNMP-Agenten und den Ports anderer Dienste verweisen Sie auf <https://ports.vmware.com/home/VMware-Cloud-Director>.

Voraussetzungen

Sie müssen alle vorhandenen Firewallregeln entfernen, die mit Net-SNMP zusammenarbeiten, da VMware-SNMP den Abrufport beim Starten und Beenden des `snmpd`-Dienstes aktiviert und deaktiviert.

Verfahren

- 1 Melden Sie sich bei der Appliance-Shell als Benutzer mit Administratorrechten an.
- 2 Deaktivieren Sie SNMP, indem Sie folgenden Befehl ausführen.

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

- 3 Zum Ändern des Ports, der vom SNMP-Agenten zum Überwachen der Abfrageanforderungen verwendet wird, führen Sie folgenden Befehl aus.

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

Konfigurieren der VMware Cloud Director-Appliance für SNMP v1 und v2c

Ab VMware Cloud Director 10.2.2 können Sie die VMware Cloud Director-Appliance für SNMP konfigurieren, indem Sie mindestens eine Community für den SNMP-Agent konfigurieren. Wenn Sie den VMware Cloud Director-SNMP-Agenten für SNMP v1 und v2c konfigurieren, bietet der Agent Unterstützung für Abfragen.

In SNMP v1 und v2c handelt es sich bei Community-Strings um Namespaces, die ein oder mehrere verwaltete Objekte enthalten. Namespaces können zwar zur Authentifizierung verwendet werden, damit wird aber der Datenaustausch nicht gesichert. Verwenden Sie SNMP v3 zum Sichern der Kommunikation.

Um den SNMP-Agenten der VMware Cloud Director-Appliance zum Senden und Empfangen von SNMP v1- und v2c-Meldungen zu aktivieren, müssen Sie mindestens eine Community für den Agenten konfigurieren. Eine SNMP-Community definiert eine Gruppe von Geräten und Verwaltungssystemen. Nur Geräte und Verwaltungssysteme, die Mitglieder derselben Community sind, können SNMP-Meldungen austauschen. Ein Gerät oder Verwaltungssystem kann Mitglied in mehreren Communities sein.

Verfahren

- 1 Melden Sie sich bei der Appliance-Shell als Benutzer mit Administratorrechten an.
- 2 Führen Sie zum Konfigurieren einer SNMP-Community den Befehl `vicfg-snmp -c` aus.

Wenn Sie Communitys beispielsweise für öffentliche, östliche und westliche Netzwerkbetriebszentren konfigurieren möchten, führen Sie folgenden Befehl aus:

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

Bei jeder Angabe einer Community mit diesem Befehl überschreiben die von Ihnen angegebenen Einstellungen die vorherige Konfiguration. Verwenden Sie zur Eingabe mehrerer Communitys ein Komma als Trennzeichen.

- 3 Aktivieren Sie SNMP, indem Sie folgenden Befehl ausführen.

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

Konfigurieren der VMware Cloud Director-Appliance für SNMP v3

Ab VMware Cloud Director 10.2.2 können Sie die VMware Cloud Director-Appliance für SNMP v3 konfigurieren. Wenn Sie den SNMP-Agenten für SNMP v3 konfigurieren, unterstützt der Agent Abrufvorgänge und bietet höhere Sicherheit, einschließlich kryptografischer Authentifizierung und Verschlüsselung.

Die Konfiguration der VMware Cloud Director-Appliance für SNMP v3 besteht aus drei Teilen.

- 1 Konfigurieren der SNMP-Engine-ID
- 2 Konfigurieren der SNMP-Authentifizierung und der Datenschutzprotokolle
- 3 Konfigurieren der SNMP-Benutzer

Jeder SNMP v3-Agent verfügt über eine Engine-ID, die als eindeutiger Bezeichner für den Agenten dient. Die Engine-ID wird mit einer Hashing-Funktion verwendet, um lokalisierte Schlüssel für die Authentifizierung und Verschlüsselung der SNMP v3-Meldungen zu generieren. Wenn Sie vor dem Aktivieren des SNMP-Agenten keine Engine-ID angeben, wird von VMware Cloud Director beim Aktivieren des eigenständigen SNMP-Agenten eine Engine-ID erzeugt.

Zum Sicherstellen der Identität eines Benutzers können Sie Authentifizierung verwenden. Der Datenschutz ermöglicht die Verschlüsselung von SNMP v3-Nachrichten, um die Vertraulichkeit der Daten sicherzustellen. Die Datenschutzprotokolle bieten ein höheres Maß an Sicherheit als SNMP v1 und v2c, die dazu Community-Strings verwenden. Sowohl Authentifizierung als auch Datenschutz sind optional. Wenn Sie Datenschutz jedoch aktivieren möchten, müssen Sie Authentifizierung aktivieren.

Der Standardwert für die Authentifizierung und die Datenschutzprotokolle lautet „Keine“.

Sie können bis zu fünf Benutzer konfigurieren, die auf die SNMP v3-Informationen zugreifen können. Benutzernamen dürfen nicht mehr als 32 Zeichen lang sein. Beim Konfigurieren eines Benutzers erzeugen Sie die Hash-Werte für Authentifizierung und Datenschutz basierend auf den Authentifizierungs- und Datenschutzwörtern des Benutzers und der Engine-ID des SNMP-Agenten. Wenn Sie nach der Konfiguration der Benutzer die Engine-ID, das Authentifizierungsprotokoll oder das Datenschutzprotokoll ändern, werden die Benutzer ungültig gemacht und müssen neu konfiguriert werden.

Voraussetzungen

Wenn Sie SNMP-Authentifizierung und Datenschutzprotokolle konfigurieren möchten, stellen Sie sicher, dass Sie die Authentifizierungs- und Datenschutzwörter für jeden zu konfigurierenden Benutzer kennen. Die Kennwörter müssen mindestens acht Zeichen lang sein.

Verfahren

- 1 Melden Sie sich bei der Appliance-Shell als Benutzer mit Administratorrechten an.
- 2 Führen Sie den Befehl `vicfg-snmp --engineid` aus, um das Ziel zu konfigurieren.

Führen Sie beispielsweise folgenden Befehl aus:

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

Wobei `80001f8880167b18238d613d6000000000` die ID darstellt, eine hexadezimale Zeichenfolge mit einer Länge von 5 bis 32 Zeichen.

- 3 (Optional) Führen Sie zum Konfigurieren des Authentifizierungsprotokolls den Befehl `vicfg-snmp --authentication` aus.

Führen Sie beispielsweise folgenden Befehl aus:

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

Wobei *protocol* entweder **none** für keine Authentifizierung oder **SHA1**, **SHA256**, **SHA384** oder **SHA512** sein muss. Wenn Sie das Authentifizierungsprotokoll beispielsweise auf „SHA512“ festlegen möchten, müssen Sie folgenden Befehl ausführen.

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

- 4 (Optional) Führen Sie zum Konfigurieren des Datenschutzprotokolls den Befehl `vicfg-snmp --privacy` aus.

Führen Sie beispielsweise folgenden Befehl aus:

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

Wobei *protocol* entweder **none** für keinen Datenschutz oder **AES128**, **AES192** bzw. **AES256** sein muss. Wenn Sie das Datenschutzprotokoll beispielsweise auf **AES128** festlegen möchten, müssen Sie folgenden Befehl ausführen.

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

- 5 Wenn Sie Authentifizierung, Datenschutz oder beides verwenden, führen Sie den folgenden Befehl aus, um die Hash-Werte für die Authentifizierung und den Datenschutz für einen Benutzer zu generieren.

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

Je nach den Authentifizierungs- und Datenschutzeinstellungen müssen Sie *authentication-password*, *privacy-password* oder beides eingeben. Die Kennwörter müssen mindestens 8 Zeichen lang sein. Notieren Sie sich die Einträge für *authentication-password* und *privacy-password*, da Sie diese zum Einrichten eines SNMP-Clients benötigen. Die Ausgabe des Befehls enthält den lokalisierten Schlüssel der Authentifizierung und den lokalisierten Schlüssel des Datenschutzes.

- 6 Konfigurieren Sie einen oder mehrere Benutzer, indem Sie den folgenden Befehl ausführen. Sie können mehrere Benutzer angeben, indem Sie sie in Form einer kommagetrennten Liste hinzufügen. Sie können bis zu fünf Benutzer konfigurieren.

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

Der Befehl umfasst die folgenden Parameter.

Parameter	Beschreibung
<i>userid</i>	Ersetzen Sie den Parameter durch den Benutzernamen.
<i>authhash</i>	Ersetzen Sie den Parameter durch den lokalisierten Schlüssel der Authentifizierung.
<i>privhash</i>	Ersetzen Sie den Parameter durch den lokalisierten Schlüssel des Datenschutzes.
<i>model</i>	Ersetzen Sie diesen Parameter durch die Stufe der für diesen Benutzer aktivierten Sicherheit, die auf auth (nur für Authentifizierung), priv (für Authentifizierung und Datenschutz) oder none (keine Authentifizierung und kein Datenschutz) festgelegt sein kann.

Wenn Sie beispielsweise einen Benutzer ohne Sicherheit konfigurieren möchten, können Sie Folgendes ausführen:

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

Wenn Sie einen Benutzer mit Autorisierungs-Hash konfigurieren möchten, können Sie Folgendes ausführen:

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

Wenn Sie einen Benutzer mit Autorisierungs-Hash und Datenschutz-Hash konfigurieren möchten, können Sie Folgendes ausführen:

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

- 7 (Optional) Wenn Sie einen oder mehrere Benutzer löschen möchten, wiederholen Sie Schritt 6 mit den neuen Benutzerdetails.

Durch eine erneute Ausführung von `vicfg-snmp --users` werden alle vorherigen Einstellungen überschrieben.

- 8 Aktivieren Sie SNMP, indem Sie folgenden Befehl ausführen.

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

Verwenden von `snmpwalk` mit VMware Cloud Director-SNMP

Ab VMware Cloud Director 10.2.2 können Sie zum Verketteten von `GETNEXT`-Anforderungen ohne Eingabe eindeutiger Befehle für jede OID bzw. jeden Knoten innerhalb einer untergeordneten Struktur den Befehl `snmpwalk` ausführen.

Voraussetzungen

- Konfigurieren Sie die VMware Cloud Director-Appliance für [Konfigurieren der VMware Cloud Director-Appliance für SNMP v1 und v2c](#) oder [Konfigurieren der VMware Cloud Director-Appliance für SNMP v3](#).

Verfahren

- 1 Stellen Sie auf einer lokalen Maschine sicher, dass der Befehl `snmpwalk` installiert wurde. Ist dies nicht der Fall, installieren Sie den Befehl gegebenenfalls.
- 2 Führen Sie den Befehl `snmpwalk` aus.

```
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
```

Wobei `-l` die Sicherheitsstufe darstellt, die auf `noAuthNoPriv`, `authNoPriv` oder `authPriv` festgelegt werden kann. Um Hilfe zum Befehl `snmpwalk` zu erhalten, können Sie `-h` ausführen.

Beispiel: Abfrage `snmpwalk`

Eine Beispielabfrage der MIB-OID `sysDescr.0` kann folgendermaßen lauten:

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

Dieser Befehl gibt die folgende Ausgabe zurück.

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

Zurücksetzen der SNMP-Einstellungen der VMware Cloud Director-Appliance

Ab VMware Cloud Director 10.2.2 können Sie den SNMP-Agenten der VMware Cloud Director-Appliance konfigurieren. Zum Löschen aller SNMP-Einstellungen und Deaktivieren des Agenten setzen Sie die SNMP-Einstellungen der Appliance zurück.

Voraussetzungen

Konfigurieren Sie die VMware Cloud Director-Appliance für [Konfigurieren der VMware Cloud Director-Appliance für SNMP v1 und v2c](#) oder [Konfigurieren der VMware Cloud Director-Appliance für SNMP v3](#).

Verfahren

- 1 Melden Sie sich bei der Appliance-Shell als Benutzer mit Administratorrechten an.
- 2 Zum Zurücksetzen aller SNMP-Einstellungen auf die Standardwerte und Deaktivieren des SNMP-Agenten führen Sie folgenden Befehl aus.

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

Anzeigen der SNMP-Einstellungen der VMware Cloud Director-Appliance

Ab VMware Cloud Director 10.2.2 können Sie die SNMP-Einstellungen anzeigen, wie z. B. UDP-Port, Communitys, V3-Benutzer, Engine-ID, Autorisierung und Datenschutzprotokolle usw.

Voraussetzungen

Konfigurieren Sie die VMware Cloud Director-Appliance für [Konfigurieren der VMware Cloud Director-Appliance für SNMP v1 und v2c](#) oder [Konfigurieren der VMware Cloud Director-Appliance für SNMP v3](#).

Verfahren

- 1 Melden Sie sich bei der Appliance-Shell als Benutzer mit Administratorrechten an.
- 2 Zum Anzeigen der SNMP-Einstellungen führen Sie den folgenden Befehl aus.

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

Beispiel: vicfg-snmp --show-Beispielausgabe

Die Beispielausgabe zeigt, dass der SNMP-Agent für einen V3-Benutzer mit einem Autorisierungs-Hash und einem Datenschutz-Hash aktiviert ist.

```
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.
```

Bearbeiten der DNS-Einstellungen der VMware Cloud Director-Appliance

Nach der Bereitstellung können Sie den bzw. die DNS-Server der VMware Cloud Director-Appliance ändern.

Wichtig Sie können den Hostnamen der Appliance nicht bearbeiten. Sie müssen eine neue Appliance mit dem gewünschten Hostnamen bereitstellen.

Voraussetzungen

Um dauerhafte Änderungen an den OVF-Eigenschaften vorzunehmen, müssen Sie die vSphere-Benutzeroberfläche zum Ändern der Werte der OVF-Eigenschaft verwenden. Weitere Informationen finden Sie im Thema „Konfigurieren von vApp-Eigenschaften“ im Handbuch *Verwaltung virtueller vSphere-Maschinen*.

Verfahren

- 1 Wenn Sie die DNS-Einstellungen zu Testzwecken vorübergehend ändern möchten, bearbeiten Sie die DNS-Einstellungen in VMware Cloud Director.
 - a Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der VMware Cloud Director-Appliance als **root** an.
 - b (Optional) Prüfen Sie die aktuelle DNS-Konfiguration, indem Sie den folgenden Befehl ausführen:

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

- c Ändern Sie den bzw. die DNS-Server.

Um mehrere DNS-Server anzugeben, legen Sie *DNS_server_IP* als kommagetrennte Liste ohne Leerzeichen fest.

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

- d Starten Sie den VAOS-Dienst neu, damit die Änderungen wirksam werden.

```
systemctl restart vaos.service
```

- 2 Wenn Sie die DNS-Einstellungen dauerhaft ändern möchten, verwenden Sie die vSphere-Benutzeroberfläche, um den Wert der Eigenschaft `vami.DNS.VMware_vCloud_Director` auf die IP-Adresse des neuen DNS-Servers festzulegen.

Geben Sie zur Angabe mehrerer DNS-Server eine kommagetrennte Liste ohne Leerzeichen ein.

Hinweis Sie müssen die VM ausschalten, um den Wert der Eigenschaft in vSphere zu ändern.

Bearbeiten der statischen Routen für die Netzwerkschnittstellen der VMware Cloud Director-Appliance

Sie können die statischen Routen für die Netzwerkschnittstellen `eth0` und `eth1` nach der ersten VMware Cloud Director-Bereitstellung ändern.

Voraussetzungen

Um dauerhafte Änderungen an den OVF-Eigenschaften vorzunehmen, müssen Sie die vSphere-Benutzeroberfläche zum Ändern der Werte der OVF-Eigenschaft verwenden. Weitere Informationen finden Sie im Thema „Konfigurieren von vApp-Eigenschaften“ im Handbuch *Verwaltung virtueller vSphere-Maschinen*.

Verfahren

- 1 Wenn Sie den Wert der statischen Route zu Testzwecken vorübergehend ändern möchten, bearbeiten Sie die statischen Routen in VMware Cloud Director.
 - a Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der VMware Cloud Director-Appliance als **root** an.
 - b (Optional) Überprüfen Sie die aktuelle Konfiguration für statische Routen.
 - Führen Sie für `eth0` folgenden Befehl aus:

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

- Führen Sie für `eth1` folgenden Befehl aus:

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

- c Ändern Sie den Wert für die statische Route.

Die statischen Routen müssen sich in einer kommagetrennten Liste mit Routenspezifikationen befinden. Beispielsweise müssen Sie für `eth0` Folgendes ausführen:

```
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"
```

- Führen Sie für `eth0` folgenden Befehl aus:

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

- Führen Sie für `eth1` folgenden Befehl aus:

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

- d Starten Sie den Netzwerkdienst auf der VMware Cloud Director-Appliance neu.

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

- 2 Wenn Sie den Wert der statischen Route dauerhaft ändern möchten, bearbeiten Sie die OVF-Eigenschaft mithilfe der vSphere-Benutzeroberfläche.

Die statischen Routen müssen sich in einer kommagetrennten Liste mit Routenspezifikationen befinden.

Hinweis Sie müssen die VM ausschalten, um den Wert der Eigenschaft in vSphere zu ändern.

- Verwenden Sie die vSphere-Benutzeroberfläche, um den Wert der Eigenschaft `vcloudnet.routes0.VMware_vCloud_Director` auf die Zeichenfolge der neuen Routenspezifikation festzulegen.
- Verwenden Sie die vSphere-Benutzeroberfläche, um den Wert der Eigenschaft `vcloudnet.routes1.VMware_vCloud_Director` auf die Zeichenfolge der neuen Routenspezifikation festzulegen.

Konfigurationskripts in der VMware Cloud Director-Appliance

Die VMware Cloud Director-Appliance enthält bestimmte Konfigurationskripts.

Verzeichnis	Beschreibung
<code>/opt/vmware/appliance/bin/</code>	Die Konfigurationskripts der Appliance.
<code>/opt/vmware/appliance/etc/</code>	Die Konfigurationsdateien der Appliance.
<code>/opt/vmware/appliance/etc/pg_hba.d/</code>	Das Verzeichnis, in dem Sie benutzerdefinierte Einträge zur Datei <code>pg_hba.conf</code> hinzufügen können. Weitere Informationen finden Sie unter Konfigurieren des externen Zugriffs auf die VMware Cloud Director-Datenbank .

Verlängern der VMware Cloud Director-Appliance-Zertifikate

Wenn Sie die VMware Cloud Director-Appliance bereitstellen, werden selbstsignierte Zertifikate mit einem Gültigkeitszeitraum von 365 Tagen generiert. Wenn in Ihrer Umgebung ablaufende oder abgelaufene Zertifikate vorhanden sind, können Sie neue selbstsignierte Zertifikate generieren. Sie müssen die Zertifikate für jede VMware Cloud Director-Zelle einzeln erneuern.

Die VMware Cloud Director-Appliance verwendet zwei Sätze von SSL-Zertifikaten. Der VMware Cloud Director-Dienst verwendet einen Satz von Zertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation. Die eingebettete PostgreSQL-Datenbank und die Verwaltungsbenutzeroberfläche der VMware Cloud Director-Appliance nutzen gemeinsam den anderen Satz von SSL-Zertifikaten.

Sie können beide Sätze selbstsignierter Zertifikate ändern. Wenn Sie alternativ dazu von einer Zertifizierungsstelle signierte Zertifikate für die HTTPS- und Konsolenproxy-Kommunikation von VMware Cloud Director verwenden, können Sie nur die eingebettete PostgreSQL-Datenbank und das Zertifikat der Verwaltungsschnittstelle der Appliance ändern. Von einer Zertifizierungsstelle signierte Zertifikate enthalten eine vollständige Vertrauenskette, die von einer bekannten öffentlichen Zertifizierungsstelle ausgeht.

Voraussetzungen

- Wenn Sie das Zertifikat für den primären Knoten in einem Datenbank-Hochverfügbarkeits-Cluster erneuern, versetzen Sie alle anderen Knoten in den Wartungsmodus, um Datenverlust zu verhindern. Weitere Informationen finden Sie unter [Verwalten einer Zelle](#).
- Wenn der FIPS-Modus aktiviert ist, muss das **root**-Kennwort der Appliance 14 oder mehr Zeichen enthalten. Weitere Informationen finden Sie im [Ändern des Root-Kennworts der VMware Cloud Director-Appliance](#).

Verfahren

- 1 Melden Sie sich direkt oder mithilfe von SSH beim Betriebssystem der VMware Cloud Director-Appliance als **root** an.
- 2 Führen Sie zum Beenden der VMware Cloud Director-Dienste den folgenden Befehl aus.

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

- 3 Generieren Sie neue selbstsignierte Zertifikate für die Datenbank und die Appliance-Verwaltungsbenutzeroberfläche oder für die Kommunikation zwischen HTTPS und Konsolen-Proxy, die Datenbank und die Appliance-Verwaltungsbenutzeroberfläche.
 - Generieren Sie selbstsignierte Zertifikate nur für die eingebettete PostgreSQL-Datenbank und die Appliance-Verwaltungsbenutzeroberfläche von VMware Cloud Director. Führen Sie den folgenden Befehl aus:

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

Dieser Befehl bewirkt, dass automatisch die neu generierten Zertifikate für die eingebettete PostgreSQL-Datenbank und die Verwaltungsschnittstelle der Appliance verwendet werden. Der PostgreSQL- und der Nginx-Server werden neu gestartet.

- Generieren Sie zusätzlich zu den Zertifikaten für die eingebettete PostgreSQL-Datenbank und die Appliance-Verwaltungsbenutzeroberfläche neue selbstsignierte Zertifikate für die Kommunikation zwischen HTTPS und Konsolen-Proxy von VMware Cloud Director.
 - a Führen Sie den folgenden Befehl aus:

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

- b Wenn Sie keine von einer Zertifizierungsstelle signierten Zertifikate verwenden, führen Sie den Befehl zum Importieren der neu generierten selbstsignierten Zertifikate in VMware Cloud Director aus.

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

- c Starten Sie den VMware Cloud Director-Dienst neu.

```
service vmware-vcd start
```

Dieser Befehl bewirkt, dass automatisch die neu generierten Zertifikate für die eingebettete PostgreSQL-Datenbank und die Verwaltungsschnittstelle der Appliance verwendet werden. Der PostgreSQL- und der Nginx-Server werden neu gestartet. Der Befehl generiert einen neuen Zertifikat-Keystore `/opt/vmware/vcloud-director/certificates.ks` mit neuen selbstsignierten Zertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation von VMware Cloud Director, die in [4](#) verwendet werden.

Ergebnisse

Die verlängerten selbstsignierten Zertifikate werden in der VMware Cloud Director-Benutzeroberfläche angezeigt.

Das neue PostgreSQL-Zertifikat wird bei der nächsten Ausführung der Funktion `appliance-sync` in den VMware Cloud Director-Truststore auf anderen VMware Cloud Director-Zellen importiert. Der Vorgang kann bis zu 60 Sekunden dauern.

Nächste Schritte

Bei Bedarf kann ein selbstsigniertes Zertifikat durch ein von einer externen oder internen Zertifizierungsstelle signiertes Zertifikat ersetzt werden.

Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und VMware Cloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats

Standardmäßig nutzen die eingebettete PostgreSQL-Datenbank und die Verwaltungsbenutzeroberfläche der VMware Cloud Director-Appliance gemeinsam einen Satz von selbstsignierten SSL-Zertifikaten. Um die Sicherheit zu erhöhen, können Sie die standardmäßigen selbstsignierten Zertifikate durch signierte Zertifikate einer Zertifizierungsstelle (CA) ersetzen.

Wenn Sie die VMware Cloud Director-Appliance bereitstellen, werden selbstsignierte Zertifikate mit einem Gültigkeitszeitraum von 365 Tagen generiert. Die VMware Cloud Director-Appliance verwendet zwei Sätze von SSL-Zertifikaten. Der VMware Cloud Director-Dienst verwendet einen Satz von Zertifikaten für die HTTPS- und die Konsolen-Proxy-Kommunikation. Die eingebettete PostgreSQL-Datenbank und die Verwaltungsbenutzeroberfläche der VMware Cloud Director-Appliance nutzen gemeinsam den anderen Satz von SSL-Zertifikaten.

Hinweis Der Vorgang zum Ersetzen der Zertifikate für die Datenbank und die Appliance-Verwaltungsbenutzeroberfläche wirkt sich nicht auf die Zertifikate für die Kommunikation zwischen HTTPS und Konsolen-Proxy aus. Wenn Sie einen der Zertifikatssätze ersetzen, gilt dies nicht notwendigerweise für den anderen Satz.

Verfahren

- 1 Senden Sie die Zertifikatssignieranforderung unter `/opt/vmware/appliance/etc/ssl/vcd_ova.csr` zum Signieren an die Zertifizierungsstelle.
- 2 Wenn Sie das Zertifikat für die primäre Datenbank ersetzen, versetzen Sie alle anderen Knoten in den Wartungsmodus, um zu verhindern, dass Daten verloren gehen.
- 3 Ersetzen Sie das vorhandene Zertifikat im PEM-Format unter `/opt/vmware/appliance/etc/ssl/vcd_ova.crt` durch das signierte Zertifikat, das von Ihrer Zertifizierungsstelle in [Schritt 1](#) abgerufen wurde.
- 4 Um das neue Zertifikat abzurufen, starten Sie die Dienste „vpostgres“, „nginx“ und „vcd_ova_ui“ neu.

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

```
systemctl restart vpostgres.service
```

- 5 Wenn Sie das Zertifikat für die primäre Datenbank ersetzen, nehmen Sie alle anderen Knoten aus dem Wartungsmodus.

Ergebnisse

Das neue Zertifikat wird bei der nächsten Ausführung der Funktion `appliance-sync` in den VMware Cloud Director-Truststore auf anderen VMware Cloud Director-Zellen importiert. Der Vorgang kann bis zu 60 Sekunden dauern.

Ersetzen des Übertragungsserverspeichers für die VMware Cloud Director-Appliance

Sie können die NFS-Freigabe der VMware Cloud Director-Appliance nach der Bereitstellung ändern.

Verfahren

- 1 Legen Sie den Dienst `vmware-vcd` still und beenden Sie ihn auf allen Appliances in der VMware Cloud Director-Servergruppe.

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

- 2 Beenden Sie den `appliance-sync.timer`-Dienst auf allen Appliances in der Servergruppe.

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

- 3 Kopieren Sie auf der primären Appliance die Daten aus der alten NFS-Freigabe in die neue.

- a Erstellen Sie einen neuen Mount-Punkt für die NFS-Freigabe.

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

- b Mounten Sie die neue NFS-Serverfreigabe auf dem neuen Mount-Punkt.

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

- c Kopieren Sie die Dateien von der alten Übertragungsfreigabe in die neue Übertragungsfreigabe.

Hinweis Die für das Kopieren der Dateien erforderliche Zeit hängt von der Anzahl der in der Freigabe des Übertragungsordners zwischengespeicherten Katalogelemente ab.

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

- d Wenn Sie die Dateien erfolgreich kopiert haben, bestätigen Sie, dass der Inhalt der alten NFS-Freigabe in der neuen NFS-Freigabe enthalten ist, indem Sie den Inhalt von `/opt/vmware/vcloud-director/data/transfer-new` überprüfen oder den folgenden Befehl ausführen.

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

- e Unmounten Sie die neue NFS-Freigabe vom temporären Mount-Punkt.

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

- f Löschen Sie den temporären Mount-Punkt.

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

- 4 Aktualisieren Sie die Datei `/etc/fstab`, indem Sie die NFS-Zeile durch den Pfad zum neuen NFS-Server ersetzen.

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

- 5 Unmounten Sie die alte NFS-Freigabe.

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

- 6 Mounten Sie die neue NFS-Freigabe.

```
mount -a
```

- 7 Bestätigen Sie, dass Sie die NFS-Freigabe erfolgreich gemountet haben, indem Sie sicherstellen, dass die Ausgabe des Befehls `mount` die gemountete NFS-Freigabe auflistet.

- 8 Ändern Sie mit dem folgenden Befehl die Zuständigkeit für das Übertragungsverzeichnis von `root` in `vcloud`.

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

- 9 Starten Sie den `appliance-sync.timer`-Dienst neu.

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

- 10 Wiederholen Sie die Schritte 4 bis 9 auf allen Knoten in der Servergruppe.

- 11 Starten Sie den Dienst `vmware-vcd` auf jedem der Knoten neu.

```
systemctl start vmware-vcd
```

- 12 Stellen Sie sicher, dass `vmware-vcd` auf allen Knoten in der Servergruppe ordnungsgemäß funktioniert.

Erhöhen der Kapazität der eingebetteten PostgreSQL-Datenbank auf einer VMware Cloud Director-Appliance

Wenn Sie nicht genügend Speicherplatz auf der PostgreSQL-Datenbankfestplatte einer VMware Cloud Director-Appliance haben, können Sie die Kapazität der eingebetteten PostgreSQL-Datenbank erhöhen.

Die PostgreSQL-Datenbank befindet sich auf der Festplatte 3. Sie hat eine Standardgröße von 80 GB. Der Vorgang kann durchgeführt werden, während die Appliances betriebsbereit sind.

Wichtig Sie müssen die Kapazität aller vorhandenen Standby-Appliances erhöhen, bevor Sie die Kapazität der primären Appliance erhöhen.

Die Festplattengröße der PostgreSQL-Datenbank auf jeder Standby-Appliance muss mit der Größe der PostgreSQL-Datenbankfestplatte auf der primären Appliance übereinstimmen.

Voraussetzungen

- Wenn Ihre VMware Cloud Director-Umgebung über Standby-Knoten verfügt, identifizieren Sie die Standby-Knoten und den primären Knoten und starten Sie den Vorgang von einem Standby-Knoten aus. Weitere Informationen zum Identifizieren der Rollen der Knoten finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).
- Wenn Ihre VMware Cloud Director-Umgebung nur aus einem primären Knoten besteht, führen Sie den Vorgang auf dem primären Knoten aus.

Verfahren

- 1 Melden Sie sich beim vSphere Client an, um die Kapazität der Festplatte 3 auf die gewünschte Größe zu erhöhen.

Die Festplattengröße der PostgreSQL-Datenbank auf jeder Standby-Appliance muss so groß sein wie die PostgreSQL-Datenbankfestplatte auf der primären Appliance.

- a Wählen Sie die virtuelle Maschine der Appliance aus, die Sie ändern möchten.
- b Wählen Sie **Aktionen > Einstellungen bearbeiten**.
- c Erhöhen Sie die Größe von **Festplatte 3** und klicken Sie auf **OK**.

Der Fortschritt der Neukonfigurationsaufgabe erscheint im Bereich **Aktuelle Aufgaben**.

- 2 Wenden Sie die Änderungen auf das Betriebssystem des Appliance-Knotens an.
 - a Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der VMware Cloud Director-Appliance als **root** an.
 - b Um die Änderung der Festplattengröße auf das Betriebssystem anzuwenden, führen Sie das folgende Skript aus.

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

- 3 Falls Ihre Umgebung nicht nur aus einer primären Appliance besteht, wiederholen Sie den Vorgang für jeden der Knoten, der über eine Datenbank verfügt.

Ändern der PostgreSQL-Konfigurationen in der VMware Cloud Director-Appliance

Sie können die PostgreSQL-Konfigurationen der VMware Cloud Director-Appliance mithilfe des PostgreSQL-Befehls `ALTER SYSTEM` ändern.

Der Befehl `ALTER SYSTEM` schreibt die Änderungen der Parametereinstellungen in die Datei `postgresql.auto.conf`, die bei der PostgreSQL-Initialisierung Vorrang vor der Datei `postgresql.conf` hat. Einige Einstellungen erfordern einen Neustart des PostgreSQL-Diensts, während andere dynamisch konfiguriert sind und keinen Neustart erfordern. Ändern Sie die Datei `postgresql.conf`, da der Betrieb des Clusters eine regelmäßige Überschreibung der Datei erfordert und die Änderungen nicht persistent sind.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem der primären Appliance als **root** an.

- 2 Ändern Sie den Benutzer in **postgres**.

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

- 3 Verwenden Sie den PostgreSQL-Befehl `ALTER SYSTEM`, um einen Parameter zu ändern.

```
psql -c "ALTER SYSTEM set parameter='value';"
```

- 4 Wiederholen Sie [Schritt 3](#) für jeden Konfigurationsparameter, den Sie ändern möchten.

- 5 Wenn einige der Parameter, die Sie ändern möchten, einen Neustart des PostgreSQL-Diensts erfordern, starten Sie den Prozess „vpostgres“ neu.

```
systemctl restart vpostgres
```

- 6 Wenn Ihre Umgebung Standby-Knoten aufweist, kopieren Sie die Datei `postgresql.auto.conf` in die Standby-Appliances und starten Sie den PostgreSQL-Dienst bei Bedarf neu.

- a Kopieren Sie die Datei `postgresql.auto.conf` vom primären Knoten auf einen Standby-Knoten.

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

- b Wenn einige der Parameter in der kopierten Datei `postgresql.auto.conf` einen Neustart erfordern, um wirksam zu werden, starten Sie den Prozess „vpostgres“ auf dem Standby-Knoten neu.

```
systemctl restart vpostgres
```

- c Wiederholen Sie [6.a](#) und [6.b](#) für jeden Standby-Knoten.

Aufheben der Registrierung einer aktiven Standby-Zelle in einem Datenbank-Hochverfügbarkeits-Cluster

Wenn Sie einen Knoten in einer anderen Rolle verwenden oder ihn aus dem Hochverfügbarkeits-Cluster entfernen möchten, müssen Sie seine Registrierung aufheben.

Weitere Informationen zur VMware Cloud Director-Appliance-API finden Sie in der [VMware Cloud Director Appliance-API-Dokumentation](#).

Sie können die Registrierung der Zelle während des normalen Systembetriebs aufheben.

Hinweis Damit der primäre Knoten normal funktioniert, muss immer mindestens ein Standby-Knoten ausgeführt werden.

Verfahren

- 1 Um den Namen des Standby-Knotens zu finden, dessen Registrierung Sie aufheben möchten, führen Sie die VMware Cloud Director Appliance-API-Methode `NODES` aus.
- 2 Führen Sie von einem der anderen Knoten aus die VMware Cloud Director-Appliance-API-Methode `UNREGISTER` aus.

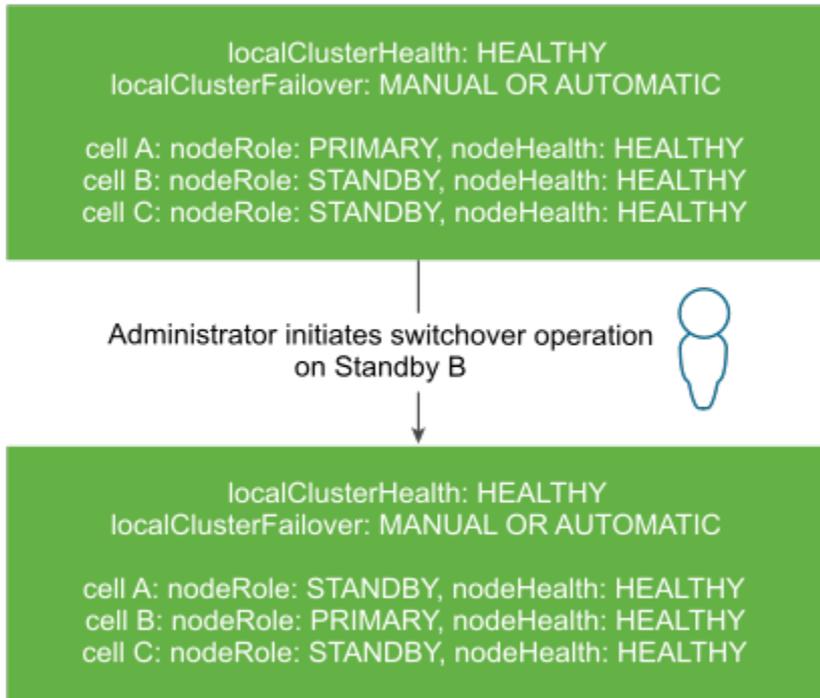
`node-name` steht dabei für den Namen der Standby-Appliance, die Sie entfernen möchten.
- 3 Um sich zu vergewissern, dass der Standby-Knoten, dessen Registrierung aufgehoben wurde, nicht mehr im Hochverfügbarkeits-Cluster der Datenbank angezeigt wird, führen Sie die API-Methode `NODES` aus.

Tauschen der Rollen der primären Zelle und einer Standby-Zelle in einem Datenbank-Hochverfügbarkeits-Cluster

Sie können die Verwaltungsschnittstelle der VMware Cloud Director-Appliance verwenden, um die Rollen der Zellen in einem Hochverfügbarkeitscluster der Datenbank zu tauschen und eine andere Zelle als primäre Zelle heraufzustufen.

Sie können die Rollen der primären und Standby-Zelle mithilfe der Verwaltungsschnittstelle der VMware Cloud Director-Appliance oder der API der VMware Cloud Director-Appliance tauschen. In diesem Verfahren werden die Schritte zum Durchführen des Switchovers mithilfe der Verwaltungsschnittstelle beschrieben.

Abbildung 3-3. Switchover zwischen der primären und einer Standby-Zelle



Voraussetzungen

- Stellen Sie sicher, dass alle Knoten im Cluster fehlerfrei und online sind. Weitere Informationen finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

Verfahren

- 1 Legen Sie die Aktivitäten für alle VMware Cloud Director-Zellen still, die Teil der Servergruppe sind, oder versetzen Sie die Zellen in den Wartungsmodus.
 Der Switchover führt dazu, dass die VMware Cloud Director-Datenbank für 30 bis 60 Sekunden nicht verfügbar ist. Zur Vermeidung unerwarteter Aufgabenfehler müssen Sie die Aktivität für alle Zellen im Cluster stilllegen.
- 2 Melden Sie sich als **root** bei der Verwaltungsschnittstelle der Appliance unter `https://primary_eth1_ip_address:5480` an.
- 3 Wählen Sie im linken Bereich **Verfügbarkeit der eingebetteten Datenbank** aus.
 Sie können die Namen der Zellen, die zugehörigen Rollen, ihren Status und den Namen der Zelle, der die Standby-Zellen folgen, anzeigen.
- 4 Stellen Sie sicher, dass der Clusterzustand `Healthy` lautet.
- 5 Klicken Sie auf die Schaltfläche **Switchover** für die Zelle, die als primäre Zelle heraufgestuft werden soll, und bestätigen Sie den Switchover.

- 6 Wenn die Switchover-Aufgabe abgeschlossen ist, starten Sie den Scheduler neu oder deaktivieren Sie den Wartungsmodus für die Zellen im Cluster.

Abonnieren von Ereignissen, Aufgaben und Metriken mithilfe eines MQTT-Clients

Mithilfe eines MQTT-Clients können Sie Meldungen zu VMware Cloud Director-Ereignissen und -Aufgaben abonnieren.

MQTT ist ein schlankes, binäres Nachrichtentransportprotokoll. VMware Cloud Director verwendet MQTT, um Informationen zu Ereignissen und Aufgaben zu veröffentlichen, die Sie mithilfe eines MQTT-Clients abonnieren können. MQTT-Nachrichten durchlaufen einen MQTT-Broker, der Nachrichten auch speichern kann, falls die Clients nicht online sind.

Ab VMware Cloud Director 10.2.2 können Sie einen MQTT-Client zum Abonnieren von Metriken verwenden.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen MQTT-Client verfügen, der WebSocket unterstützt.
- Stellen Sie sicher, dass Sie einer von WebSocket aktualisierten Anforderung Kopfzeilen hinzufügen können.
- Wenn Sie Metriken abonnieren möchten, konfigurieren Sie die Metrikerfassung und aktivieren Sie die Veröffentlichung von Metriken. Weitere Informationen finden Sie im [Konfigurieren der Erfassung und Veröffentlichung von Metriken](#).

Verfahren

- 1 Melden Sie sich mithilfe des OpenAPI-Endpoints bei VMware Cloud Director an.
- 2 Legen Sie zum Herstellen einer WebSocket-Verbindung die Eigenschaft „Sec-WebSocket-Protocol“ auf `mqtt` fest. Legen Sie weiterhin fest, dass der Client die Verbindung über den Pfad `/messaging/mqtt` herstellt, fügen Sie einen Autorisierungs-Header hinzu und befolgen Sie den standardmäßigen MQTT-Verbindungs-Flow.

Sie erhalten das JWT-Token über die standardmäßige Anmeldungsanforderung an VMware Cloud Director. Sie können den Benutzernamen und das Kennwort leer lassen.

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

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

- 3 Nachdem die Verbindung hergestellt wurde, können Sie über den MQTT-Client Themen abonnieren.

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

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

Organisationsadministratoren können mithilfe von Platzhaltern auf alle organisationsbezogenen Themen zugreifen.

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

Systemadministratoren können mithilfe von Platzhaltern auf alle Themen zugreifen.

```
publish/#
```

- 4 (Optional) Abonnieren Sie Metriken für VMware Cloud Director 10.2.2 oder höher.

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

Nur **Systemadministratoren** können auf das Metrikthema zugreifen.

Automatische Skalierungsgruppen

Ab VMware Cloud Director 10.2.2 können Sie Mandantenbenutzern die automatische Skalierung von Anwendungen in Abhängigkeit von der aktuellen CPU- und Speichernutzung ermöglichen.

Je nach den vordefinierten Kriterien für die CPU- und Arbeitsspeichernutzung können Mandanten VMware Cloud Director verwenden, um die Anzahl der VMs in einer ausgewählten Skalierungsgruppe automatisch hoch- oder herunterzuskalieren. Damit Mandanten Anwendungen automatisch skalieren können, müssen Sie die automatische Skalierungslösung konfigurieren, veröffentlichen und Zugriff darauf gewähren.

Zum Ausgleichen der Serverlast, die Sie zum Ausführen derselben Anwendung konfigurieren, können Sie VMware NSX Advanced Load Balancer (Avi Networks) verwenden.

Konfigurieren und Veröffentlichen des Plug-Ins für automatische Skalierung

Bevor Sie Mandanten Zugriff gewähren, müssen Sie die Lösung für die automatische Skalierung von Gruppen konfigurieren. Sie können die automatische Skalierung ab VMware Cloud Director 10.2.2 verwenden.

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem einer beliebigen Zelle im Cluster als **root** an.
- 2 Aktivieren Sie die Erfassung von Metrikdaten, indem Sie die Metrikerfassung in einer Cassandra-Datenbank einrichten oder Metriken ohne Metrikdatenpersistenz erfassen.
 - [Installieren und Konfigurieren einer Cassandra-Datenbank zum Speichern von historischen Metrikdaten](#)
 - Zum Erfassen von Metrikdaten ohne Datenpersistenz führen Sie die folgenden Befehle aus:

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

3 Aktivieren Sie die Veröffentlichung von Metriken.

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

4 Erstellen Sie eine Datei vom Typ `metrics.groovy` im Verzeichnis `/tmp` mit folgenden Inhalten.

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
        historicInterval=20
        entity="VM"
        instance=""
        minReportingInterval=300
        aggregator="AVERAGE"
    }
}
```

5 Importieren Sie die Datei.

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

6 Wenn Sie Cassandra zuvor konfiguriert haben, aktualisieren Sie das Cassandra-Schema, indem Sie die Adressen der Knoten, die Datenbankauthentifizierungsdetails sowie die Port- und Metriklebensdauer in Tagen korrekt angeben.

```
$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 Wenn Sie die Zelle mit einem von einer Zertifizierungsstelle signierten Zertifikat ausführen, verwenden Sie den folgenden Befehl zum Aktivieren der automatischen Skalierung.

```
$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>
```

Wenn Sie den Befehl über das Terminal ausführen, verwenden Sie als Escape-Zeichen für alle Sonderzeichen den umgekehrten Schrägstrich (`\`).

8 Starten Sie die Zelle neu.

```
service vmware-vcd restart
```

9 [Veröffentlichen des Rechtepakets für die automatische Skalierung](#)

Veröffentlichen des Rechtepakets für die automatische Skalierung

Wenn Mandanten Anwendungen automatisch skalieren sollen, müssen Sie das Rechtepaket für eine oder mehrere Organisationen in Ihrem System veröffentlichen. Sie können die automatische Skalierung ab VMware Cloud Director 10.2.2 verwenden.

Voraussetzungen

[Konfigurieren und Veröffentlichen des Plug-Ins für automatische Skalierung](#)

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Rechtepakete** aus.
- 3 Stellen Sie sicher, dass keine **Legacy-Rechtepakete** für die Mandantenorganisationen vorhanden sind, denen Zugriff auf die automatische Skalierung gewährt werden soll.
- 4 Wählen Sie das Paket **vmware:scalegroup Entitlement** aus und klicken Sie auf **Veröffentlichen**.
- 5 So veröffentlichen Sie das Paket:
 - a Wählen Sie **An Mandanten veröffentlichen**.
 - b Wählen Sie die Organisationen aus, für welche die Rolle veröffentlicht werden soll.
 - Wenn Sie das Paket für alle vorhandenen und neu erstellten Organisationen in Ihrem System veröffentlichen möchten, aktivieren Sie **An alle Mandanten veröffentlichen**.
 - Wenn Sie das Paket für bestimmte Organisationen in Ihrem System veröffentlichen möchten, wählen Sie die Organisationen einzeln aus.
- 6 Klicken Sie auf **Speichern**.

Nächste Schritte

Fügen Sie die notwendigen **VMWARE:SCALEGROUP**-Rechte zu den Mandantenrollen hinzu, die Skalierungsgruppen verwenden sollen. Weitere Informationen finden Sie unter [Anzeigen und Bearbeiten einer globalen Mandantenrolle](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Überwachen der Integrität des VMware Cloud Director-Appliance-Datenbankclusters

Sie können Ihren VMware Cloud Director-Appliance-Cluster überwachen, indem Sie die Verwaltungsbenutzeroberfläche der VMware Cloud Director-Appliance, die Appliance-API oder die Open Source Tool Suite repmgr verwenden.

Sie können auch die Verwaltungsschnittstelle der VMware Cloud Director-Appliance verwenden, um den Failover-Modus der Appliance anzuzeigen. Der Failover-Modus gibt an, ob VMware Cloud Director bei einem Ausfall der primären Datenbank automatisch ein Datenbank-Failover auslöst oder ob das Failover manuell vom **Systemadministrator** initiiert werden muss.

Wenn der Failover-Modus knotenübergreifend inkonsistent ist, lautet der Failover-Modus auf `Indeterminate`. Der Modus `Indeterminate` kann zwischen den Knoten und den einer alten primären Zelle folgenden Knoten zu inkonsistenten Clusterzuständen führen. Sie müssen das Problem ermitteln und manuell beheben.

Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance

Sie können den Clusterzustand mithilfe der Verwaltungsschnittstelle der VMware Cloud Director-Appliance überwachen.

Sie können die Namen der Zellen in einem Cluster, die Rollen der Zellen, den Zellenstatus, den Namen der Zelle, der die Standby-Zellen folgen, und den Failover-Modus des Clusters mithilfe der Verwaltungsbenutzeroberfläche der VMware Cloud Director-Appliance oder der VMware Cloud Director-Appliance-API anzeigen. In diesem Verfahren werden die Schritte zum Überwachen des Clusterzustands der Appliance mithilfe der Verwaltungsbenutzeroberfläche beschrieben.

Verfahren

- 1 Melden Sie sich als **root** bei der Verwaltungsschnittstelle der Appliance unter `https://primary_eth1_ip_address:5480` an.
- 2 Wählen Sie im linken Bereich **Verfügbarkeit der eingebetteten Datenbank** aus.

Sie können die DNS-Kurznamen der Knoten, ihre Rollen, ihren Status, den Namen des zugehörigen Upstream-Knotens, d. h. den aktuellen primären Knoten, und die für die Knoten verfügbaren Aktionen anzeigen.

In der Spalte **Folgen** weist ein Fragezeichen (?) vor dem Hostnamen darauf hin, dass der aktuelle primäre Knoten nicht erreichbar ist. Ein Ausrufezeichen (!) vor dem Hostnamen weist darauf hin, dass die Metadaten des aktuellen primären Knotens nicht aktualisiert wurden und möglicherweise falsch sind oder dass der Knoten nicht an den aktuellen primären Knoten angehängt ist. Das Problem kann auftreten, wenn Sie den Knoten nach einer längeren Zeit der Inaktivität neu starten. Wenn der Knoten nicht an den primären Knoten angehängt werden kann, müssen Sie seine Registrierung aufheben und ihn durch einen neuen Standby-Knoten ersetzen.

3 Zeigen Sie den Clusterzustand an.

Clusterzustand	Beschreibung
Fehlerfrei	<p>Der Cluster befindet sich in einem fehlerfreien Zustand. Die primäre und beide Standby-Zellen sind online und betriebsbereit.</p> <p>Die Benutzeroberfläche und API von VMware Cloud Director sind funktionsfähig.</p>
Herabgestuft	<p>Der Cluster befindet sich in einem herabgestuften Zustand. Die primäre und eine der Standby-Zellen sind online und betriebsbereit. Die andere Standby-Zelle ist jedoch nicht funktionsfähig. Die primäre Datenbank ist in diesem Zustand funktionsfähig. Wenn jedoch ein weiterer Datenbankfehler bei einer der betriebsbereiten Zellen auftritt, funktioniert die primäre Datenbank nicht mehr. Die nicht funktionsfähige Standby-Zelle muss schnellstmöglich durch eine neue funktionierende Standby-Zelle ersetzt werden, damit der Cluster wieder den Zustand <code>Healthy</code> aufweist.</p> <p>Die Benutzeroberfläche und API von VMware Cloud Director sind funktionsfähig.</p>
No_Active_Primary	<p>Eine funktionierende primäre Datenbank steht nicht zur Verfügung. Wenn zwei betriebsbereite Standby-Zellen vorhanden sind, muss eine dieser Zellen zur neuen primären Zelle heraufgestuft werden. Wenn die Umgebung keine zwei betriebsbereiten Standby-Zellen enthält, müssen Sie das Problem ermitteln und manuell beheben.</p> <p>Die Benutzeroberfläche und die API von VMware Cloud Director sind nicht verfügbar.</p>
Read_Only_Primary	<p>Eine primäre Online-Datenbank ist vorhanden, weist aber den Status <code>Read_Only</code> auf, da die Umgebung keine betriebsbereite Standby-Zelle enthält. Zwei neue Standby-Zellen müssen bereitgestellt werden.</p> <p>Die Benutzeroberfläche und die API von VMware Cloud Director sind nicht verfügbar.</p>

Clusterzustand	Beschreibung
Critical_Problem	<p>Der Cluster befindet sich in einem inkonsistenten Zustand. Beispiel: Mehrere primäre Zellen sind online oder eine Standby-Zelle folgt der falschen primären Zelle. Sie müssen das Problem ermitteln und manuell beheben.</p> <p>Dieser Zustand kann sich auf die Verfügbarkeit der Benutzeroberfläche und der API von VMware Cloud Director auswirken.</p>
SSH_Problem	<p>Das SSH-Problem weist darauf hin, dass der postgres-Benutzer keine Verbindung zu seinen gleichrangigen Datenbankknoten über SSH herstellen kann. Sie müssen dieses kritische Problem schnellstmöglich beheben. Weitere Informationen finden Sie im Die Clusterintegrität weist auf ein SSH-Problem hin.</p> <p>Die VMware Cloud Director-Benutzeroberfläche und -API sind möglicherweise nicht voll funktionsfähig.</p>

4 Zeigen Sie den Failover-Modus der Appliance an.

Failover-Modus	Beschreibung
Automatisch	Bei einem Ausfall der primären Datenbank löst VMware Cloud Director automatisch ein Datenbank-Failover aus.
Manuell	Bei einem Ausfall der primären Datenbank müssen Sie mithilfe der Verwaltungsbenutzeroberfläche oder der Failover-API der VMware Cloud Director-Appliance ein Datenbank-Failover initiieren.
Unbestimmt	<p>Der Failover-Modus ist nicht über alle Knoten des Clusters hinweg konsistent. Sie müssen das Problem ermitteln und beheben. Setzen Sie <code>FailoverMode</code> mithilfe der VMware Cloud Director-Appliance-API entweder auf <code>Manual</code> oder auf <code>Automatic</code> zurück.</p> <p>Weitere Informationen finden Sie in den Erläuterungen zu <code>FailoverMode</code> unter <i>API-Schema-Referenz für VMware Cloud Director-Appliance</i>.</p>

Anzeigen des Dienststatus der VMware Cloud Director-Appliance

Sie können den Status der VMware Cloud Director-Appliance-Dienste mithilfe der Appliance-Verwaltungsbenutzeroberfläche von VMware Cloud Director überwachen.

Auf der Registerkarte „Dienste“ können Sie die Dienste `vmware-vcd`, `vpostgres` und `appliance-sync.timer` für die primären und Standby-Appliances sowie die Dienste `vmware-vcd` und `appliance-sync.timer` für Anwendungszellen überwachen.

Der Dienst `appliance-sync.timer` führt regelmäßig den `appliance-sync.service` aus, der relevante Informationen für alle Knoten im Datenbank-HA-Cluster oder in der VMware Cloud Director-Servergruppe freigibt. `appliance-sync.service` führt eine regelmäßige Prüfung und Synchronisierung der benötigten Dateien für die Funktionalität der VMware Cloud Director-Appliance durch, indem die Konfigurationsdateien der Appliances gelesen und in die Appliance-Gruppe geschrieben werden. Die ordnungsgemäßen Zustände des Timers sind `waiting` und `running`.

Verfahren

- 1 Melden Sie sich als **root** bei der Verwaltungsschnittstelle der Appliance unter `https://primary_eth1_ip_address:5480` an.
- 2 Wählen Sie im linken Fensterbereich die Registerkarte **Dienste** aus.
- 3 Zeigen Sie den Status der VMware Cloud Director-Dienste an.

Überprüfen des Verbindungsstatus eines Datenbank-Hochverfügbarkeits-Clusters

Sie können die Replication Manager-Tool-Suite verwenden, um die Konnektivität zwischen den Knoten in Ihrem Datenbank-Hochverfügbarkeits-Cluster zu überprüfen.

Verfahren

- 1 Melden Sie sich, bei Bedarf mithilfe von SSH, als **root** beim Betriebssystem einer der aktiven Zellen im Cluster an.
- 2 Ändern Sie den Benutzer in **postgres**.

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

- 3 Überprüfen Sie die Konnektivität des Clusters.
 - Mit dem Befehl `repmgr cluster matrix` wird der Befehl `repmgr cluster show` auf jedem Knoten des Clusters ausgeführt und das Ergebnis als Matrix angezeigt.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf cluster matrix
```

Im folgenden Beispiel sind Knoten 1 und Knoten 2 aktiv und Knoten 3 ist inaktiv. Jede Zeile entspricht einem Server und stellt das Ergebnis des Tests einer ausgehenden Verbindung von diesem Server dar.

Die drei Einträge in der dritten Zeile sind mit einem ?-Symbol markiert, da Knoten 3 nicht verfügbar ist und keine Informationen zu seinen ausgehenden Verbindungen vorhanden sind.

```

      Name| Id | 1 | 2 | 3
-----+-----+-----+-----
node 1 | 1 | * | * | x
node 2 | 2 | * | * | x
node 3 | 3 | ? | ? | ?

```

- Mit dem Befehl `repmgr cluster crosscheck` werden die Verbindungen zwischen den einzelnen Knotenkombinationen geprüft. Er liefert möglicherweise einen besseren Überblick über die Clusterkonnektivität.

```

/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/
repmgr.conf cluster crosscheck

```

Im folgenden Beispiel führt der Knoten, von dem aus Sie den Befehl `repmgr cluster crosscheck` ausführen, seine Clustermatrix-Systemausgabe mit der Ausgabe der anderen Knoten zusammen und führt eine Gegenkontrolle zwischen den Knoten durch. In diesem Fall sind alle Knoten aktiv, aber die Firewall verwirft Pakete, die von Knoten 1 stammen und an Knoten 3 gerichtet sind. Dies ist ein Beispiel für eine asymmetrische Netzwerkpartition, bei der Knoten 1 keine Pakete an Knoten 3 senden kann.

```

      Name| Id | 1 | 2 | 3
-----+-----+-----+-----
node 1 | 1 | * | * | x
node 2 | 2 | * | * | *
node 3 | 3 | * | * | *

```

Nächste Schritte

Um den gesamten Verbindungsstatus in Ihrem Datenbank-Hochverfügbarkeits-Cluster zu ermitteln, führen Sie diese Befehle auf jedem Knoten aus und vergleichen Sie die Ergebnisse.

Überprüfen des Replizierungsstatus eines Knotens in einem Datenbank-Hochverfügbarkeits-Cluster

Sie können die Replication Manager-Tool-Suite und das interaktive PostgreSQL-Terminal verwenden, um den Replizierungsstatus einzelner Knoten in einem Datenbank-Hochverfügbarkeits-Cluster zu überprüfen.

Verfahren

- 1 Melden Sie sich, bei Bedarf mithilfe von SSH, als `root` beim Betriebssystem eines der aktiven Knoten im Cluster an.
- 2 Ändern Sie den Benutzer in `postgres`.

```

sudo -i -u postgres

```

3 Überprüfen Sie den Replizierungsstatus des Knotens.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf
node status
```

Die Systemausgabe für den primären Knoten liefert Informationen zum Knoten, zur PostgreSQL-Version und zu den Replizierungsdetails. Beispiel:

```
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
```

Die Systemausgabe für einen Standby-Knoten liefert Informationen zum Knoten, zur PostgreSQL-Version, zu den Replizierungsdetails und zu einem Upstream-Knoten. Beispiel:

```
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 (Optional) Für detailliertere Informationen verwenden Sie das interaktive PostgreSQL-Terminal, in dem Sie den Replizierungsstatus der Knoten überprüfen können.

Das interaktive PostgreSQL-Terminal kann Informationen darüber liefern, ob die empfangenen Protokolldatensätze der Standby-Knoten hinter den vom primären Knoten gesendeten Protokollen zurückbleiben.

- a Stellen Sie eine Verbindung zum `psql`-Terminal her.

```
/opt/vmware/vpostgres/current/bin/psql
```

- b Um die Anzeige zu erweitern und die Abfrageergebnisse leichter lesbar zu machen, führen Sie den Befehl `set \x` aus.
- c Führen Sie eine Replizierungsstatusabfrage je nach der Rolle des Knotens aus.

Option	Aktion
Führen Sie eine Abfrage auf dem primären Knoten aus.	<code>select* from pg_stat_replication;</code>
Führen Sie eine Abfrage auf einem Standby-Knoten aus.	<code>select* from pg_stat_wal_receiver;</code>

Überprüfen des Status von VMware Cloud Director-Diensten

Sie können die Verwaltungsschnittstelle der VMware Cloud Director-Appliance verwenden, um den Status der VMware Cloud Director-Dienste für die Zelle anzuzeigen, bei der Sie angemeldet sind.

Verfahren

- 1 Melden Sie sich als **root** bei der Verwaltungsschnittstelle der Appliance unter `https://primary_eth1_ip_address:5480` an.

- 2 Zur Anzeige des Status der Dienste wählen Sie im linken Fensterbereich **Dienste** aus.

Wenn die VMware Cloud Director-Appliance ordnungsgemäß funktioniert, werden die Dienste `vmware-vcd` und `vpostgres` ausgeführt.

Nächste Schritte

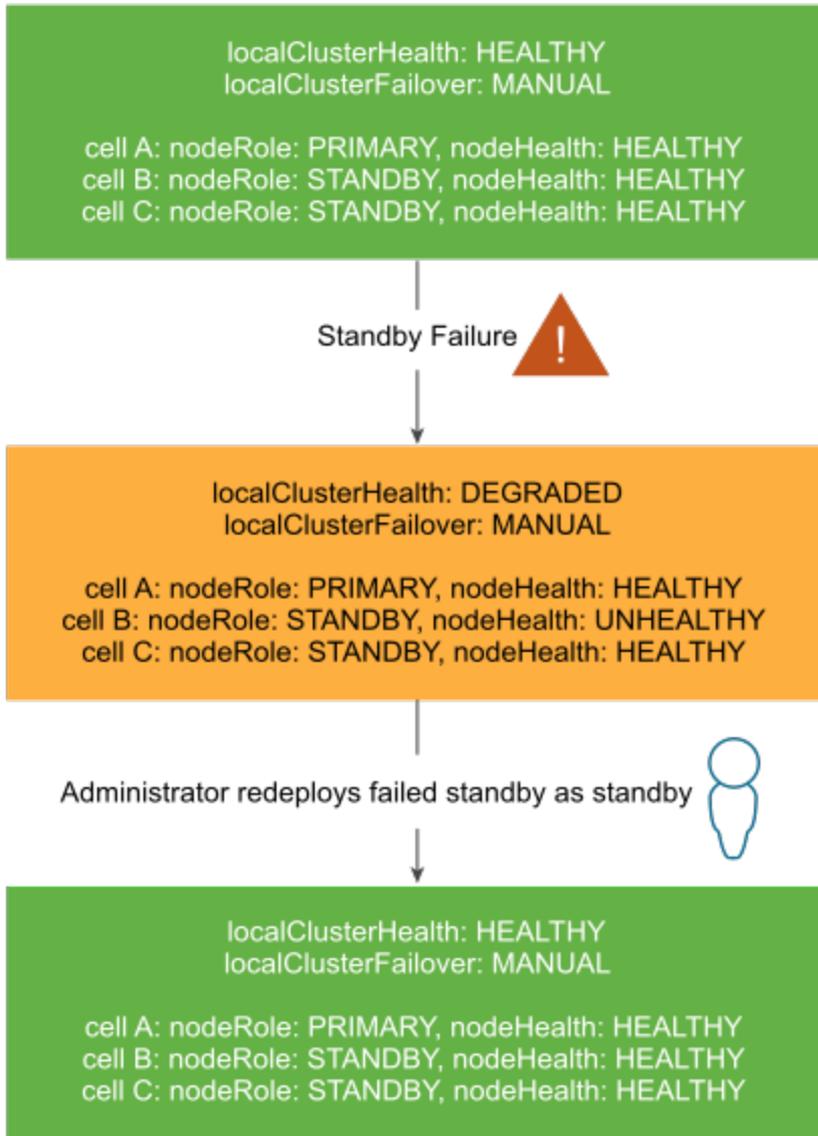
Wenn Sie den Status des `repmgrd`-Dienstes zu Debugging-Zwecken überprüfen müssen, müssen Sie die API der VMware Cloud Director-Appliance verwenden.

Wiederherstellung des Datenbankclusters der VMware Cloud Director-Appliance

Wenn bei der Datenbank oder einem der VMware Cloud Director-Knoten ein Fehler vorliegt, können Sie Ihren Datenbankcluster wiederherstellen.

Wenn eine Zelle im Hochverfügbarkeitscluster der Datenbank ausfällt, werden im Systemzustand des Clusters neben dem Fehler auch Lösungen zur Fehlerbehebung angegeben. Beispielsweise wird im Systemzustand des `Degraded`-Clusters ein Fehler mit einer Standby-Zelle angegeben. Ein Systemadministrator muss die fehlgeschlagene Zelle erneut bereitstellen.

Abbildung 3-4. Wiederherstellen nach einem Fehler in einer Standby-Zelle



Wenn eine primäre Zelle im Hochverfügbarkeitscluster der Datenbank ausfällt, kann sich der Zustand des Clusters in `No_Active_Primary` ändern. Hiermit wird angegeben, dass die fehlgeschlagene primäre Zelle vom Systemadministrator repariert werden muss.

Wiederherstellen nach einem Ausfall der primären Zelle in einem Hochverfügbarkeits-Cluster

Wenn die primäre Zelle nicht ordnungsgemäß ausgeführt wird, muss zur Wiederherstellung der VMware Cloud Director-Datenbank eine der Standby-Zellen zur neuen primären Zelle werden, und Sie müssen eine neue Standby-Zelle bereitstellen. Je nach Fehlermodus stuft die VMware Cloud Director-Appliance automatisch eine Standby-Zelle zur neuen primären Zelle herauf, oder Sie müssen sie manuell heraufstufen.

Je nach Failover-Modus der VMware Cloud Director-Appliance gibt es zwei verschiedene Workflows für die Wiederherstellung nach einem Ausfall der primären Zelle. Mithilfe dieser Workflows können Sie die IP-Adressen und den Hostnamen der fehlgeschlagenen primären Zelle wiederverwenden, wenn Sie die neue Standby-Zelle bereitstellen.

Wiederherstellungs-Workflow für Failover-Modus „Manuell“

Wenn sich die primäre Zelle im Zustand `Not reachable` oder `Failed` befindet und die beiden Standby-Zellen im Zustand `Running` ausgeführt werden, können Sie eine Wiederherstellung nach dem Ausfall mithilfe der HTML5-Benutzeroberfläche der Appliance und der VMware Cloud Director-Appliance-API vornehmen.

Informationen zum Anzeigen des Zustands der Zellen im Cluster finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

- 1 Fahren Sie den VMware Cloud Director-Prozess mithilfe des Zellenverwaltungstools herunter wenn möglich. Führen Sie in der fehlgeschlagenen primären Zelle den folgenden Befehl aus:

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

- 2 Schalten Sie die fehlgeschlagene primäre VM aus.
- 3 Stufen Sie eine Standby-Zelle zur neuen primären Zelle herauf.
 - a Melden Sie sich als **root** bei der Appliance-Verwaltungsbenutzeroberfläche einer aktiven Standby-Zelle an: `https://standby_ip_address:5480`.
 - b Klicken Sie in der Spalte **Rolle** für die Standby-Zelle, die zur neuen primären Zelle werden soll, auf **Heraufstufen**.

Die Verwaltungsbenutzeroberfläche zeigt zwei Zellen mit der Rolle `Primär` an. Die ursprüngliche primäre Zelle hat den Status `Fehlgeschlagen`, und die neue primäre Zelle weist den Status `Wird ausgeführt` auf. Die Clusterintegrität ist `Herabgestuft`.

- 4 Entfernen Sie aus einer beliebigen anderen Zelle, die nicht der fehlgeschlagenen primären Zelle entspricht, mithilfe der API-Methode `Unregister` der Appliance die fehlgeschlagene primäre Appliance aus dem `repmgr`-Hochverfügbarkeitscluster. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API-Dokumentation](#).

- 5 Entfernen Sie die fehlgeschlagene primäre Appliance aus der VMware Cloud Director-Servergruppe.
 - a Melden Sie sich als **Administrator** beim Service Provider Admin Portal an.
 - b Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - c Klicken Sie im linken Bereich auf **Cloud-Zellen**.
 - d Wählen Sie die inaktive Zelle aus und klicken Sie auf **Registrierung aufheben**.
- 6 Wenn Sie die IP-Adresse und den Hostnamen der fehlgeschlagenen primären Appliance wiederverwenden möchten, stellen Sie sicher, dass die fehlgeschlagene primäre Appliance ausgeschaltet bleibt, oder verwenden Sie den vSphere Client zum Löschen dieser Appliance.
- 7 Stellen Sie eine neue Standby-Appliance bereit. Sie können [Starten der Bereitstellung der VMware Cloud Director-Appliance](#) oder [Bereitstellen der VMware Cloud Director-Appliance mit dem VMware OVF Tool](#).

Nach der Bereitstellung der neuen Standby-Appliance muss die Clusterintegrität auf `Fehlerfrei` lauten.
- 8 Wenn der FIPS-Modus der VMware Cloud Director-Appliance vor der Wiederherstellung aktiviert war, müssen Sie ihn mithilfe der API der VMware Cloud Director-Appliance erneut festlegen.

Der FIPS-Modus der Zelle wird automatisch wiederhergestellt.

Wiederherstellung für Failover-Modus „Automatisch“

Wenn sich die primäre Zelle im Zustand `Failed` befindet, stuft VMware Cloud Director automatisch eine Standby-Zelle zur neuen aktiven primären Zelle herauf, aber der Cluster befindet sich im Zustand `Herabgestuft`, weil nur eine aktive Standby-Zelle vorhanden ist. Sie können mithilfe der HTML5-Benutzeroberfläche und der VMware Cloud Director-Appliance-API eine Wiederherstellung nach dem Ausfall vornehmen.

Informationen zum Anzeigen des Zustands der Zellen im Cluster finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

- 1 Fahren Sie den VMware Cloud Director-Prozess mithilfe des Zellenverwaltungstools herunter, wenn möglich. Führen Sie in der fehlgeschlagenen primären Zelle den folgenden Befehl aus:

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

- 2 Schalten Sie die fehlgeschlagene primäre VM aus.

Die Verwaltungsbenutzeroberfläche zeigt zwei Zellen mit der Rolle `Primär` an. Die ursprüngliche primäre Zelle hat den Status `Fehlgeschlagen`, und die neue primäre Zelle weist den Status `Wird ausgeführt auf`. Die Clusterintegrität ist `Herabgestuft`.

- 3 Entfernen Sie aus einer beliebigen anderen Zelle, die nicht der fehlgeschlagenen primären Zelle entspricht, mithilfe der API-Methode `Unregister` der Appliance die fehlgeschlagene primäre Appliance aus dem `repmgr`-Hochverfügbarkeitscluster. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API-Dokumentation](#).
- 4 Entfernen Sie die fehlgeschlagene primäre Appliance aus der VMware Cloud Director-Servergruppe.
 - a Melden Sie sich als **Administrator** beim Service Provider Admin Portal an.
 - b Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - c Klicken Sie im linken Bereich auf **Cloud-Zellen**.
 - d Wählen Sie die inaktive Zelle aus und klicken Sie auf **Registrierung aufheben**.
- 5 Wenn Sie die IP-Adresse und den Hostnamen der fehlgeschlagenen primären Appliance wiederverwenden möchten, stellen Sie sicher, dass die fehlgeschlagene primäre Appliance ausgeschaltet ist, oder verwenden Sie den vSphere Client zum Löschen dieser Appliance.
- 6 Stellen Sie eine neue Standby-Appliance bereit. Sie können [Starten der Bereitstellung der VMware Cloud Director-Appliance](#) oder [Bereitstellen der VMware Cloud Director-Appliance mit dem VMware OVF Tool](#). Nach der Bereitstellung der neuen Standby-Appliance muss die Clusterintegrität auf `Fehlerfrei` lauten.
- 7 Verwenden Sie in einer beliebigen anderen Zelle, die nicht mit der fehlgeschlagenen primären Zelle übereinstimmt, die API-Methode `Failover` der Appliance, um den Failover-Modus des Clusters auf `Automatic` festzulegen. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API-Dokumentation](#).
- 8 Wenn der FIPS-Modus der VMware Cloud Director-Appliance vor der Wiederherstellung aktiviert war, müssen Sie ihn mithilfe der API der VMware Cloud Director-Appliance erneut festlegen.

Der FIPS-Modus der Zelle wird automatisch wiederhergestellt.

Wiederherstellen nach einem Ausfall einer Standby-Zelle in einem Hochverfügbarkeits-Cluster

Wenn eine Standby-Zelle nicht ordnungsgemäß ausgeführt wird, können Sie eine Wiederherstellung nach dem Ausfall durchführen, indem Sie eine neue Standby-Zelle bereitstellen.

Wenn sich eine der Standby-Zellen im Zustand `Not reachable` oder `Failed` befindet, können Sie eine neue Zelle bereitstellen. Informationen zum Anzeigen des Zustands der Zellen im Cluster finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

Mithilfe dieses Workflows können Sie die IP-Adressen und den Hostnamen der fehlgeschlagenen Standby-Zelle wiederverwenden, wenn Sie die neue Standby-Zelle bereitstellen.

- 1 Fahren Sie den VMware Cloud Director-Prozess gegebenenfalls mithilfe des Zellenverwaltungstools herunter. Führen Sie in der fehlgeschlagenen Standby-Zelle den folgenden Befehl aus:

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

- 2 Schalten Sie die fehlgeschlagene Standby-VM aus.
- 3 Entfernen Sie aus einer beliebigen anderen Zelle, die nicht der fehlgeschlagenen Standby-Zelle entspricht, mithilfe der API-Methode `Unregister` der Appliance die fehlgeschlagene Standby-Zelle aus dem repmgr-Hochverfügbarkeitscluster. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API-Dokumentation](#).
- 4 Verwenden Sie das Service Provider Admin Portal, um die fehlgeschlagene Standby-Appliance aus der VMware Cloud Director-Servergruppe zu entfernen.
 - a Wählen Sie in der oberen Navigationsleiste unter **Ressourcen Cloud-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **Cloud-Zellen**.
 - c Wählen Sie eine inaktive Zelle aus und klicken Sie auf **Registrierung aufheben**.
- 5 Wenn Sie die IP-Adresse und den DNS-Namen der fehlgeschlagenen Standby-Zelle wiederverwenden möchten, müssen Sie sicherstellen, dass die fehlgeschlagene Standby-Appliance ausgeschaltet bleibt oder gelöscht wird.
- 6 Stellen Sie eine neue Standby-Appliance bereit. Sie können [Starten der Bereitstellung der VMware Cloud Director-Appliance](#) oder [Bereitstellen der VMware Cloud Director-Appliance mit dem VMware OVF Tool](#).

Nach der Bereitstellung der neuen Standby-Appliance muss die Clusterintegrität auf Fehlerfrei lauten.

- 7 Verwenden Sie zum Zurücksetzen des Failover-Modus des Clusters auf `Automatic` in einer beliebigen anderen als der fehlgeschlagenen Standby-Zelle die API-Methode `Failover` der Appliance. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API-Dokumentation](#).

Weitere Informationen zum automatischen Failover-Modus finden Sie unter [Automatisches Failover der VMware Cloud Director-Appliance](#).

- 8 Wenn der FIPS-Modus der VMware Cloud Director-Appliance vor der Wiederherstellung aktiviert war, müssen Sie ihn mithilfe der API der VMware Cloud Director-Appliance erneut festlegen.

Der FIPS-Modus der Zelle wird automatisch wiederhergestellt.

Aufheben der Registrierung einer fehlgeschlagenen primären oder Standby-Zelle in einem Hochverfügbarkeits-Datenbankcluster

Wenn der primäre oder Standby-Knoten in Ihrem Hochverfügbarkeits-Datenbankcluster fehlschlägt, können Sie die VMware Cloud Director-API zum Aufheben der Registrierung des fehlgeschlagenen Knotens verwenden, um ihn aus dem Cluster zu entfernen und inkonsistente Clusterstatusdaten zu vermeiden.

Weitere Informationen zur Verwendung der VMware Cloud Director-API finden Sie im Abschnitt zur `UNREGISTER`-API-Methode in der Dokumentation zur VMware Cloud Director-Appliance-API unter <https://developer.vmware.com/>.

Voraussetzungen

- Vergewissern Sie sich, dass der Knoten, dessen Registrierung Sie aufheben möchten, inaktiv ist, und notieren Sie sich seinen Namen. Informationen zum Status der Zellen und zum Namen der Zelle, auf die die Standby-Zellen folgen, finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).
- Wenn Sie die Registrierung eines primären Knotens aufheben möchten, stellen Sie sicher, dass der fehlgeschlagene primäre Knoten inaktiv ist und keine nachfolgenden Standby-Knoten aufweist, und stufen Sie einen neuen primären Knoten herauf.

Verfahren

- ◆ Zum Entfernen des inaktiven Knotens stellen Sie eine Löschanforderung auf einem aktiven Knoten, auf dem der Befehl ausgeführt werden soll.

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

Behebung von Fehlern der Appliance

Wenn die Bereitstellung der VMware Cloud Director-Appliance fehlschlägt oder die Appliance nicht ordnungsgemäß funktioniert, können Sie die Protokolldateien der Appliance prüfen, um die Ursache des Problems zu ermitteln.

Der technische Support von VMware fordert routinemäßig Diagnoseinformationen zur Bearbeitung von Support-Anfragen an. Sie können das `vmware-vcd-support`-Skript zum Erfassen von Hostprotokolldaten und VMware Cloud Director-Protokollen verwenden. Weitere Informationen zum Erfassen von Diagnoseinformationen für VMware Cloud Director finden Sie unter <https://kb.vmware.com/s/article/1026312>. Bei Ausführung des `vmware-vcd-support`-Skripts enthalten die Protokolle unter Umständen Informationen zu außer Betrieb genommenen oder ersetzten Zellen mit dem Status `FAIL`. Weitere Informationen finden Sie unter <https://kb.vmware.com/s/article/71349>.

Prüfen der Protokolldateien in der VMware Cloud Director-Appliance

Nach der Bereitstellung der VMware Cloud Director-Appliance können Sie die „firstboot“- und Datenbankprotokolle auf Fehler und Warnungen prüfen.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der VMware Cloud Director-Appliance als **root** an.
- 2 Navigieren Sie zu `/opt/vmware/var/log`.
- 3 Prüfen Sie die Protokolldateien.
 - Die Datei `firstboot` enthält Protokollierungsinformationen im Zusammenhang mit dem ersten Start der Appliance.
 - Das Verzeichnis `/opt/vmware/var/log/vcd/` enthält Protokolle im Zusammenhang mit der Einrichtung der Tool-Suite Replication Manager (repmgr) und der Neukonfiguration und Appliance-Synchronisierung.
 - Das Verzeichnis `/opt/vmware/var/log/vcd/pg/` enthält Protokolle, die sich auf die Sicherung der eingebetteten Appliance-Datenbank beziehen.
 - Die Datei `/opt/vmware/etc/vami/ovfEnv.xml` enthält die OVF-Parameter der Bereitstellung.

Die VMware Cloud Director-Zelle kann nach der Bereitstellung der Appliance nicht gestartet werden

Sie haben die VMware Cloud Director-Appliance erfolgreich bereitgestellt, aber die VMware Cloud Director-Dienste werden möglicherweise nicht gestartet.

Problem

Der `vmware-vcd`-Dienst ist nach der Bereitstellung der Appliance inaktiv.

Ursache

Wenn Sie eine primäre Zelle bereitgestellt haben, kann es vorkommen, dass die VMware Cloud Director-Dienste aufgrund eines vorab belegten gemeinsam genutzten NFS-Übertragungsdienstspeichers nicht gestartet werden. Bevor Sie die primäre Appliance bereitstellen, darf der Übertragungsdienstspeicher keine `responses.properties`-Datei und kein `appliance-nodes`-Verzeichnis enthalten.

Wenn Sie eine Standby-oder vCD-Anwendungszelle bereitgestellt haben, können die VMware Cloud Director-Dienste aufgrund einer fehlenden `responses.properties`-Datei im gemeinsam genutzten NFS-Übertragungsspeicher nicht gestartet werden. Bevor Sie eine Standby-oder vCD-Anwendungs-Appliance bereitstellen, muss der gemeinsam genutzte Übertragungsspeicher die `responses.properties`-Datei enthalten.

Hinweis Wenn Ihr Cluster für automatisches Failover konfiguriert ist, müssen Sie nach der Bereitstellung einer zusätzlichen oder mehrerer zusätzlicher Zellen die Appliance-API verwenden, um den Failover-Modus auf `Automatic` zurückzusetzen. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API](#). Der standardmäßige Failover-Modus für neue Zellen lautet `Manual`. Wenn der Failover-Modus für die Knoten des Clusters inkonsistent ist, lautet der Failover-Modus des Clusters `Indeterminate`. Der Modus `Indeterminate` kann zwischen den Knoten und den einer alten primären Zelle folgenden Knoten zu inkonsistenten Clusterzuständen führen. Informationen zum Anzeigen des Failover-Modus des Clusters finden Sie unter [Anzeigen des Clusterzustands und des Failover-Modus der VMware Cloud Director-Appliance](#).

Lösung

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der VMware Cloud Director-Appliance als `root` an.
- 2 Prüfen Sie das Protokoll `/opt/vmware/var/log/vcd/setupvcd.log` auf Fehlermeldungen bezüglich des NFS-Speichers.
- 3 Bereiten Sie den NFS-Speicher für den Appliance-Typ vor.
- 4 Stellen Sie die Zelle erneut bereit.

Die Wiederherstellung nach der NFS-Validierung schlägt während der anfänglichen Konfiguration der Appliance fehl

Wenn die Validierung des freigegebenen Speichers während der anfänglichen Konfiguration der VMware Cloud Director-Appliance fehlschlägt, zeigt der Bereitsteller Fehlermeldungen an, mit denen Sie das Problem beheben können.

Problem

Während der Bereitstellung der VMware Cloud Director-Appliance zeigt der Bereitsteller eine Fehlermeldung an, die sich auf die NFS-Freigabe bezieht.

Ursache

Wenn Sie den Übertragungsserverspeicher nicht für VMware Cloud Director vorbereiten, schlägt die NFS-Validierung während der Bereitstellung fehl.

Lösung

Version	Fehler	Aktion
10.2	<code>/opt/vmware/vcloud-director/data/transfer/xyz</code> ist im Besitz eines unbekanntes Benutzers mit der UID 999; erwartet: 1003	Überprüfen Sie die Konfiguration der Benutzer-ID des Benutzers vcloud auf dem NFS-Server. Die ID des Benutzers vcloud muss auf dem NFS-Server und der Appliance mit demselben Wert angegeben werden.
10.2	<code>/opt/vmware/vcloud-director/data/transfer/xyz</code> ist im Besitz eines unbekanntes Benutzers mit der GID 999; erwartet: 1002	Überprüfen Sie die Konfiguration der Gruppen-ID des Benutzers vcloud auf dem NFS-Server. Die ID des Benutzers vcloud muss auf dem NFS-Server und der Appliance mit demselben Wert angegeben werden.
10.2	Die Datei auf der Übertragungsfreigabe kann nicht geändert werden	Stellen Sie fest, warum die Appliance nicht auf der gemounteten NFS-Freigabe schreiben kann. Um zu überprüfen, warum die Freigabe nicht beschreibbar ist, versuchen Sie, die NFS-Freigabe mit einer anderen Linux-Maschine zu mounten.
10.2	Zeitüberschreitung bei <code>/usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test</code> . Dauer: 5 Sekunden	Stellen Sie fest, warum diese Appliance die angegebene NFS-Freigabe nicht innerhalb von 5 Sekunden mounten kann. Um zu bestätigen, dass die NFS-Freigabe nicht zeitnah gemountet werden kann, versuchen Sie, sie mit einer anderen Linux-Maschine zu mounten. Überprüfen Sie alternativ die Exporteinstellungen des NFS-Servers für diese NFS-Freigabe.
10.2	Fehler bei <code>/usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test</code>	Stellen Sie fest, warum diese Appliance die angegebene NFS-Freigabe nicht mounten kann. Um zu bestätigen, dass die NFS-Freigabe nicht gemountet werden kann, versuchen Sie, sie mit einer anderen Linux-Maschine zu mounten. Überprüfen Sie alternativ die Exporteinstellungen des NFS-Servers für diese NFS-Freigabe.
10.2	Übertragungsfreigabeverzeichnis ist nicht vorhanden: <code>/opt/vmware/vcloud-director/data/transfer</code>	Das Übertragungsfreigabeverzeichnis oder der Mount-Punkt ist nicht vorhanden. Erstellen Sie dieses Verzeichnis.

Version	Fehler	Aktion
10.2	Unerwartete Berechtigungen für die Datei „/opt/vmware/vcloud-director/data/transfer/xyz“ während des Vorgangs: touch xyz. Erwartet: root root 644. Gefunden: root, root, 600	Stellen Sie fest, warum der Dateibesitzer, die Gruppe oder die Berechtigungen von den erwarteten Werten abweichen, nachdem der angegebene Vorgang auf der NFS-Übertragungsfreigabe ausgeführt wurde. Beheben Sie das Problem.
10.2	Die Uhrzeit des NFS-Servers ist nicht mehr synchron mit der Uhrzeit der Appliance. Der Zeitunterschied beträgt 3 Minuten, 12 Sekunden.	Überprüfen Sie die Uhrzeiteinstellungen auf dem NFS-Server und der Appliance. Wenn eine oder beide Einstellungen nicht korrekt sind, setzen Sie sie auf die korrekte Uhrzeit und stellen Sie sicher, dass Sie mithilfe von NTP synchronisiert werden.
10.2	Unerwartete Berechtigungen für die Datei „/opt/vmware/vcloud-director/data/transfer/xyz“ während des Vorgangs: chmod xyz. Erwartet: root root 750. Gefunden: root, root, 700	Stellen Sie fest, warum der Dateibesitzer, die Gruppe oder die Berechtigungen von den erwarteten Werten abweichen, nachdem der angegebene Vorgang auf der NFS-Übertragungsfreigabe ausgeführt wurde. Beheben Sie das Problem.
10.2	Unerwartete Berechtigungen für die Datei „/opt/vmware/vcloud-director/data/transfer/xyz“ während des Vorgangs: chown xyz. Erwartet: root root 750. Gefunden: root, root, 700	Stellen Sie fest, warum der Dateibesitzer, die Gruppe oder die Berechtigungen von den erwarteten Werten abweichen, nachdem der angegebene Vorgang auf der NFS-Übertragungsfreigabe ausgeführt wurde. Beheben Sie das Problem.
10.2 und höher	Ungültige oder fehlende Befehlsargumente. Nutzung: <code>nfsValidate nfs_mount_string</code>	Der JSON-Anforderungstext kann nicht analysiert werden. Geben Sie einen gültigen JSON-Anforderungstext an.
10.2 und höher	Leere <code>nfs_mount</code> -Zeichenfolge	Der Anforderungstext enthält keine NFS-Mount-Zeichenfolge. Geben Sie ein Argument für die NFS-Mount-Zeichenfolge an.
10.2 und höher	Ungültige <code>nfs_mount</code> -Zeichenfolge: <code>nfs_mount_string_argument</code>	Ändern Sie die NFS-Mount-Zeichenfolge in das gültige Format <code>IP_address: path</code>
10.2 und höher	Ungültiger Zellentyp: <code>cell_type_string</code>	Der Zellentyp muss <code>primary</code> , <code>standby</code> oder <code>cell</code> sein. Wenn der OVF-Parameter keinem dieser Werte entspricht, überprüfen Sie die Konfiguration der Appliance.

Version	Fehler	Aktion
10.2 und höher	Die vorausgesetzte Konfiguration des Betriebssystems wurde nicht abgeschlossen.	Die Datei /opt/vmware/appliance/etc/os-configuration-completed fehlt in der Appliance. Konfigurieren Sie das Betriebssystem.
10.2 und höher	Die Systeminstallation der Cloud Director-Appliance ist bereits abgeschlossen.	Die Datei /opt/vmware/appliance/etc/vcd-configuration-completed wurde in der Appliance gefunden. Die Cloud Director-Installation ist bereits abgeschlossen. Sie dürfen dieses Skript nicht ausführen.
10.2 und höher	Das Verzeichnis „10.150.170.3:/data/transfer/cells“ ist bereits vorhanden. Die primäre Appliance erfordert, dass es entfernt wird.	Dieses Verzeichnis darf nicht auf der primären Appliance vorhanden sein. Das Verzeichnis ist auf dem NFS-Server vorhanden. Sie müssen es entfernen.
10.2 und höher	Das Verzeichnis „10.150.170.3:/data/transfer/appliance-nodes“ ist bereits vorhanden. Die primäre Appliance erfordert, dass es entfernt wird.	Dieses Verzeichnis darf nicht auf der primären Appliance vorhanden sein. Das Verzeichnis ist auf dem NFS-Server vorhanden. Sie müssen es entfernen.
10.2 und höher	Die Datei „responses.properties“ ist bereits auf der Übertragungsfreigabe vorhanden. Die primäre Appliance erfordert, dass es entfernt wird.	Die responses.properties-Dateien dürfen nicht auf der primären Appliance vorhanden sein. Sie müssen sie entfernen.
10.2 und höher	Die Datei „responses.properties“ fehlt auf der Übertragungsfreigabe. Sie sollte bereits auf einer Standby- oder Zellen-Appliance vorhanden sein.	Auf einer Standby- oder Zellen-Appliance muss die Datei responses.properties vorhanden sein. Die primäre Appliance ist möglicherweise noch nicht konfiguriert. Sie müssen die primäre Appliance konfigurieren, bevor Sie zusätzliche Zellen konfigurieren.
10.2 und höher	„nfsValidate“ kann nicht ausgeführt werden, während das System eingerichtet wird.	Warten Sie, bis die Systeminstallation abgeschlossen ist, bevor Sie versuchen, nfsValidate zu starten.
10.2 und höher	Das tmp-Verzeichnis für die Verwendung durch das folgende Skript konnte nicht erstellt werden: /opt/vmware/vcloud-director/data/nfs-test	Überprüfen Sie die Dateisystemberechtigungen, um festzustellen, warum dieses Verzeichnis nicht erstellt werden kann.

Version	Fehler	Aktion
10.2.1	Die Datei kann auf der angegebenen NFS-Freigabe nicht erstellt werden. Möglicherweise ist sie nicht beschreibbar. Dies kann darauf zurückzuführen sein, dass das exportierte NFS-Dateisystem schreibgeschützt ist oder „no_root_squash“ nicht angegeben wurde.	Stellen Sie fest, warum die Appliance nicht auf der gemounteten NFS-Freigabe schreiben kann. Um zu überprüfen, warum die Freigabe nicht beschreibbar ist, versuchen Sie, die NFS-Freigabe mit einer anderen Linux-Maschine zu mounten.
10.2.1	Für die Datei auf der angegebenen Übertragungsfreigabe kann kein chmod-Vorgang ausgeführt werden	Stellen Sie fest, warum die Appliance die Zugriffsberechtigungen von Dateisystemobjekten auf der gemounteten NFS-Freigabe nicht ändern kann. Versuchen Sie, die NFS-Freigabe mithilfe einer anderen Linux-Maschine zu mounten.
10.2.1	Für die Datei auf der angegebenen Übertragungsfreigabe kann kein chown-Vorgang ausgeführt werden	Stellen Sie fest, warum die Appliance den Besitzer von Dateisystemobjekten auf der gemounteten NFS-Freigabe nicht ändern kann. Versuchen Sie, die NFS-Freigabe mithilfe einer anderen Linux-Maschine zu mounten.
10.2.1	Beim Mounten ist eine Zeitüberschreitung aufgetreten	Stellen Sie fest, warum diese Appliance die angegebene NFS-Freigabe nicht innerhalb von 5 Sekunden mounten kann. Um zu bestätigen, dass die NFS-Freigabe nicht zeitnah gemountet werden kann, versuchen Sie, sie mit einer anderen Linux-Maschine zu mounten. Überprüfen Sie alternativ die Exporteinstellungen des NFS-Servers für diese NFS-Freigabe.
10.2.1	Beim Mounten ist ein Fehler aufgetreten	Stellen Sie fest, warum diese Appliance die angegebene NFS-Freigabe nicht mounten kann. Um zu bestätigen, dass die NFS-Freigabe nicht gemountet werden kann, versuchen Sie, sie mit einer anderen Linux-Maschine zu mounten. Überprüfen Sie alternativ die Exporteinstellungen des NFS-Servers für diese NFS-Freigabe.

Version	Fehler	Aktion
10.2.1	Die angegebene NFS-Freigabe ist im Besitz eines unbekanntes Benutzers mit UID 123. Es wurde „root“ erwartetDie angegebene NFS-Freigabe ist im Besitz einer unbekanntes Gruppe mit GID 456. Es wurde „root“ erwartet	Stellen Sie fest, warum der erwartete Dateibesitzer, die Gruppe oder beide von den erwarteten Werten abweichen, nachdem der angegebene Vorgang auf der NFS-Übertragungsfreigabe ausgeführt wurde, und beheben Sie das Problem.
10.2.1	Unerwarteter Besitz und/oder unerwartete Berechtigungen auf angegebener NFS-Freigabe. Erwartet: root:root mit Modus: 750. Gefunden: root:root mit Modus 777	Stellen Sie fest, warum einige oder alle der erwarteten Werte für den Dateibesitzer, die Gruppe und den Modus nicht den erwarteten Werten entsprechen, nachdem der angegebene Vorgang auf der NFS-Übertragungsfreigabe ausgeführt wurde. Beheben Sie das Problem.
10.2.1	Die Uhrzeit des NFS-Servers ist nicht mehr synchron mit der Uhrzeit der Appliance. Der Zeitunterschied beträgt: 1:55:14.603510	Überprüfen Sie die Uhrzeiteinstellungen auf dem NFS-Server und der Appliance. Wenn eine oder beide Einstellungen nicht korrekt sind, setzen Sie sie auf die korrekte Uhrzeit und stellen Sie sicher, dass Sie mithilfe von NTP synchronisiert werden.

Neukonfigurieren des VMware Cloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der VMware Cloud Director-Appliance fehl

Wenn Sie die VMware Cloud Director-Appliance migrieren oder wiederherstellen, schlägt die Ausführung des Befehls `configure` unter Umständen fehl.

Problem

Während der Migration oder Wiederherstellung von VMware Cloud Director in einer neuen Umgebung der VMware Cloud Director-Appliance führen Sie den Befehl `configure` aus, um den VMware Cloud Director-Dienst in jeder neuen Zelle neu zu konfigurieren. Der Befehl `configure` schlägt unter Umständen mit der Fehlermeldung `sun.security.validator.ValidatorException: Validierung des PKIX-Pfads fehlgeschlagen: java.security.cert.CertPathValidatorException: Signaturprüfung fehlgeschlagen` fehl.

Lösung

- 1 Führen Sie den Befehl in der Zielzelle aus.

```
sed -i '/vcd_ova.crt/ s/$/ --force /' /opt/vmware/appliance/bin/appliance-sync.sh
```

2 Warten Sie 1 Minute und führen Sie den Befehl `configure` erneut aus.

Der Standby-Knoten einer VMware Cloud Director-Appliance ist nicht mehr erreichbar

VMware Cloud Director erhält die synchrone Streaming-Replizierung zwischen den Knoten aufrecht. Wenn ein Standby-Knoten nicht mehr erreichbar ist, müssen Sie die Ursache ermitteln und das Problem beheben.

Problem

Die Verwaltungsbensutzeroberfläche der VMware Cloud Director-Appliance zeigt die Clusterintegrität als `DEGRADED` an, und der Status eines der Standard-Knoten lautet `nicht erreichbar`.

Die `/nodes`-API gibt die folgenden Informationen zurück: `localClusterHealth` ist `DEGRADED`, der `status` des Knotens lautet `nicht erreichbar` und `nodeHealth` ist `UNHEALTHY`.

Beispiel: Die `/nodes`-API gibt möglicherweise die folgenden Informationen für den Knoten zurück.

```
{
  "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"
]
}

```

Ursache

Um die Datenintegrität zu gewährleisten, verwendet die PostgreSQL-Datenbank Write-Ahead Logging (WAL). Der primäre Knoten streamt WAL zu Replizierungs- und Wiederherstellungszwecken konstant zu den aktiven Standby-Knoten. Die Standby-Knoten verarbeiten WAL, wenn sie es empfangen. Wenn ein Standby-Knoten nicht erreichbar ist, empfängt er kein WAL mehr und kann kein Kandidat für die Heraufstufung zum neuen primären Knoten mehr sein.

Lösung

- ◆ Vergewissern Sie sich, dass die virtuelle Maschine des nicht erreichbaren Standby-Knotens ausgeführt wird.
- ◆ Vergewissern Sie sich, dass die Netzwerkverbindung zum Standby-Knoten funktioniert.
- ◆ Vergewissern Sie sich, dass kein SSH-Problem vorliegt, das die Kommunikation des Standby-Knotens mit den anderen Knoten verhindern könnte.
- ◆ Vergewissern Sie sich, dass der vpostgres-Dienst auf dem Standby-Knoten ausgeführt wird.

Nächste Schritte

Informationen zur Überprüfung, ob Netzwerk- oder SSH Probleme vorliegen, finden Sie unter [Überprüfen des Verbindungsstatus eines Datenbank-Hochverfügbarkeits-Clusters](#).

Der Standby-Knoten einer VMware Cloud Director-Appliance ist nicht mehr angehängt

VMware Cloud Director erhält die synchrone Streaming-Replizierung zwischen den Knoten aufrecht. Wenn ein Standby-Knoten nicht mehr angehängt ist, müssen Sie die Ursache ermitteln und das Problem beheben.

Problem

Die Verwaltungsbeneoberfläche der VMware Cloud Director-Appliance zeigt die Clusterintegrität als `DEGRADED` an, der Status eines der nicht angehängten Standard-Knoten lautet `wird ausgeführt` und ein Ausrufezeichen (!) wird vor dem Namen des Upstream-Knotens für das Standby angezeigt.

Das PostgreSQL-Protokoll zeigt, dass der primäre Knoten ein WAL-Segment gelöscht hat.

```
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 000000110000002100000080 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 000000110000002100000080 has already been removed
```

Die `/nodes-API` gibt die folgenden Information zurück: `localClusterHealth` ist `DEGRADED`, der `status` des Knotens lautet `wird ausgeführt` und `nodeHealth` ist `HEALTHY`. Ein Ausrufezeichen (!) wird vor dem Namen des Upstream-Knotens für das Standby angezeigt und die `/nodes-API` gibt eine Warnmeldung zurück, dass der Standby-Knoten nicht an seinen Upstream-Knoten angehängt ist.

Beispiel: Die `/nodes`-API gibt möglicherweise die folgenden Informationen für den Knoten zurück.

```
{
  "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"
    }
},
"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) "
]
}

```

Wenn ein Standby-Knoten nicht mehr angehängt ist, müssen Sie ihn so bald wie möglich wieder anhängen. Wenn der Knoten zu lange nicht mehr angehängt ist, fällt er möglicherweise bei der Verarbeitung des kontinuierlichen Streaming von WAL-Datensätzen vom primären Knoten so stark zurück, dass die Replizierung für ihn möglicherweise nicht mehr fortgesetzt werden kann.

Ursache

Um die Datenintegrität zu gewährleisten, verwendet die PostgreSQL-Datenbank Write-Ahead Logging (WAL). Der primäre Knoten streamt WAL zu Replizierungs- und Wiederherstellungszwecken konstant zu den aktiven Standby-Knoten. Die Standby-Knoten verarbeiten WAL, wenn sie es empfangen. Wenn ein Standby-Knoten nicht mehr angehängt ist, empfängt er kein WAL mehr und kann kein Kandidat für die Heraufstufung zum neuen primären Knoten mehr sein.

Lösung

- 1 Stellen Sie einen neuen Standby-Knoten bereit.
- 2 Heben Sie die Registrierung des nicht angehängten Standby-Knotens auf.

Nächste Schritte

Weitere Informationen finden Sie im [Wiederherstellen nach einem Ausfall einer Standby-Zelle in einem Hochverfügbarkeits-Cluster](#).

Die Clusterintegrität weist auf ein SSH-Problem hin

In einer Bereitstellung der VMware Cloud Director-Appliance mit Datenbank-HA-Konfiguration kann der **postgres**-Benutzer keine Verbindung zu seinen gleichrangigen Datenbankknoten über SSH herstellen.

Problem

Wenn zwischen den Datenbankknoten ein SSH-Problem besteht, zeigt VMware Cloud Director die `localClusterHealth` als `SSH_PROBLEM` an. Sie müssen dieses kritische Problem schnellstmöglich beheben.

Sie können die `localClusterHealth` mithilfe der Verwaltungsbenuzoberfläche der VMware Cloud Director-Appliance anzeigen oder die `/nodes-API` der VMware Cloud Director-Appliance ausführen. Weitere Informationen finden Sie in der [VMware Cloud Director-Appliance-API-Dokumentation](#).

Wenn Sie die `/nodes-API` auf einem Peer-Knoten des Knotens mit dem SSH-Problem ausführen, gibt die `/nodes-API` Informationen mit dem Hinweis zurück, dass die `localClusterHealth` auf `SSH_PROBLEM` und das `localClusterFailover` auf `UNBESTIMMT` lautet. Der Failover-Modus lautet `UNBESTIMMT`, da der Knoten, auf dem Sie die `/nodes-API` ausführen, keine Verbindung zu einem der zugehörigen Peer-Knoten über SSH herstellen kann. In den "details" im "failover"-Ausgabeteil des Antworttexts für den Knoten mit dem SSH-Problem wird Folgendes angezeigt: `ssh fehlgeschlagen. Befehl: ssh unreachable_standby_host_IP /usr/bin/grep failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf.`

Wenn beispielsweise bei einem Standby-Knoten ein SSH-Problem vorliegt und Sie `GET https://primary_host_IP:5480/api/1.0.0/nodes` ausführen, gibt die `/nodes-API` möglicherweise die folgenden Informationen zurück.

```
{
  "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": []
}

```

Wenn Sie GET `https://unreachable_standby_host_IP:5480/api/1.0.0/nodes` ausführen, weil der Knoten nicht vertrauenswürdig ist, sind die Daten zu `localClusterFailover` und `localClusterState` unter Umständen nicht korrekt. Die `/nodes`-API gibt Warnmeldungen mit dem Hinweis zurück, dass `unreachable_standby_host_name` keine Verbindung zu den zugehörigen Peer-Knoten herstellen kann.

Beispiel: Die /nodes-API gibt möglicherweise die folgenden Informationen zurück.

```
{
  "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)"
]
}

```

Ursache

VMware Cloud Director speichert die SSH-Zertifikate des **postgres**-Benutzers im Speicher des gemeinsam genutzten NFS-Übertragungsservers. Alle Datenbankknoten müssen über Zugriff auf den gemeinsam genutzten Speicher des Übertragungsservers verfügen. Wenn ein Datenbankknoten nicht mehr vertrauenswürdig ist, weil die SSH-Zertifikate des **postgres**-Benutzers entweder nicht mehr gültig oder nicht mehr zugänglich sind, kann dieser Knoten keine Befehle auf den zugehörigen Peer-Knoten mithilfe eines SSH-Clients ausführen. Die VMware Cloud Director-Appliance muss diese Funktion aufweisen, um im HA-Modus ordnungsgemäß ausgeführt werden zu können.

Lösung

- 1 Finden Sie heraus, ob ein Konnektivitätsproblem zwischen den Knoten besteht, und beheben Sie das Problem. Weitere Informationen finden Sie im [Überprüfen des Verbindungsstatus eines Datenbank-Hochverfügbarkeits-Clusters](#).
- 2 Stellen Sie sicher, dass der `appliance-sync.timer`-Dienst auf den Knoten mit dem SSH-Problem ausgeführt wird, indem Sie folgenden Befehl verwenden.

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

Der Befehl gibt beispielsweise Folgendes zurück:

```
* 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 Wenn der Status des `appliance-sync.timer`-Dienstes nicht auf **Aktiv** festgelegt ist, starten Sie den Dienst neu, indem Sie folgenden Befehl ausführen.

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

- 4 Warten Sie etwa 90 Sekunden und stellen Sie sicher, dass die Clusterintegrität auf **FEHLERFREI** festgelegt ist, indem Sie die VMware Cloud Director-Verwaltungsbenutzeroberfläche verwenden oder die `/nodes-API` aufrufen.

Verwenden der Protokolldateien zur Fehlerbehebung bei VMware Cloud Director-Updates und -Patches

Sie können die Protokolldateien auf Fehler und Warnungen prüfen, wenn Sie Patches auf die VMware Cloud Director-Appliance anwenden.

Problem

Wenn der Befehl `vamicli` einen Fehler zurückgibt, können Sie die Protokolldateien zur Fehlerbehebung verwenden.

Lösung

- 1 Melden Sie sich direkt oder mithilfe von SSH bei der Konsole der VMware Cloud Director-Appliance als **root** an.
- 2 Navigieren Sie zur entsprechenden Protokolldatei.
 - Wenn `vamicli update --check` fehlschlägt, navigieren Sie zu `/opt/vmware/var/log/vami/vami.log`.
 - Wenn `vamicli update --install latest` fehlschlägt, navigieren Sie zu `/opt/vmware/var/log/vami/updatecli.log`.
- 3 Prüfen Sie die Protokolldatei.

Suchen nach VMware Cloud Director-Updates schlägt fehl

Wenn Sie nach Updates der VMware Cloud Director-Appliance suchen, schlägt die Ausführung des Befehls `vamicli update --check` möglicherweise fehl.

Problem

Während der Anwendung eines Patches auf die VMware Cloud Director-Appliance führen Sie den Befehl `vamicli update --check` aus, um nach verfügbaren Updates zu suchen. Der Befehl `vamicli update --check` schlägt möglicherweise fehl mit Fehler: Fehler beim Herunterladen des Manifests. Wenden Sie sich an Ihren Anbieter.

Ursache

Der Pfad zum Update-Repository-Verzeichnis ist falsch.

Lösung

- 1 Führen Sie den Befehl `vamicli` mit dem richtigen Pfad aus.

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

- 2 Führen Sie den Befehl erneut aus, um nach Updates zu suchen.

```
vamicli update --check
```

Installieren des neuesten Updates von VMware Cloud Director schlägt fehl

Wenn Sie die neuesten Updates auf der VMware Cloud Director-Appliance installieren, schlägt die Ausführung des Befehls `vamicli update --install latest` möglicherweise fehl.

Problem

Während der Anwendung eines Patches auf die VMware Cloud Director-Appliance führen Sie den Befehl `vamicli update --install latest` aus, um den neuesten verfügbaren Patch anzuwenden. Der Befehl `vamicli update --install latest` schlägt möglicherweise fehl mit Fehler: Fehler beim Ausführen der Paketinstallation

Ursache

Der Fehler tritt auf, wenn der Zugriff auf den NFS-Server nicht möglich ist.

Lösung

- 1 Stellen Sie sicher, dass auf den unter `/opt/vmware/vcloud-director/data/transfer` gemounteten NFS-Server zugegriffen werden kann.
- 2 Führen Sie den Befehl erneut aus, um den verfügbaren Patch anzuwenden.

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

Installation, Upgrade und Verwaltung von VMware Cloud Director unter Linux

4

Sie erstellen eine VMware Cloud Director-Servergruppe, indem Sie die VMware Cloud Director-Software auf einem oder mehreren Linux-Servern installieren oder eine oder mehrere Instanzen der VMware Cloud Director-Appliance bereitstellen. Während des Installationsvorgangs führen Sie die Erstkonfiguration von VMware Cloud Director durch. Dies umfasst auch die Einrichtung der Netzwerk- und Datenbankverbindungen.

Die VMware Cloud Director-Software für Linux erfordert eine externe Datenbank, während die VMware Cloud Director-Appliance eine eingebettete PostgreSQL-Datenbank verwendet.

Nachdem Sie die VMware Cloud Director-Servergruppe erstellt haben, integrieren Sie die VMware Cloud Director-Installation in Ihre vSphere-Ressourcen. Für Netzwerkressourcen kann VMware Cloud Director NSX Data Center for vSphere oder NSX-T Data Center oder beides verwenden.

Wenn Sie ein Upgrade einer vorhandenen VMware Cloud Director-Installation durchführen, aktualisieren Sie die VMware Cloud Director-Software und das Datenbankschema und behalten die bestehenden Beziehungen zwischen Servern, der Datenbank und vSphere bei.

Wenn Sie eine vorhandene VMware Cloud Director-Installation unter Linux auf die VMware Cloud Director-Appliance migrieren, aktualisieren Sie die VMware Cloud Director-Software und migrieren die Datenbank in die eingebettete Datenbank in der Appliance.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurationsplanung](#)
- [Vorbereitung der Installation von VMware Cloud Director](#)
- [Installieren von VMware Cloud Director unter Linux](#)
- [Nach dem Installieren von VMware Cloud Director](#)
- [Upgrade von VMware Cloud Director unter Linux](#)
- [Nach dem Upgrade von VMware Cloud Director](#)

Konfigurationsplanung

vSphere bietet VMware Cloud Director Speicher-, Rechen- und Netzwerkkapazität. Überlegen Sie vor der Installation, wie viel vSphere- und VMware Cloud Director-Kapazität Sie für Ihre Cloud benötigen, und planen Sie eine Konfiguration, die diese Kapazität unterstützt.

Die Konfigurationsanforderungen sind von mehreren Faktoren abhängig. Dazu gehören die Anzahl der Organisationen in der Cloud, die Anzahl der Benutzer in den einzelnen Organisationen und der Aktivitätsgrad dieser Benutzer. Die folgenden Richtlinien sind für die meisten Konfigurationen als Ausgangspunkt geeignet:

- Teilen Sie jedem vCenter Server-System, für das in Ihrer Cloud der Zugriff ermöglicht werden soll, eine VMware Cloud Director-Zelle zu.
- Stellen Sie sicher, dass alle Linux-Zielserver für VMware Cloud Director mindestens die für Arbeitsspeicher und Speicher definierten Mindestanforderungen erfüllen. Eine Aufstellung dieser Anforderungen finden Sie unter *VMware Cloud Director-Versionshinweise*.
- Wenn Sie VMware Cloud Director unter Linux installieren möchten, konfigurieren Sie die VMware Cloud Director-Datenbank wie in [Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux](#) beschrieben.

Vorbereitung der Installation von VMware Cloud Director

Vor der Installation von VMware Cloud Director auf einem Linux-Server müssen Sie Ihre Umgebung vorbereiten.

Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux

Die VMware Cloud Director-Zellen speichern gemeinsam genutzte Informationen in einer Datenbank. Vor der Installation von VMware Cloud Director unter Linux müssen Sie eine PostgreSQL-Datenbankinstanz installieren und konfigurieren und das VMware Cloud Director-Datenbankbenutzerkonto erstellen.

PostgreSQL-Datenbanken haben spezifische Konfigurationsanforderungen, wenn sie mit VMware Cloud Director eingesetzt werden.

Sie müssen ein separates, dediziertes Datenbankschema erstellen, das von VMware Cloud Director verwendet werden soll. VMware Cloud Director kann ein Datenbankschema nicht mit einem anderen VMware-Produkt gemeinsam verwenden.

VMware Cloud Director unterstützt SSL-Verbindungen für die PostgreSQL-Datenbank. Sie können SSL für die PostgreSQL-Datenbank während einer unbeaufsichtigten Konfiguration von Netzwerk- und Datenbankverbindungen oder nach dem Erstellen der VMware Cloud Director-Servergruppe aktivieren. Weitere Informationen erhalten Sie unter [Referenz für unbeaufsichtigte Konfiguration](#) und [Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank](#).

Hinweis Nur VMware Cloud Director unter Linux verwendet eine externe Datenbank. Die VMware Cloud Director-Appliance verwendet die eingebettete PostgreSQL-Datenbank.

Voraussetzungen

Informationen zu den unterstützten VMware Cloud Director-Datenbanken finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#).

Sie müssen mit den Befehlen, den Skripting-Möglichkeiten und der Bedienung von PostgreSQL vertraut sein.

Verfahren

- 1 Konfigurieren Sie den Datenbankserver.

Ein Datenbankserver mit 16 GB Arbeitsspeicher, 100 GB Speicher und 4 CPUs eignet sich für typische VMware Cloud Director-Servergruppen.

- 2 Installieren Sie eine unterstützte PostgreSQL-Verteilung auf dem Datenbankserver.

- Der `SERVER_ENCODING`-Wert der Datenbank muss `UTF-8` sein. Dieser Wert wird bei der Installation der Datenbank festgelegt und entspricht immer der Codierung, die vom Datenbankserver-Betriebssystem verwendet wird.
- Verwenden Sie den PostgreSQL-`initdb`-Befehl, um den Wert von `LC_COLLATE` und `LC_CTYPE` auf `en_US.UTF-8` festzulegen. Beispiel:

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

- 3 Erstellen Sie den Datenbankbenutzer.

Mit dem folgenden Befehl wird der Benutzer `vcloud` erstellt.

```
create user vcloud;
```

- 4 Erstellen Sie die Datenbankinstanz und ernennen Sie einen Besitzer.

Verwenden Sie einen Befehl wie den folgenden, um einen Datenbankbenutzer mit dem Namen `vcloud` als Besitzer der Datenbank anzugeben.

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

- 5 Weisen Sie dem Konto des Datenbankbesitzers ein Datenbankkennwort zu.

Der folgende Befehl weist dem Datenbankbesitzer `vcloud` das Kennwort `vcloudpass` zu.

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

- 6 Ermöglichen Sie dem Datenbankbesitzer, sich bei der Datenbank anzumelden.

Der folgende Befehl weist dem Datenbankbesitzer `vcloud` die Option `login` zu.

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

Nächste Schritte

Nach dem Erstellen der VMware Cloud Director-Servergruppe können Sie die PostgreSQL-Datenbank so konfigurieren, dass SSL-Verbindungen aus den VMware Cloud Director-Zellen benötigt und bestimmte Datenbankparameter für optimale Leistung angepasst werden. Weitere Informationen finden Sie unter [Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank](#).

Vorbereiten des Übertragungsserverspeichers für VMware Cloud Director unter Linux

Um temporären Speicher für Uploads, Downloads und Katalogelemente, die extern veröffentlicht oder abonniert werden, bereitzustellen, müssen Sie veranlassen, dass alle Server in einer VMware Cloud Director-Servergruppe auf ein NFS- oder ein anderes gemeinsam genutztes Speichervolume zugreifen können.

Jedes Mitglied der Servergruppe mountet dieses Volume am selben Mount-Punkt: `/opt/vmware/vcloud-director/data/transfer`. Der Speicher auf diesem Volume wird auf viele Arten genutzt, einschließlich der folgenden:

- Während der Übertragung wird dieser Speicher durch Uploads und Downloads belegt. Wenn die Übertragung abgeschlossen ist, werden die Uploads und Downloads aus dem Speicher entfernt. Übertragungen, bei denen 60 Minuten lang keine Fortschritte erzielt werden, werden als „Abgelaufen“ markiert und vom System bereinigt. Da zu übertragende Bilder groß sein können, wird empfohlen, für diesen Zweck mindestens mehrere hundert Gigabyte zuzuweisen.
- Katalogobjekte in Katalogen, die extern veröffentlicht werden und für die Zwischenspeicherung von veröffentlichten Inhalten aktiviert ist, belegen diesen Speicher. Objekte von Katalogen, die extern veröffentlicht werden, aber keine Zwischenspeicherung ermöglichen, belegen diesen Speicher nicht. Wenn Sie Unternehmen in Ihrer Cloud die Möglichkeit bieten, Kataloge zu erstellen, die extern veröffentlicht werden, können Sie davon ausgehen, dass Hunderte oder sogar Tausende Katalogobjekte Speicherplatz auf diesem Volume benötigen. Die Größe der einzelnen Katalogelemente entspricht ungefähr der Größe einer virtuellen Maschine im komprimierten OVF-Format.

Hinweis Das Volume des Übertragungsserverspeichers muss über Kapazitäten für zukünftige Erweiterungen verfügen.

Optionen für den freigegebenen Speicher

Ein herkömmlicher Linux-basierter NFS-Server oder andere Lösungen wie Microsoft Windows Server, die NFS-Funktion VMware vSAN-Dateidienst usw. können den freigegebenen Speicher bereitstellen. Ab vSAN 7.0 können Sie die Funktion vSAN-Dateidienst zum Exportieren von NFS-Freigaben unter Verwendung der Protokolle NFS 3.0 und NFS 4.1 verwenden. Weitere Informationen zum vSAN-Dateidienst finden Sie im Handbuch *Verwalten von VMware vSAN* in der [Produktdokumentation zu VMware vSphere](#).

Anforderungen an die Konfiguration des NFS-Servers

Es gibt bestimmte Anforderungen an die Konfiguration des NFS-Servers, damit VMware Cloud Director Dateien in einen NFS-basierten Übertragungsserverspeicher schreiben und daraus lesen kann. Wegen dieser Anforderungen kann der **vCloud**-Benutzer die standardmäßigen Cloud-Vorgänge durchführen, während der **root**-Benutzer für die Erfassung von Protokollen mit mehreren Zeilen zuständig ist.

- In der Exportliste für den NFS-Server muss jedes Servermitglied in der VMware Cloud Director-Servergruppe über Lese-/Schreibzugriff auf den freigegebenen Speicherort verfügen, der in der Exportliste angegeben ist. Diese Funktion ermöglicht dem **vCloud**-Benutzer, Dateien in den freigegebenen Speicherort zu schreiben und Dateien daraus zu lesen.
- Der NFS-Server muss über das **root**-Systemkonto allen Servern in der VMware Cloud Director-Servergruppe Lese-/Schreibzugriff auf den freigegebenen Speicherort erteilen. Diese Funktion ermöglicht das gleichzeitige Erfassen der Protokolle aus allen Zellen in einem einzelnen Paket, indem das `vmware-vcd-support`-Skript mit den entsprechenden Optionen für Mehrfachzellen verwendet wird. Sie können diese Anforderung erfüllen, indem Sie `no_root_squash` in der NFS-Exportkonfiguration für diesen freigegebenen Speicherort verwenden.

Beispiel für Linux-NFS-Server

Wenn der Linux-NFS-Server ein Verzeichnis mit dem Namen „vCDspace“ als Übertragungsspeicher für die VMware Cloud Director-Servergruppe mit dem Speicherort `/nfs/vCDspace` verwendet, müssen Sie zum Exportieren dieses Verzeichnisses sicherstellen, dass der zugehörige Besitzer und die Berechtigungen auf **root:root** und **750** festgelegt sind. Die Methode `no_root_squash` wird zum Erteilen von Lese-/Schreibzugriff auf den freigegebenen Speicherort für drei Zellen mit den Namen „vCD-Cell1-IP“, „vCD-Cell2-IP“ und „vCD-Cell3-IP“ verwendet. Sie müssen der Datei `/etc/exports` die folgenden Zeilen hinzufügen.

```
/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)
```

In der Exportzeile darf zwischen der IP-Adresse jeder Zelle und der unmittelbar folgenden linken Klammer kein Leerzeichen vorhanden sein. Wenn der NFS-Server neu gestartet wird, während die Zellen Daten in den freigegebenen Speicherort schreiben, wird mit der Option `sync` in der Exportkonfiguration verhindert, dass die Daten im freigegebenen Speicherort beschädigt werden. Ein Unterverzeichnis eines Dateisystems wird zuverlässig exportiert, wenn Sie die Option `no_subtree_check` in der Exportkonfiguration verwenden.

Für jeden Server in der VMware Cloud Director-Servergruppe müssen Sie über einen entsprechenden Eintrag in der Datei `/etc/exports` des NFS-Servers verfügen, damit sie alle diese NFS-Freigabe mounten können. Führen Sie nach dem Vornehmen von Änderungen an der Datei `/etc/exports` auf dem NFS-Server den Befehl `exportfs -a` aus, um die NFS-Freigaben erneut zu exportieren.

Überlegungen beim Planen des Upgrades Ihrer VMware Cloud Director-Installation auf eine höhere Version

Während eines Upgrades einer VMware Cloud Director-Servergruppe führen Sie die Installationsdatei für die aktualisierte Version aus, um alle Mitglieder der VMware Cloud Director-Servergruppe zu aktualisieren. Aus Gründen der Übersichtlichkeit laden einige Unternehmen die Installationsdatei für das Upgrade in den Speicherort des Übertragungsservers herunter und führen sie von dort aus, da alle Zellen Zugriff auf diesen Speicherort haben. Da der **root**-Benutzer zum Ausführen der Upgrade-Installationsdatei verwendet werden muss, müssen Sie bei Nutzung des Übertragungsserverspeichers zum Ausführen eines Upgrades sicherstellen, dass der **root**-Benutzer die Upgrade-Installationsdatei ausführen kann, während Sie das Upgrade durchführen. Wenn Sie das Upgrade nicht als **root**-Benutzer ausführen können, muss die Datei in einen anderen Speicherort kopiert werden, in dem Sie sie als **root**-Benutzer ausführen können, z. B. in einem anderen Verzeichnis außerhalb des NFS-Mounts.

Herunterladen und Installieren des öffentlichen Schlüssels von VMware

Die Installationsdatei ist digital signiert. Zur Überprüfung der Gültigkeit der Signatur müssen Sie den öffentlichen Schlüssel von VMware herunterladen und installieren.

Sie können das `rpm`-Tool von Linux und den öffentlichen VMware-Schlüssel verwenden, um die digitale Signatur der VMware Cloud Director-Installationsdatei oder jeder anderen signierten Datei zu verifizieren, die Sie von `vmware.com` herunterladen. Wenn Sie den öffentlichen Schlüssel auf dem Computer installieren, auf dem VMware Cloud Director installiert werden soll, wird die Überprüfung als Teil des Installations- oder Aktualisierungsvorgangs durchgeführt. Sie können die Signatur jedoch auch manuell vor dem Beginn des Installations- oder Aktualisierungsvorgangs überprüfen und anschließend die verifizierte Datei für alle Installationen oder Upgrades verwenden.

Hinweis Auf der Download-Website finden Sie außerdem einen Prüfsummenwert für den Download. Dieser Wert wird in zwei üblichen Formaten präsentiert. Eine Verifizierung der Prüfsumme bestätigt, dass der heruntergeladene Dateinhalt mit dem auf der Website bereitgestellten Inhalt identisch ist. Sie liefert keine Aussage über die Gültigkeit der digitalen Signatur.

Verfahren

- 1 Erstellen Sie ein Verzeichnis zur Speicherung der öffentlichen Schlüssel für VMware-Pakete.
- 2 Laden Sie unter Verwendung eines Webbrowsers alle öffentlichen Schlüssel für VMware-Pakete aus dem Verzeichnis <http://packages.vmware.com/tools/keys> herunter.
- 3 Speichern Sie die Schlüsseldateien in dem von Ihnen erstellten Verzeichnis.

- 4 Führen Sie für jeden heruntergeladenen Schlüssel den folgenden Befehl zum Importieren des Schlüssels aus.

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

key_path steht für das Verzeichnis, in dem Sie die Schlüssel gespeichert haben.

key_name steht für den Dateinamen eines Schlüssels.

Installieren und Konfigurieren von NSX Data Center for vSphere für VMware Cloud Director

Wenn Sie Ihre VMware Cloud Director-Installation so planen, dass Netzwerkressourcen von NSX Data Center for vSphere verwendet werden, müssen Sie NSX Data Center for vSphere installieren und konfigurieren und eine eindeutige Instanz von NSX Manager jeder Instanz von vCenter Server zuordnen, die in der VMware Cloud Director-Installation enthalten sein soll.

NSX Manager ist im Download für NSX Data Center for vSphere enthalten. Die neuesten Informationen zur Kompatibilität zwischen VMware Cloud Director und anderen VMware-Produkten finden Sie in den *VMware-Produkt-Interoperabilitätstabellen* unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. Informationen zu den Netzwerkanforderungen finden Sie unter [Netzwerkkonfigurationsanforderungen für VMware Cloud Director](#).

Wichtig Dieses Verfahren ist nur anzuwenden, wenn Sie VMware Cloud Director neu installieren. Wenn Sie eine vorhandene Installation von VMware Cloud Director aktualisieren, lesen Sie die Informationen unter [Upgrade von VMware Cloud Director unter Linux](#).

Voraussetzungen

Überprüfen Sie, ob jedes Ihrer vCenter Server-Systeme die Anforderungen für die Installation von NSX Manager erfüllt.

Verfahren

- 1 Führen Sie die Installationsaufgabe für die virtuelle NSX Manager-Appliance durch.
Weitere Informationen dazu finden Sie im *Installationshandbuch für NSX*.
- 2 Melden Sie sich bei der virtuellen NSX Manager-Appliance, die Sie installiert haben, an und überprüfen Sie die Einstellungen, die Sie während der Installation angegeben haben.
- 3 Ordnen Sie die virtuelle NSX Manager-Appliance, die Sie zusammen mit dem vCenter Server-System installiert haben, das Sie zu VMware Cloud Director hinzufügen möchten, Ihrer geplanten VMware Cloud Director-Installation zu.
- 4 Konfigurieren Sie die VXLAN-Unterstützung in den zugehörigen NSX Manager-Instanzen.
VMware Cloud Director erstellt VXLAN-Netzwerkpools, um Netzwerkressourcen für Anbieter-VDCs bereitzustellen. Wenn die VXLAN-Unterstützung nicht im zugeordneten NSX Manager

konfiguriert wurde, wird bei den Anbieter-VDCs ein Netzwerkpool-Fehler angezeigt, und Sie müssen einen anderen Typ von Netzwerkpool erstellen und ihn dem Anbieter-VDC zuordnen. Weitere Informationen zum Konfigurieren der VXLAN-Unterstützung finden Sie im *Administratorhandbuch für NSX*.

- 5 (Optional) Wenn Edge Gateways im System verteiltes Routing bereitstellen sollen, richten Sie einen NSX Controller-Cluster ein.

Weitere Informationen dazu finden Sie im *Administratorhandbuch für NSX*.

Installieren und Konfigurieren von NSX-T Data Center für VMware Cloud Director

Wenn in Ihrer VMware Cloud Director-Installation Netzwerkressourcen von NSX-T Data Center verwendet werden sollen, müssen Sie mindestens eine NSX-T Data Center-Instanz installieren und konfigurieren.

Wichtig Um die NSX-T Data Center-Objekte und -Tools zu konfigurieren, verwenden Sie die vereinfachte Richtlinien-Benutzeroberfläche und die Richtlinien-APIs, die der vereinfachten Benutzeroberfläche entsprechen. Weitere Informationen hierzu finden Sie in der Übersicht zu NSX-T Manager im *NSX-T Data Center-Verwaltungshandbuch*.

Die neuesten Informationen zur Kompatibilität zwischen VMware Cloud Director und anderen VMware-Produkten finden Sie in den [VMware-Produkt-Interoperabilitätstabellen](#).

Informationen zu den Netzwerkanforderungen finden Sie unter [Netzwerkkonfigurationsanforderungen für VMware Cloud Director](#).

Dieses Verfahren ist nur anzuwenden, wenn Sie VMware Cloud Director neu installieren. Wenn Sie eine vorhandene Installation von VMware Cloud Director aktualisieren, lesen Sie die Informationen unter [Upgrade von VMware Cloud Director unter Linux](#).

Voraussetzungen

Machen Sie sich mit NSX-T Data Center vertraut.

Verfahren

- 1 Stellen Sie die virtuellen NSX-T Manager-Appliances bereit und konfigurieren Sie sie.
Weitere Informationen zur NSX-T Manager-Bereitstellung finden Sie im *NSX-T Data Center-Installationshandbuch*.
- 2 Erstellen Sie Transportzonen basierend auf Ihren Netzwerkanforderungen.
Weitere Informationen zu Transportzonen finden Sie im *NSX-T Data Center-Installationshandbuch*.

Hinweis

- 3 Stellen Sie Edge-Knoten und einen Edge-Cluster bereit und konfigurieren Sie diese.

Weitere Informationen zur NSX Edge-Erstellung finden Sie im *NSX-T Data Center-Installationshandbuch*.

- 4 Konfigurieren Sie die ESXi-Host-Transportknoten.

Weitere Informationen zum Konfigurieren eines Transportknotens für verwaltete Hosts finden Sie im *NSX-T Data Center-Installationshandbuch*.

- 5 Erstellen Sie ein Tier-0-Gateway.

Weitere Informationen zur Tier-0-Erstellung finden Sie im *NSX-T Data Center-Verwaltungshandbuch*.

Nächste Schritte

Nach der Installation von VMware Cloud Director haben Sie folgende Möglichkeiten:

- 1 Registrieren der NSX-T Manager-Instanz bei Ihrer Cloud

Informationen zur Registrierung einer NSX-T Manager-Instanz finden Sie im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

- 2 Erstellen eines Netzwerkpools, der von einer NSX-T Data Center-Transportzone gestützt wird

Weitere Informationen zum Erstellen eines Netzwerkpools, der von einer NSX-T Data Center-Transportzone gestützt wird, finden Sie im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

- 3 Importieren des Tier-0-Gateways als externes Netzwerk

Weitere Informationen zum Hinzufügen eines externen Netzwerks, das von einem logischen NSX-T Data Center-Tier-0-Router gestützt wird, finden Sie im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Installieren von VMware Cloud Director unter Linux

Sie können eine VMware Cloud Director-Servergruppe erstellen, indem Sie die VMware Cloud Director-Software von einem oder mehreren Linux-Servern installieren. Durch die Installation und Konfiguration des ersten Mitglieds der Gruppe wird eine Antwortdatei erstellt, mithilfe der Sie weitere Mitglieder der Gruppe konfigurieren können.

Dieses Verfahren gilt nur für Neuinstallationen. Eine Beschreibung des entsprechenden Verfahrens für die Aktualisierung einer vorhandenen VMware Cloud Director-Installation finden Sie unter [Upgrade von VMware Cloud Director unter Linux](#).

Wichtig Gemischte VMware Cloud Director-Installationen unter Linux und VMware Cloud Director-Appliance-Bereitstellungen in einer Servergruppe werden nicht unterstützt.

Ab Version 10.1 können Dienstleister und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Verweigerungsliste interner Hosts, die für Mandanten, die die VMware Cloud Director-API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Verweigerungsliste, nachdem Sie die Installation oder das Upgrade von VMware Cloud Director durchgeführt haben und bevor Sie Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie im [Konfigurieren einer Negativliste für Testverbindungen](#).

Voraussetzungen

- Vergewissern Sie sich, dass die Zielsever Ihrer Servergruppe den Anforderungen unter [Kapitel 2 VMware Cloud Director-Hardware- und Softwareanforderungen](#) entsprechen.
- Vergewissern Sie sich, dass Sie für jeden Endpoint der Zielsever für Ihre Servergruppe ein SSL-Zertifikat erstellt haben. Alle Verzeichnisse im Pfadnamen für die SSL-Zertifikate müssen für alle Benutzer lesbar sein. Durch die Verwendung desselben Keystore-Pfads für alle Mitglieder einer Servergruppe wird der Installationsvorgang vereinfacht. Beispiel: `/tmp/certificates.ks`. Weitere Informationen finden Sie unter [Vor dem Erstellen von SSL-Zertifikaten für VMware Cloud Director unter Linux](#).
- Vergewissern Sie sich, dass Sie ein NFS- oder anderes freigegebenes Speichervolumen vorbereitet haben, auf das alle Zielsever für Ihre VMware Cloud Director-Servergruppe zugreifen können. Weitere Informationen finden Sie unter [Vorbereiten des Übertragungsserverspeichers für VMware Cloud Director unter Linux](#).
- Überprüfen Sie, ob eine VMware Cloud Director-Datenbank erstellt wird und ob alle Server in der Gruppe auf diese zugreifen können. Weitere Informationen finden Sie im [Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux](#). Überprüfen Sie, ob der Datenbankdienst beim Neustart des Datenbankservers gestartet wird.
- Überprüfen Sie, ob alle VMware Cloud Director-Server, der Datenbankserver, alle vCenter Server-Systeme und die zugeordneten NSX Manager-Instanzen jeden Hostnamen in der Umgebung wie in [Netzwerkkonfigurationsanforderungen für VMware Cloud Director](#) beschrieben auflösen können.
- Überprüfen Sie, ob alle VMware Cloud Director-Server und der Datenbankserver mit einem Netzwerkzeitserver mit den in [Netzwerkkonfigurationsanforderungen für VMware Cloud Director](#) angegebenen Toleranzen synchronisiert sind.
- Wenn Sie Benutzer oder Gruppen von einem LDAP-Dienst importieren möchten, überprüfen Sie, ob alle VMware Cloud Director-Server auf diesen Dienst zugreifen können.

- Öffnen Sie die Firewall-Ports gemäß der Beschreibung in [Empfehlungen für die Netzwerksicherheit](#). Port 443 muss zwischen VMware Cloud Director und den vCenter Server-Systemen offen sein.

Verfahren

1 Installieren von VMware Cloud Director auf dem ersten Mitglied einer Servergruppe

Nachdem Sie Ihre Umgebung vorbereitet und die Voraussetzungen überprüft haben, können Sie mit dem Erstellen der VMware Cloud Director-Servergruppe beginnen, indem Sie das VMware Cloud Director-Installationsprogramm auf dem ersten Linux-Zielserver ausführen.

2 Erstellen und Verwalten von SSL-Zertifikaten für VMware Cloud Director unter Linux

VMware Cloud Director verwendet SSL, um die Kommunikation zwischen Clients und Servern zu sichern. Jeder VMware Cloud Director-Server muss zwei unterschiedliche SSL-Endpoints unterstützen – einen für die HTTPS- und einen für die Konsolen-Proxy-Kommunikation.

3 Konfigurieren der Netzwerk- und Datenbankverbindungen

Nach der Installation von VMware Cloud Director auf dem ersten Mitglied der Servergruppe müssen Sie das Konfigurationsskript ausführen, das die Netzwerk- und Datenbankverbindungen für diese Zelle erstellt. Das Skript erstellt eine Antwortdatei, die Sie beim Konfigurieren zusätzlicher Mitglieder der Servergruppe verwenden müssen.

4 Installieren von VMware Cloud Director auf einem weiteren Mitglied einer Servergruppe

Sie können jederzeit Server zu einer VMware Cloud Director-Servergruppe hinzufügen. Da alle Server in einer Servergruppe mit denselben Datenbankverbindungsdetails konfiguriert werden müssen, müssen Sie die Antwortdatei verwenden, die Sie bei der Konfiguration des ersten Mitglieds der Gruppe erstellt haben.

Nächste Schritte

Verwenden Sie den Befehl „system-setup“ des Zellenverwaltungsprogramms, um die Datenbank der Servergruppe mit einem Systemadministratorkonto und zugehörigen Informationen zu initialisieren. Weitere Informationen finden Sie im [Konfigurieren einer VMware Cloud Director-Installation](#).

Installieren von VMware Cloud Director auf dem ersten Mitglied einer Servergruppe

Nachdem Sie Ihre Umgebung vorbereitet und die Voraussetzungen überprüft haben, können Sie mit dem Erstellen der VMware Cloud Director-Servergruppe beginnen, indem Sie das VMware Cloud Director-Installationsprogramm auf dem ersten Linux-Zielserver ausführen.

VMware Cloud Director für Linux wird als digital signierte ausführbare Datei mit einem Namen im Format `vmware-vcloud-director-distribution-v. v-nnnnnn.bin` verteilt, wobei `v.v.v` die Produktversion und `nnnnnn` die Build-Nummer darstellt. Beispiel: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Durch Ausführen dieser ausführbaren Datei wird VMware Cloud Director installiert oder aktualisiert.

Das VMware Cloud Director-Installationsprogramm überprüft, ob der Zielsever alle Voraussetzungen für die Plattform erfüllt, und installiert dann die VMware Cloud Director-Software auf diesem Server.

Voraussetzungen

- Überprüfen Sie, ob Sie die für den Zielsever benötigten Superuser-Anmeldeinformationen besitzen.
- Laden Sie den öffentlichen Schlüssel von VMware auf den Zielsever herunter und installieren Sie ihn, wenn das Installationsprogramm die digitale Signatur der Installationsdatei überprüfen soll. Wenn Sie die digitale Signatur der Installationsdatei bereits überprüft haben, müssen Sie sie nicht erneut während der Installation überprüfen. Weitere Informationen finden Sie unter [Herunterladen und Installieren des öffentlichen Schlüssels von VMware](#).

Verfahren

- 1 Melden Sie sich beim Zielsever als **root** an.

- 2 Laden Sie die Installationsdatei auf den Zielsever herunter.

Wenn Sie die Software auf einem Medium gekauft haben, kopieren Sie die Installationsdatei an einen Speicherort, auf den der Zielsever zugreifen kann.

- 3 Überprüfen Sie, ob die Prüfsumme der heruntergeladenen Datei mit der auf der Downloadseite angezeigten Prüfsumme übereinstimmt.

Die Download-Seite stellt jeweils einen Wert für die MD5- und die SHA1-Prüfsumme zur Verfügung. Verwenden Sie das geeignete Tool, um zu überprüfen, ob die Prüfsumme der heruntergeladenen Installationsdatei mit der Prüfsumme der Downloadseite übereinstimmt. Ein Linux-Befehl mit dem folgenden Format zeigt die Prüfsumme für *Installationsdatei* an.

```
[root@cell11 /tmp]# md5sum installation-file
```

Der Befehl gibt die Prüfsumme der Installationsdatei zurück, die mit der MD5-Prüfsumme von der Downloadseite übereinstimmen muss.

- 4 Stellen Sie sicher, dass die Installationsdatei ausführbar ist.

Die Installationsdatei erfordert die Berechtigung **execute**. Um sicherzustellen, dass sie diese Berechtigung besitzt, öffnen Sie ein Konsolen-, Shell- oder Terminalfenster, und führen Sie den folgenden Linux-Befehl aus, wobei *installation-file* der vollständige Pfadname zur VMware Cloud Director-Installationsdatei ist.

```
[root@cell11 /tmp]# chmod u+x installation-file
```

- 5 Führen Sie die Installationsdatei aus.

Um die Installationsdatei auszuführen, geben Sie den vollständigen Pfadnamen ein, z. B.:

```
[root@cell11 /tmp]# ./Installationsdatei
```

Diese Datei enthält ein Installationskript und ein eingebettetes RPM-Paket.

Hinweis Sie können die Installationsdatei nicht von einem Verzeichnis ausführen, dessen Pfadname Leerzeichen einschließt.

Wenn Sie den öffentlichen Schlüssel von VMware nicht auf dem Zielsystem installiert haben, gibt das Installationsprogramm eine Warnung in der folgenden Form aus:

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

Das Installationsprogramm führt folgende Aktionen aus.

- a Es überprüft, ob der Host alle Anforderungen erfüllt.
- b Es verifiziert die digitale Signatur für die Installationsdatei.
- c Es erstellt den/die `vcloud`-Benutzer und -Gruppe.
- d Es entpackt das VMware Cloud Director-RPM-Paket.
- e Es installiert die Software.

Nach Abschluss der Installation werden Sie vom Installationsprogramm aufgefordert, das Konfigurationskript auszuführen, das die Netzwerk- und Datenbankverbindungen konfiguriert.

- 6 Wählen Sie aus, ob das Konfigurationskript ausgeführt werden soll.
 - a Um das Konfigurationskript im interaktiven Modus auszuführen, geben Sie `y` ein und drücken Sie die Eingabetaste.
 - b Um das Konfigurationskript zu einem späteren Zeitpunkt im interaktiven oder im unbeaufsichtigten Modus auszuführen, geben Sie `n` ein und drücken Sie die Eingabetaste.

Erstellen und Verwalten von SSL-Zertifikaten für VMware Cloud Director unter Linux

VMware Cloud Director verwendet SSL, um die Kommunikation zwischen Clients und Servern zu sichern. Jeder VMware Cloud Director-Server muss zwei unterschiedliche SSL-Endpoints unterstützen – einen für die HTTPS- und einen für die Konsolen-Proxy-Kommunikation.

Bei den Endpoints kann es sich um separate IP-Adressen oder eine einzelne IP-Adresse mit zwei verschiedenen Ports handeln. Es wird für jeden Endpunkt ein eigenes SSL-Zertifikat benötigt. Sie können dasselbe Zertifikat für beide Endpoints verwenden, z. B. mithilfe eines Platzhalterzertifikats.

Vor dem Erstellen von SSL-Zertifikaten für VMware Cloud Director unter Linux

Wenn Sie VMware Cloud Director für Linux installieren, müssen Sie für jedes Mitglied der Servergruppe zwei Zertifikate erstellen und diese in Host-Keystores importieren.

Hinweis Sie müssen die Zertifikate für die Mitglieder der Servergruppe nur nach der Installation von VMware Cloud Director unter Linux erstellen. Die VMware Cloud Director-Appliance erstellt während des ersten Startvorgangs selbstsignierte SSL-Zertifikate.

Verfahren

1 Melden Sie sich beim VMware Cloud Director-Server als **root** an.

2 Listen Sie die IP-Adressen für den Server auf.

Verwenden Sie einen Befehl wie `ifconfig` zur Erkennung der IP-Adressen dieses Servers.

3 Führen Sie für jede IP-Adresse den folgenden Befehl aus, um den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) abzurufen, an den die IP-Adresse gebunden ist.

```
nslookup IP-Adresse
```

4 Notieren Sie sich jede IP-Adresse und den jeweils zugeordneten FQDN. Wenn Sie nicht dieselbe IP-Adresse für beide Dienste verwenden, müssen Sie eine IP-Adresse für den HTTPS-Dienst und eine IP-Adresse für den Konsolen-Proxy-Dienst festlegen.

Sie müssen die FQDNs zum Erstellen der Zertifikate und die IP-Adressen zum Konfigurieren der Netzwerk- und der Datenbankverbindungen angeben. Notieren Sie sich andere FQDNs, die die IP-Adresse erreichen können, da Sie diese angeben müssen, wenn das Zertifikat einen alternativen Antragstellernamen (SAN) enthalten soll.

Nächste Schritte

Erstellen Sie die Zertifikate für beide Endpoints. Sie können von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority, CA) signierte Zertifikate oder selbstsignierte Zertifikate verwenden.

Hinweis Von einer Zertifizierungsstelle signierte Zertifikate bieten die höchste Vertrauensebene.

- Informationen zum Erstellen und Importieren von SSL-Zertifikaten, die von einer Zertifizierungsstelle signiert wurden, finden Sie unter [Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores für VMware Cloud Director unter Linux](#).
- Informationen zum Erstellen von selbstsignierten SSL-Zertifikaten finden Sie unter [Erstellen von selbstsignierten SSL-Zertifikaten für VMware Cloud Director unter Linux](#).

- Informationen zum Importieren Ihres eigenen privaten Schlüssels und der von einer Zertifizierungsstelle signierten Zertifikatsdateien finden Sie unter [Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores mit importierten privaten Schlüsseln für VMware Cloud Director unter Linux](#).

Erstellen von selbstsignierten SSL-Zertifikaten für VMware Cloud Director unter Linux

Selbstsignierte Zertifikate bieten die Möglichkeit, SSL bequem für VMware Cloud Director in Umgebungen zu konfigurieren, in denen minimale Bedenken in Bezug auf Vertraulichkeit herrschen.

Jeder VMware Cloud Director-Server benötigt zwei SSL-Zertifikate in einer JCEKS-Keystore-Datei, eins für den HTTPS-Dienst und eins für den Konsolen-Proxy-Dienst.

Sie verwenden das `cell-management-tool`, um die selbstsignierten SSL-Zertifikate zu erstellen. Das Dienstprogramm `cell-management-tool` wird vor dem Ausführen des Konfigurations-Agent und nach dem Ausführen der Installationsdatei auf der Zelle installiert. Weitere Informationen finden Sie im [Installieren von VMware Cloud Director auf dem ersten Mitglied einer Servergruppe](#).

Wichtig In diesen Beispielen wird eine Schlüssellänge von 2048 Bit angegeben, Sie sollten jedoch die Sicherheitsanforderungen Ihrer Installation zunächst überprüfen, um die geeignete Schlüssellänge auszuwählen. Schlüssel mit einer Länge von weniger als 1024 Bit werden entsprechend NIST Special Publication 800-131A nicht mehr unterstützt.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem des VMware Cloud Director-Servers als **root** an.
- 2 Führen Sie den Befehl zum Erstellen eines Schlüsselpaars aus einem öffentlichen und einem privaten Schlüssel für den HTTPS- und den Konsolen-Proxy-Dienst aus.

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

Der Befehl erstellt oder aktualisiert einen Keystore in `certificates.ks`, der das Kennwort `passwd` aufweist. Das `cell-management-tool` erstellt die Zertifikate mithilfe der Standardwerte des Befehls. Je nach DNS-Konfiguration Ihrer Umgebung ist der CN des Ausstellers für jeden Dienst entweder auf die IP-Adresse oder den FQDN festgelegt. Für das Zertifikat wird die Standardschlüssellänge von 2048-Bit verwendet und das Zertifikat läuft ein Jahr nach der Erstellung ab.

Wichtig Die Keystore-Datei und das Verzeichnis, in dem sie sich befindet, müssen vom Benutzer **vcloud.vcloud** gelesen werden können. Das Installationsprogramm von VMware Cloud Director erstellt diesen Benutzer und diese Gruppe.

Nächste Schritte

Notieren Sie sich den Keystore-Pfadnamen. Sie benötigen den Keystore-Pfadnamen, wenn Sie das Konfigurationsskript zum Erstellen der Netzwerk- und Datenbankverbindungen für die VMware Cloud Director-Zelle ausführen. Weitere Informationen finden Sie unter [Konfigurieren der Netzwerk- und Datenbankverbindungen](#).

Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores für VMware Cloud Director unter Linux

Das Erstellen und Importieren der von einer Zertifizierungsstelle signierten Zertifikate bietet die höchste Vertrauensebene für die SSL-Kommunikation und hilft Ihnen, die Verbindungen innerhalb Ihrer Cloud-Infrastruktur zu sichern.

Jeder VMware Cloud Director-Server benötigt zwei SSL-Zertifikate, um die Kommunikation zwischen Clients und Servern zu sichern. Jeder VMware Cloud Director-Server muss zwei unterschiedliche SSL-Endpoints unterstützen – einen für die HTTPS- und einen für die Konsolen-Proxy-Kommunikation.

Bei den beiden Endpoints kann es sich um separate IP-Adressen oder eine einzelne IP-Adresse mit zwei verschiedenen Ports handeln. Es wird für jeden Endpunkt ein eigenes SSL-Zertifikat benötigt. Sie können dasselbe Zertifikat für beide Endpoints verwenden, z. B. mithilfe eines Platzhalterzertifikats.

Bei den Zertifikaten für beide Endpoints müssen sowohl ein definierter X.500-Name als auch eine X.509 Subject Alternative Name-Erweiterung angegeben werden.

Sie können von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority, CA) signierte Zertifikate oder selbstsignierte Zertifikate verwenden.

Sie verwenden das `cell-management-tool`, um die selbstsignierten SSL-Zertifikate zu erstellen. Das Dienstprogramm `cell-management-tool` wird vor dem Ausführen des Konfigurations-Agent und nach dem Ausführen der Installationsdatei auf der Zelle installiert. Weitere Informationen finden Sie im [Installieren von VMware Cloud Director auf dem ersten Mitglied einer Servergruppe](#).

Wenn Sie bereits über einen eigenen privaten Schlüssel und eine von einer Zertifizierungsstelle signierte Zertifikatsdatei verfügen, befolgen Sie die in [Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores mit importierten privaten Schlüsseln für VMware Cloud Director unter Linux](#) beschriebenen Schritte.

Wichtig In diesen Beispielen wird eine Schlüssellänge von 2048 Bit angegeben, Sie sollten jedoch die Sicherheitsanforderungen Ihrer Installation zunächst überprüfen, um die geeignete Schlüssellänge auszuwählen. Schlüssel mit einer Länge von weniger als 1024 Bit werden entsprechend NIST Special Publication 800-131A nicht mehr unterstützt.

Voraussetzungen

- Vergewissern Sie sich, dass Sie Zugriff auf einen Computer haben, auf dem Version 8 oder höher der Java-Laufzeitumgebung installiert ist, damit Sie die Zertifikate mithilfe des Befehls `keytool` importieren können. Das VMware Cloud Director-Installationsprogramm

platziert eine Kopie von `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`, aber Sie können diesen Vorgang auf jedem Computer durchführen, auf dem eine Java-Laufzeitumgebung installiert ist. Zertifikate, die mit dem Befehl `keytool` von jeder anderen Quelle erstellt werden, werden für die Verwendung mit VMware Cloud Director nicht unterstützt. Diese Befehlszeilenbeispiele setzen voraus, dass `keytool` im Pfad des Benutzers enthalten ist.

- Machen Sie sich mit dem Befehl `keytool` vertraut.
- Weitere Details zu den verfügbaren Optionen für den Befehl `generate-certs` finden Sie unter [Generieren von selbstsignierten Zertifikaten für die HTTPS- und Konsolenproxy-Endpoints](#).
- Weitere Informationen zu den verfügbaren Optionen für den Befehl `certificates` finden Sie unter [Ersetzen der Zertifikate für die HTTPS- und Konsolenproxy-Endpoints](#).

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem der VMware Cloud Director-Serverzelle als **root** an.
- 2 Führen Sie den Befehl zum Erstellen eines Schlüsselpaars aus einem öffentlichen und einem privaten Schlüssel für den HTTPS- und den Konsolen-Proxy-Dienst aus.

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

Der Befehl erstellt oder aktualisiert einen Keystore in `certificates.ks` mit dem angegebenen Kennwort. Zertifikate werden mithilfe der Standardwerte des Befehls erstellt. Je nach DNS-Konfiguration Ihrer Umgebung ist der CN des Ausstellers für jeden Dienst entweder auf die IP-Adresse oder den FQDN festgelegt. Für das Zertifikat wird die Standardschlüssellänge von 2048-Bit verwendet und das Zertifikat läuft ein Jahr nach der Erstellung ab.

Wichtig Die Keystore-Datei und das Verzeichnis, in dem sie sich befindet, müssen vom Benutzer **vcloud.vcloud** gelesen werden können. Das Installationsprogramm von VMware Cloud Director erstellt diesen Benutzer und diese Gruppe.

3 Erstellen Sie eine Zertifikatssignieranforderung für den HTTPS- und den Konsolenproxydienst.

Wichtig Wenn Sie separate IP-Adressen für den HTTPS- und den Konsolenproxydienst verwenden, passen Sie die Hostnamen und IP-Adressen in den folgenden Befehlen an.

- a Erstellen Sie eine Zertifikatssignieranforderung in der Datei `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 Erstellen Sie eine Zertifikatssignieranforderung in der Datei `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 Senden Sie die Zertifikatssignieranforderungen an die Zertifizierungsstelle.

Wenn Ihre Zertifizierungsstelle die Angabe eines Webservertyps verlangt, geben Sie Jakarta Tomcat an.

Sie erhalten die von der Zertifizierungsstelle signierten Zertifikate.

5 Importieren Sie die signierten Zertifikate in den PKCS12-Keystore.

- a Importieren Sie das Stammzertifikat der Zertifizierungsstelle aus der Datei `root.cer` in die Keystore-Datei `certificates.ks`.

```
keytool -import -storetype PKCS12 -storepass keystore_password -keystore
certificates.ks -alias root -file root_certificate_file
```

- b Wenn Sie Zwischenzertifikate erhalten haben, importieren Sie sie aus der Datei `intermediate.cer` in die Keystore-Datei `certificates.ks`.

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

- c Importieren Sie das Zertifikat des HTTPS-Diensts.

```
keytool -import -storetype PKCS12 -storepass keystore_password -keystore
certificates.ks -alias http -file http_certificate_file
```

- d Importieren Sie das Konsolen-Proxy-Dienstzertifikat.

```
keytool -import -storetype PKCS12 -storepass keystore_password -keystore
certificates.ks -alias consoleproxy -file console_proxy_certificate_file
```

Die Befehle überschreiben die Datei `certificates.ks` mit den neu erworbenen, von der Zertifizierungsstelle signierten Versionen der Zertifikate.

- 6 Um zu überprüfen, ob die Zertifikate in den PKCS12-Keystore importiert wurden, führen Sie den Befehl zum Auflisten der Inhalte der Keystore-Datei aus.

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

- 7 Wiederholen Sie diesen Vorgang auf allen VMware Cloud Director-Servern in der Servergruppe.

Nächste Schritte

- Wenn Sie Ihre VMware Cloud Director-Instanz noch nicht konfiguriert haben, führen Sie das Skript `configure` aus, um den Zertifikat-Keystore in VMware Cloud Director zu importieren. Weitere Informationen finden Sie unter [Konfigurieren der Netzwerk- und Datenbankverbindungen](#).

Hinweis Wenn Sie die Keystore-Datei `certificates.ks` auf einem anderen Computer als dem Server erstellt haben, auf dem Sie die Liste der vollqualifizierten Domännennamen und ihre zugehörigen IP-Adressen generiert haben, kopieren Sie die Keystore-Datei nun auf diesen Server. Sie benötigen den Keystore-Pfadnamen, wenn Sie das Konfigurationskript ausführen.

- Wenn Sie Ihre VMware Cloud Director-Instanz bereits installiert und konfiguriert haben, verwenden Sie den Befehl `certificates` des Zellenverwaltungstools zum Importieren des Zertifikat-Kestores. Weitere Informationen finden Sie im [Ersetzen der Zertifikate für die HTTPS- und Konsolenproxy-Endpoints](#).

Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Kestores mit importierten privaten Schlüsseln für VMware Cloud Director unter Linux

Wenn Sie über einen eigenen privaten Schlüssel und von einer Zertifizierungsstelle signierte Zertifikatsdateien verfügen, müssen Sie vor dem Importieren der Kestores in die VMware Cloud Director-Umgebung Keystore-Dateien erstellen, in die die Zertifikate und die privaten Schlüssel für den HTTPS- und den Konsolen-Proxy-Dienst importiert werden.

Voraussetzungen

- Weitere Informationen finden Sie im [Vor dem Erstellen von SSL-Zertifikaten für VMware Cloud Director unter Linux](#).
- Vergewissern Sie sich, dass Sie Zugriff auf einen Computer haben, auf dem Version 8 oder höher der Java-Laufzeitumgebung installiert ist, damit Sie die Zertifikate mithilfe des Befehls `keytool` importieren können. Das VMware Cloud Director-Installationsprogramm platziert eine Kopie von `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`, aber Sie können diesen Vorgang auf jedem Computer durchführen, auf dem eine Java-Laufzeitumgebung installiert ist. Zertifikate, die mit dem Befehl `keytool` von jeder anderen Quelle erstellt werden, werden für die Verwendung mit VMware Cloud Director nicht unterstützt. Diese Befehlszeilenbeispiele setzen voraus, dass `keytool` im Pfad des Benutzers enthalten ist.
- Machen Sie sich mit dem Befehl `keytool` vertraut.

- Laden Sie OpenSSL herunter und installieren Sie es.
- Weitere Informationen zu den verfügbaren Optionen für den Befehl `certificates` finden Sie unter [Ersetzen der Zertifikate für die HTTPS- und Konsolenproxy-Endpoints](#).

Verfahren

- 1 Wenn Sie über Zwischenzertifikate verfügen, führen Sie den Befehl aus, um das von der Zertifizierungsstelle signierte Root-Zertifikat mit den Zwischenzertifikaten zu kombinieren und eine Zertifikatskette zu erstellen.

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

- 2 Verwenden Sie OpenSSL, um für den HTTPS- und den Konsolen-Proxy-Dienst PKCS12-Keystore-Zwischendateien mit dem privaten Schlüssel, der Zertifikatskette und dem entsprechenden Alias zu erstellen, und geben Sie ein Kennwort für jede Keystore-Datei an.

- a Erstellen Sie die Keystore-Datei für den HTTPS-Dienst.

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.p12 -chain
```

- b Erstellen Sie die Keystore-Datei für den Konsolen-Proxy-Dienst.

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.p12 -chain
```

- 3 Verwenden Sie `keytool`, um die PKCS12-Keystores in den Keystore `certificates.ks` zu importieren.

- a Führen Sie den Befehl zum Importieren des PKCS12-Keystore für den HTTPS-Dienst aus.

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

- b Führen Sie den Befehl zum Importieren des PKCS12-Keystore für den Konsolen-Proxy-Dienst aus.

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

- 4 Um zu überprüfen, ob die Zertifikate in den Keystore importiert wurden, führen Sie den Befehl zum Auflisten der Inhalte der Keystore-Datei aus.

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

- 5 Wiederholen Sie diese Schritte für alle VMware Cloud Director-Zellen in Ihrer Umgebung.

Nächste Schritte

- Wenn Sie Ihre VMware Cloud Director-Instanz noch nicht konfiguriert haben, führen Sie das Skript `configure` aus, um den Zertifikat-Keystore in VMware Cloud Director zu importieren. Weitere Informationen finden Sie unter [Konfigurieren der Netzwerk- und Datenbankverbindungen](#).

Hinweis Wenn Sie die Keystore-Datei `certificates.ks` auf einem anderen Computer als dem Server erstellt haben, auf dem Sie die Liste der vollqualifizierten Domännennamen und ihre zugehörigen IP-Adressen generiert haben, kopieren Sie die Keystore-Datei auf diesen Server. Sie benötigen den Keystore-Pfadnamen, wenn Sie das Konfigurationsskript ausführen.

- Wenn Sie Ihre VMware Cloud Director-Instanz bereits installiert und konfiguriert haben, verwenden Sie den Befehl `certificates` des Zellenverwaltungstools zum Importieren des Zertifikat-Keystores. Weitere Informationen finden Sie im [Ersetzen der Zertifikate für die HTTPS- und Konsolenproxy-Endpoints](#).

Konfigurieren der Netzwerk- und Datenbankverbindungen

Nach der Installation von VMware Cloud Director auf dem ersten Mitglied der Servergruppe müssen Sie das Konfigurationsskript ausführen, das die Netzwerk- und Datenbankverbindungen für diese Zelle erstellt. Das Skript erstellt eine Antwortdatei, die Sie beim Konfigurieren zusätzlicher Mitglieder der Servergruppe verwenden müssen.

Alle Mitglieder der VMware Cloud Director-Servergruppe verwenden die Datenbankverbindung und andere Konfigurationsdetails gemeinsam. Wenn Sie das Konfigurationsskript auf dem ersten Mitglied der VMware Cloud Director-Servergruppe ausführen, erstellt das Skript eine Antwortdatei, in der die Datenbankverbindungsinformationen für die Verwendung in späteren Serverinstallationen aufbewahrt werden.

Sie können das Konfigurationsskript entweder im interaktiven Modus oder im unbeaufsichtigten Modus ausführen. Bei einer interaktiven Konfiguration führen Sie den Befehl ohne Optionen aus. Das Skript fordert Sie anschließend auf, die erforderlichen Informationen zur Einrichtung einzugeben. Bei einer unbeaufsichtigten Konfiguration geben Sie die Informationen zur Einrichtung mithilfe der Befehlsoptionen an.

Wenn Sie eine einzige IP-Adresse mit zwei verschiedenen Ports für den HTTPS- und den Konsolenproxydienst verwenden möchten, müssen Sie das Konfigurationsskript im unbeaufsichtigten Modus ausführen.

Hinweis Das Zellenverwaltungstool enthält Unterbefehle, mit denen Sie die ursprünglich konfigurierten Netzwerk- und Datenbankverbindungsdetails ändern können. Mit diesen Unterbefehlen vorgenommene Änderungen werden in die globale Konfigurationsdatei und in die Antwortdatei geschrieben. Informationen zur Verwendung des Zellenverwaltungstools finden Sie unter [Kapitel 5 Überblick über das Zellenverwaltungstool](#).

Voraussetzungen

- Lesen Sie für eine interaktive Konfiguration die Informationen unter [Interaktive Konfigurationsreferenz](#).
- Lesen Sie für eine unbeaufsichtigte Konfiguration die Informationen unter [Referenz für unbeaufsichtigte Konfiguration](#).
- Bevor Sie eine unbeaufsichtigte Konfiguration ausführen, stellen Sie sicher, dass der Wert der Umgebungsvariable `V_CLOUD_HOME` auf den vollständigen Pfadnamen des Verzeichnisses festgelegt ist, in dem VMware Cloud Director installiert ist. Dieser Wert lautet meistens `/opt/vmware/vcloud-director`.

Verfahren

- 1 Melden Sie sich beim VMware Cloud Director-Server als Root-Benutzer an.
- 2 Führen Sie den `configure`-Befehl aus:

- Bei interaktivem Modus führen Sie den Befehl aus und geben an der Eingabeaufforderungen die erforderlichen Informationen ein.

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

- Bei unbeaufsichtigtem Modus führen Sie den Befehl mit den entsprechenden Optionen und Argumenten aus.

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

Das Skript prüft die Informationen und führt dann die folgenden Aktionen durch:

- a Es initialisiert die Datenbank und verbindet den Server mit ihr.
 - b Es zeigt eine URL an, die Sie mit dem Assistenten **VMware Cloud Director einrichten** nach dem Start des VMware Cloud Director-Diensts verbinden können.
 - c Es bietet das Starten der VMware Cloud Director-Zelle an.
- 3 (Optional) Notieren Sie sich die URL des Assistenten **VMware Cloud Director einrichten** und geben Sie `y` ein, um den VMware Cloud Director-Dienst zu starten.

Sie können den Dienst auch später mit dem Befehl `service vmware-vcd start` starten.

Ergebnisse

Datenbankverbindungsinformationen und andere wiederverwendbare Informationen, die Sie während der Konfiguration angegeben haben, werden in der Antwortdatei aufbewahrt, die sich auf diesem Server unter `/opt/vmware/vcloud-director/etc/responses.properties` befindet. Diese Datei enthält vertrauliche Informationen, die Sie wiederverwenden müssen, wenn Sie Server zu einer Servergruppe hinzufügen.

Nächste Schritte

Speichern Sie eine Kopie der Antwortdatei an einem sicheren Ort. Schränken Sie den Zugriff auf sie ein, und achten Sie darauf, dass sie an einem sicheren Ort gesichert wird. Wenn Sie diese Datei sichern, senden Sie keinen Klartext über ein öffentliches Netzwerk.

Wenn Sie Server zu der Servergruppe hinzufügen möchten, mounten Sie den gemeinsam genutzte Übertragungsspeicher unter `/opt/vmware/vcloud-director/data/transfer`.

Interaktive Konfigurationsreferenz

Wenn Sie das `configure`-Skript im interaktiven Modus ausführen, fordert Sie das Skript zur Eingabe der folgenden Informationen auf.

Um einen Standardwert zu akzeptieren, drücken Sie die Eingabetaste.

Tabelle 4-1. Erforderliche Informationen während einer interaktiven Netzwerk- und Datenbankkonfiguration

Erforderliche Informationen	Beschreibung
IP-Adresse für den HTTPS-Dienst	Standardmäßig die erste verfügbare IP-Adresse
IP-Adresse für den Konsolen-Proxy-Dienst	Standardmäßig die erste verfügbare IP-Adresse Hinweis Wenn Sie eine einzige IP-Adresse mit zwei verschiedenen Ports für den HTTPS- und den Konsolenproxydienst verwenden möchten, müssen Sie das Konfigurationsskript im unbeaufsichtigten Modus ausführen.
Vollständiger Pfad der Java-Keystore-Datei	Beispiel: <code>/opt/keystore/certificates.ks</code> .
Kennwort für den Keystore	Weitere Informationen finden Sie unter Vor dem Erstellen von SSL-Zertifikaten für VMware Cloud Director unter Linux .
Kennwort des privaten Schlüssels für das HTTPS-SSL-Zertifikat	Weitere Informationen finden Sie unter Vor dem Erstellen von SSL-Zertifikaten für VMware Cloud Director unter Linux .
Kennwort für den privaten Schlüssel für das Konsolen-Proxy-SSL-Zertifikat	Weitere Informationen finden Sie unter Vor dem Erstellen von SSL-Zertifikaten für VMware Cloud Director unter Linux .

Tabelle 4-1. Erforderliche Informationen während einer interaktiven Netzwerk- und Datenbankkonfiguration (Fortsetzung)

Erforderliche Informationen	Beschreibung
Remote-Überwachungsprotokollierung für einen Syslog-Host aktivieren	<p>Dienste in den einzelnen VMware Cloud Director-Zellen protokollieren Überwachungsmeldungen an die VMware Cloud Director-Datenbank, in der diese 90 Tage aufbewahrt werden. Um Überwachungsmeldungen für einen längeren Zeitraum zu speichern, können Sie die VMware Cloud Director-Dienste so konfigurieren, dass diese die Überwachungsmeldungen nicht nur an die VMware Cloud Director-Datenbank, sondern zusätzlich auch an das <code>syslog</code>-Dienstprogramm senden.</p> <ul style="list-style-type: none"> ■ Zum Überspringen drücken Sie die Eingabetaste. ■ Zum Aktivieren geben Sie den Syslog-Hostnamen oder die IP-Adresse an.
Wenn Sie die Remote-Überwachungsprotokollierung aktiviert haben, UDP-Port des Syslog-Hosts	Die Standardeinstellung lautet 514.
Hostname oder die IP-Adresse des Datenbankservers	Der Server, auf dem die Datenbank ausgeführt wird.
Datenbankport	Die Standardeinstellung lautet 5432.
Datenbankname	Standardmäßig „vcloud“.
Name des Datenbankbenutzers	Weitere Informationen finden Sie im Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux .
Datenbankkennwort	Weitere Informationen finden Sie im Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux .
Dem Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) von VMware beitreten oder nicht daran teilnehmen	<p>Dieses Produkt nimmt am Programm zur Verbesserung der Benutzerfreundlichkeit („CEIP“) von VMware teil. Einzelheiten im Hinblick auf die über CEIP gesammelten Daten und die Zwecke, für die diese von VMware verwendet werden, finden Sie im Trust & Assurance Center unter http://www.vmware.com/trustvmware/ceip.html. Mit dem Zellenverwaltungstool können Sie dem CEIP von VMware für dieses Produkt jederzeit beitreten bzw. dieses verlassen. Weitere Informationen finden Sie im Kapitel 5 Überblick über das Zellenverwaltungstool.</p> <p>Um dem Programm beizutreten, geben Sie y ein. Wenn Sie nicht am VMware-CEIP-Programm teilnehmen möchten, geben Sie n ein.</p>

Referenz für unbeaufsichtigte Konfiguration

Wenn Sie das `configure`-Skript in einem unbeaufsichtigten Modus ausführen, geben Sie die Informationen zur Einrichtung an der Befehlszeile als Optionen und Argumente an.

Tabelle 4-2. Optionen und Argumente des Konfigurationsdienstprogramms

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Zeigt eine Zusammenfassung von Konfigurationsoptionen und -argumenten an
<code>--config-file (-c)</code>	Pfad zur <code>global.properties</code> -Datei	Die Informationen, die Sie bei der Ausführung des Konfigurationsdienstprogramms bereitstellen, werden in dieser Datei gespeichert. Wenn Sie diese Option auslassen, wird der Standardspeicherort <code>/opt/vmware/vcloud-director/etc/global.properties</code> verwendet.
<code>--console-proxy-ip (-cons)</code>	IPv4-Adresse mit optionaler Portnummer	Das System verwendet diese Adresse für den Konsolen-Proxy-Dienst von VMware Cloud Director. Beispiel: <code>10.17.118.159</code> .
<code>--console-proxy-port-https</code>	Ganzzahl im Bereich 0 bis 65535	Portnummer für die Verwendung für den Konsolen-Proxy-Dienst von VMware Cloud Director.
<code>--database-ssl</code>	<code>true</code> oder <code>false</code>	Sie können die PostgreSQL-Datenbank so konfigurieren, dass eine richtig signierte SSL-Verbindung von VMware Cloud Director benötigt wird. Wenn Sie die PostgreSQL-Datenbank zur Verwendung eines selbstsignierten oder privaten Zertifikats konfigurieren möchten, finden Sie weitere Informationen unter Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank .
<code>--database-host (-dbhost)</code>	IP-Adresse oder vollqualifizierter Domänenname des VMware Cloud Director-Datenbank-Hosts	Weitere Informationen finden Sie im Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux .
<code>--database-name (-dbname)</code>	Der Datenbankdienstname	Weitere Informationen finden Sie im Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux .

Tabelle 4-2. Optionen und Argumente des Konfigurationsdienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
<code>--database-password (-dbpassword)</code>	Kennwort für den Datenbankbenutzer. Der Wert kann null sein.	Weitere Informationen finden Sie im Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux .
<code>--database-port (-dbport)</code>	Portnummer, die vom Datenbankdienst auf dem Datenbank-Host verwendet wird	Weitere Informationen finden Sie im Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux .
<code>--database-type (-dbtype)</code>	Der Datenbanktyp. Der unterstützte Typ ist <code>postgres</code> .	Optional. Der Datenbanktyp ist standardmäßig <code>postgres</code> . Weitere Informationen finden Sie im Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux .
<code>--database-user (-dbuser)</code>	Benutzername des Datenbankbenutzers.	Weitere Informationen finden Sie im Konfigurieren einer externen PostgreSQL-Datenbank für VMware Cloud Director unter Linux .
<code>--enable-ceip</code>	<code>true</code> oder <code>false</code>	Dieses Produkt nimmt am Programm zur Verbesserung der Benutzerfreundlichkeit („CEIP“) von VMware teil. Einzelheiten im Hinblick auf die über CEIP gesammelten Daten und die Zwecke, für die diese von VMware verwendet werden, finden Sie im Trust & Assurance Center unter http://www.vmware.com/trustvmware/ceip.html . Mit dem Zellenverwaltungstool können Sie dem CEIP von VMware für dieses Produkt jederzeit beitreten bzw. dieses verlassen. Weitere Informationen finden Sie im Kapitel 5 Überblick über das Zellenverwaltungstool .
<code>--uuid (-g)</code>	Keine	Generiert einen neuen eindeutigen Bezeichner für die Zelle

Tabelle 4-2. Optionen und Argumente des Konfigurationsdienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
<code>--primary-ip (-ip)</code>	IPv4-Adresse mit optionaler Portnummer	Das System verwendet diese Adresse für den Webschnittstellendienst von VMware Cloud Director. Beispiel: <i>10.17.118.159</i> .
<code>--primary-port-http</code>	Ganzzahl im Bereich 0 bis 65535	Portnummer zur Verwendung für HTTP-Verbindungen (unsicher) zum Webschnittstellendienst von VMware Cloud Director
<code>--primary-port-https</code>	Ganzzahl im Bereich 0 bis 65535	Portnummer zur Verwendung für HTTPS-Verbindungen (sicher) zum Webschnittstellendienst von VMware Cloud Director
<code>--keystore (-k)</code>	Pfad zum Java-Keystore, der Ihre SSL-Zertifikate und privaten Schlüssel enthält	Muss ein vollständiger Pfadname sein. Beispiel: <i>/opt/keystore/certificates.ks</i> .
<code>--syslog-host (-loghost)</code>	IP-Adresse oder vollqualifizierter Domänenname des Syslog-Server-Hosts	Dienste in den einzelnen VMware Cloud Director-Zellen protokollieren Überwachungsmeldungen an die VMware Cloud Director-Datenbank, in der diese 90 Tage aufbewahrt werden. Um Überwachungsmeldungen für einen längeren Zeitraum zu speichern, können Sie die VMware Cloud Director-Dienste so konfigurieren, dass diese die Überwachungsmeldungen nicht nur an die VMware Cloud Director-Datenbank, sondern zusätzlich auch an das <code>syslog</code> -Dienstprogramm senden.
<code>--syslog-port (-logport)</code>	Ganzzahl im Bereich 0 bis 65535	Der Port, an dem der <code>syslog</code> -Vorgang den angegebenen Server überwacht. Ist standardmäßig 514, wenn nicht angegeben.

Tabelle 4-2. Optionen und Argumente des Konfigurationsdienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
<code>--response-file (-r)</code>	Pfad zur Antwortdatei	Muss ein vollständiger Pfadname sein. Ist standardmäßig <code>/opt/vmware/vcloud-director/etc/responses.properties</code> , wenn nicht angegeben. Alle Informationen, die Sie beim Ausführen der Konfiguration eingeben, werden in dieser Datei gespeichert. Wichtig Diese Datei enthält vertrauliche Informationen, die Sie wiederverwenden müssen, wenn Sie Server zu einer Servergruppe hinzufügen. Speichern Sie die Datei an einem sicheren Ort und stellen Sie sie nur bei Bedarf zur Verfügung.
<code>--unattended-installation (-unattended)</code>	Keine	Gibt eine unbeaufsichtigte Installation an.
<code>--keystore-password (-w)</code>	Kennwort für SSL-Zertifikat-Keystore	Kennwort für SSL-Zertifikat-Keystore.

Beispiel: Unbeaufsichtigte Konfiguration mit zwei IP-Adressen

Der folgende Beispielbefehl führt eine unbeaufsichtigte Konfiguration eines VMware Cloud Director-Servers mit zwei verschiedenen IP-Adressen für den HTTPS- und den Konsolenproxydienst aus.

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

Beispiel: Unbeaufsichtigte Konfiguration mit einer einzelnen IP-Adresse

Der folgende Beispielbefehl führt eine unbeaufsichtigte Konfiguration eines VMware Cloud Director-Servers mit einer einzelnen IP-Adresse aus, die zwei verschiedene Ports für den HTTPS- und den Konsolenproxydienst aufweist.

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

Schützen und Wiederverwenden der Antwortdatei

Details zu Netzwerk- und Datenbankverbindungen, die Sie für die erste VMware Cloud Director-Zelle konfigurieren, werden in einer Antwortdatei gespeichert. Diese Datei enthält vertrauliche Informationen, die Sie wiederverwenden müssen, wenn Sie der Servergruppe Server hinzufügen. Sie müssen die Datei an einem sicheren Ort speichern.

Die Antwortdatei wird unter `/opt/vmware/vcloud-director/etc/responses.properties` auf dem ersten Server erstellt, für den Sie die Netzwerk- und Datenbankverbindungen konfigurieren. Wenn Sie der Gruppe Server hinzufügen, müssen Sie mithilfe einer Kopie der Antwortdatei Konfigurationsparameter zur Verfügung stellen, die alle Server gemeinsam nutzen.

Wichtig Das Zellenverwaltungstool enthält Unterbefehle, mit denen Sie die ursprünglich angegebenen Netzwerk- und Datenbankverbindungsdetails ändern können. Mit diesen Tools vorgenommene Änderungen werden in die globale Konfigurationsdatei und in die Antwortdatei geschrieben. Sie müssen deshalb sicherstellen, dass die Antwortdatei vorhanden (in `/opt/vmware/vcloud-director/etc/responses.properties`) und beschreibbar ist, bevor Sie einen der Befehle verwenden, mit denen diese geändert werden können.

Verfahren

1 Schützen Sie die Antwortdatei.

Speichern Sie eine Kopie der Datei an einem sicheren Ort. Schränken Sie den Zugriff auf sie ein, und achten Sie darauf, dass sie an einem sicheren Ort gesichert wird. Wenn Sie die Datei sichern, senden Sie keinen Klartext über ein öffentliches Netzwerk.

2 Verwenden Sie die Antwortdatei wieder.

- a Kopieren Sie die Datei an einen Ort, auf den der Server zugreifen kann, den Sie konfigurieren möchten.

Hinweis Sie müssen die VMware Cloud Director-Software auf einem Server installieren, damit Sie die Antwortdatei erneut für die Konfiguration verwenden können. Alle Verzeichnisse im Pfadnamen für die Antwortdatei müssen für den Benutzer `vcloud.vcloud` lesbar sein, wie in diesem Beispiel gezeigt.

```
[root@cell11 /tmp]# ls -l responses.properties
-rw----- 1 vcloud vcloud 418 Jun 8 13:42 responses.properties
```

Dieser Benutzer und diese Gruppe werden vom Installationsprogramm erstellt.

- b Führen Sie das Konfigurationsskript mit der Option `-r` aus und geben Sie den Pfadnamen der Antwortdatei an.

Melden Sie sich als Root an, öffnen Sie ein Konsolen-, Shell- oder Terminalfenster, und geben Sie Folgendes ein:

```
[root@cell11 /tmp]# /opt/vmware/vcloud-director/bin/configure -r /path-to-response-file
```

Nächste Schritte

Nachdem Sie die zusätzlichen Server konfiguriert haben, löschen Sie die Kopie der Antwortdatei, mit der Sie sie konfiguriert haben.

Installieren von VMware Cloud Director auf einem weiteren Mitglied einer Servergruppe

Sie können jederzeit Server zu einer VMware Cloud Director-Servergruppe hinzufügen. Da alle Server in einer Servergruppe mit denselben Datenbankverbindungsdetails konfiguriert werden müssen, müssen Sie die Antwortdatei verwenden, die Sie bei der Konfiguration des ersten Mitglieds der Gruppe erstellt haben.

Wichtig Gemischte VMware Cloud Director-Installationen unter Linux und VMware Cloud Director-Appliance-Bereitstellungen in einer Servergruppe werden nicht unterstützt.

Voraussetzungen

- Vergewissern Sie sich, dass Sie Zugriff auf die Antwortdatei haben, die bei der Konfiguration des ersten Mitglieds dieser Servergruppe erstellt wurde. Weitere Informationen finden Sie unter [Konfigurieren der Netzwerk- und Datenbankverbindungen](#).
- Vergewissern Sie sich, dass Sie den gemeinsam genutzten Übertragungsspeicher auf dem ersten Mitglied der VMware Cloud Director-Servergruppe unter `/opt/vmware/vcloud-director/data/transfer` gemountet haben.

Verfahren

1 Melden Sie sich beim Zielsever als **root** an.

2 Laden Sie die Installationsdatei auf den Zielsever herunter.

Wenn Sie die Software auf einem Medium gekauft haben, kopieren Sie die Installationsdatei an einen Speicherort, auf den der Zielsever zugreifen kann.

3 Stellen Sie sicher, dass die Installationsdatei ausführbar ist.

Die Installationsdatei erfordert die Berechtigung **execute**. Um sicherzustellen, dass sie diese Berechtigung besitzt, öffnen Sie ein Konsolen-, Shell- oder Terminalfenster, und führen Sie den folgenden Linux-Befehl aus, wobei *installation-file* der vollständige Pfadname zur VMware Cloud Director-Installationsdatei ist.

```
[root@cell11 /tmp]# chmod u+x installation-file
```

4 Führen Sie die Installationsdatei aus.

Um die Installationsdatei auszuführen, geben Sie den vollständigen Pfadnamen ein, z. B.:

```
[root@cell11 /tmp]# ./Installationsdatei
```

Diese Datei enthält ein Installationskript und ein eingebettetes RPM-Paket.

Hinweis Sie können die Installationsdatei nicht von einem Verzeichnis ausführen, dessen Pfadname Leerzeichen einschließt.

Wenn Sie den öffentlichen Schlüssel von VMware nicht auf dem Zielsystem installiert haben, gibt das Installationsprogramm eine Warnung in der folgenden Form aus:

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

Das Installationsprogramm führt folgende Aktionen aus.

- a Es überprüft, ob der Host alle Anforderungen erfüllt.
- b Es verifiziert die digitale Signatur für die Installationsdatei.
- c Es erstellt den/die `vcloud`-Benutzer und -Gruppe.
- d Es entpackt das VMware Cloud Director-RPM-Paket.
- e Es installiert die Software.

Nach Abschluss der Installation werden Sie vom Installationsprogramm aufgefordert, das Konfigurationskript auszuführen, das die Netzwerk- und Datenbankverbindungen konfiguriert.

- 5 Geben Sie `n` ein und drücken Sie die Eingabetaste, um die Ausführung des Konfigurationskripts abzulehnen.

Sie führen das Konfigurationskript später aus, indem Sie die Antwortdatei als Eingabe bereitstellen.

- 6 Mounten Sie den gemeinsam genutzten Übertragungsspeicher unter `/opt/vmware/vcloud-director/data/transfer`.

Alle VMware Cloud Director-Server in der Servergruppe müssen dieses Volume auf dem gleichen Einhängepunkt mounten.

- 7 Kopieren Sie die Antwortdatei an einen Ort, auf den dieser Server zugreifen kann.

Alle Verzeichnisse im Pfadnamen der Antwortdatei müssen von Root gelesen werden können.

8 Führen Sie das Konfigurationsskript aus.

- a Führen Sie den Befehl `configure` aus, indem Sie den Pfadnamen der Antwortdatei angeben.

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

Das Skript kopiert die Antwortdatei in einen Speicherort, der von `vcloud.vcloud` gelesen werden kann, und führt das Konfigurationsskript mit der Antwortdatei als Eingabe aus.

- b Geben Sie in den Eingabeaufforderungen die IP-Adressen für den HTTP-Dienst und den Konsolen-Proxy-Dienst an.
- c Wenn das Konfigurationsskript in dem in der Antwortdatei angegebenen Pfadnamen keine gültigen Zertifikate findet, geben Sie den Pfadnamen der Zertifikate und Kennwörter ein, wenn Sie dazu aufgefordert werden.

Das Skript prüft die Informationen, verbindet den Server mit der Datenbank und bietet an, die VMware Cloud Director-Zelle zu starten.

9 (Optional) Geben Sie `y` ein, um den VMware Cloud Director-Dienst zu starten.

Sie können den Dienst auch später mit dem Befehl `service vmware-vcd start` starten.

Nächste Schritte

Wiederholen Sie den Vorgang, um dieser Servergruppe weitere Server hinzuzufügen.

Wenn die VMware Cloud Director-Dienste auf allen Servern ausgeführt werden, müssen Sie die VMware Cloud Director-Datenbank mit einem Lizenzschlüssel, einem Systemadministratorkonto und zugehörigen Informationen initialisieren. Sie können die Datenbank mithilfe des Zellenverwaltungstools mit dem Unterbefehl `system-setup` initialisieren. Weitere Informationen finden Sie im [Konfigurieren einer VMware Cloud Director-Installation](#).

Nach dem Installieren von VMware Cloud Director

Nach dem Erstellen der VMware Cloud Director-Servergruppe können Sie Microsoft Sysprep-Dateien und die Cassandra-Datenbank installieren. Wenn Sie eine PostgreSQL-Datenbank verwenden, können Sie SSL konfigurieren und einige Parameter in der Datenbank anpassen.

Ab Version 10.1 können Dienstanbieter und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Verweigerungsliste interner Hosts, die für Mandanten, die die VMware Cloud Director-API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Verweigerungsliste, nachdem Sie die Installation oder das Upgrade von VMware Cloud Director durchgeführt haben und bevor Sie Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie im [Konfigurieren einer Negativliste für Testverbindungen](#).

Anpassen öffentlicher Adressbücher für VMware Cloud Director unter Linux

Zum Erfüllen der Anforderungen des Lastausgleichsdiensts oder Proxys können Sie die Webadressen des Standard-Endpoints für das VMware Cloud Director-Webportal, die VMware Cloud Director-API und den Konsolen-Proxy ändern.

Voraussetzungen

Stellen Sie sicher, dass Sie sich als **Systemadministrator** angemeldet haben. Nur ein **Systemadministrator** kann öffentliche Endpoints anpassen.

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste des Service Provider Admin Portal **Administration** aus.
- 2 Klicken Sie im linken Bereich unter **Einstellungen** auf **Öffentliche Adressen**.
- 3 Um die öffentlichen Endpoints anzupassen, klicken Sie auf **Bearbeiten**.
- 4 Bearbeiten Sie zum Anpassen der VMware Cloud Director-URLs die **Webportal**-Endpoints.
 - a Geben Sie eine benutzerdefinierte öffentliche VMware Cloud Director-URL für (nicht sichere) HTTP-Verbindungen ein.
 - b Geben Sie eine benutzerdefinierte öffentliche VMware Cloud Director-URL für (sichere) HTTPS-Verbindungen ein und klicken Sie auf **Hochladen**, um die Zertifikate hochzuladen, die die Vertrauenskette für diesen Endpoint bilden.

Die Zertifikatskette muss mit dem vom Dienst-Endpoint verwendeten Zertifikat übereinstimmen. Hierbei handelt es sich um das Zertifikat, das auf alle VMware Cloud Director-Zellen-Keystores mit dem Alias `consoleproxy` hochgeladen wurde. SSL-Terminierung der Konsolen-Proxy-Verbindungen auf einem Lastausgleichsdienst wird nicht unterstützt. Die Zertifikatskette muss ein Endpoint-Zertifikat, Zwischenzertifikate und ein Stammzertifikat im PEM-Format ohne einen privaten Schlüssel enthalten.

- 5 (Optional) Um die Cloud Director REST API- und die OpenAPI-URLs anzupassen, deaktivieren Sie die Option **Webportaleinstellungen verwenden**.

- a Geben Sie eine benutzerdefinierte HTTP-Basis-URL ein.

Wenn Sie die HTTP-Basis-URL beispielsweise auf **http://vcloud.example.com** setzen, können Sie auf die VMware Cloud Director-API unter `http://vcloud.example.com/api` und auf VMware Cloud Director OpenAPI unter `http://vcloud.example.com/cloudapi` zugreifen.

- b Geben Sie eine benutzerdefinierte HTTPS REST API-Basis-URL ein und klicken Sie auf **Hochladen**, um die Zertifikate hochzuladen, die die Vertrauenskette für diesen Endpoint bilden.

Wenn Sie die Basis-URL der HTTPS-REST API beispielsweise auf **https://vcloud.example.com** setzen, können Sie auf die VMware Cloud Director-API unter `https://vcloud.example.com/api` und auf VMware Cloud Director OpenAPI unter `https://vcloud.example.com/cloudapi` zugreifen.

Die Zertifikatskette muss mit dem vom Dienst-Endpoint verwendeten Zertifikat übereinstimmen. Hierbei handelt es sich entweder um das Zertifikat, das auf alle VMware Cloud Director-Zellen-Keystores mit dem Alias `http` hochgeladen wurde, oder um das VIP-Zertifikat des Lastausgleichsdiensts, wenn SSL-Terminierung verwendet wird. Die Zertifikatskette muss ein Endpoint-Zertifikat, Zwischenzertifikate und ein Stammzertifikat im PEM-Format ohne einen privaten Schlüssel enthalten.

- 6 Geben Sie die Adresse eines benutzerdefinierten öffentlichen VMware Cloud Director-Konsolen-Proxys ein.

Bei dieser Adresse handelt es sich um den vollqualifizierten Domännennamen (FQDN) des VMware Cloud Director-Servers oder Lastausgleichsdiensts mit der Portnummer. Der Standardport ist 443.

Wichtig Die VMware Cloud Director-Appliance verwendet ihre `eth0`-NIC an dem benutzerdefinierten Port 8443 für den Konsolen-Proxy-Dienst.

Geben Sie für eine VMware Cloud Director-Appliance-Instanz mit dem FQDN `vcloud.example.com` beispielsweise **vcloud.example.com:8443** ein.

VMware Cloud Director verwendet die Konsolen-Proxy-Adresse beim Öffnen eines Remote-Konsolenfensters auf einer VM.

- 7 Klicken Sie zum Speichern der Änderungen auf **Speichern**.

Installieren und Konfigurieren einer Cassandra-Datenbank zum Speichern von historischen Metrikdaten

VMware Cloud Director kann Metriken erfassen, die aktuelle und historische Informationen über die Leistung und den Ressourcenverbrauch der virtuellen Maschinen in Ihrer Cloud zur Verfügung stellen. Daten für historische Metriken werden in einem Cassandra-Cluster gespeichert.

Cassandra ist eine Open Source-Datenbank, die Sie verwenden können, um den zugrunde liegenden Speicher für eine skalierbare, leistungsfähige Lösung zur Erfassung von Zeitreihendaten (z. B. Metriken für virtuelle Maschinen) bereitzustellen. Wenn VMware Cloud Director das Abrufen von historischen Metriken aus virtuellen Maschinen unterstützen soll, müssen Sie einen Cassandra-Cluster installieren und konfigurieren und das Dienstprogramm `cell-management-tool` zum Herstellen einer Verbindung zwischen dem Cluster und VMware Cloud Director verwenden. Für das Abrufen aktueller Metriken ist keine optionale Datenbanksoftware erforderlich.

Voraussetzungen

- Bevor Sie die optionale Datenbanksoftware konfigurieren, stellen Sie sicher, dass VMware Cloud Director installiert ist und ausgeführt wird.
- Wenn Sie noch nicht mit Cassandra vertraut sind, lesen Sie die Informationen unter <http://cassandra.apache.org/>.
- Eine Liste der Cassandra-Versionen, die zur Verwendung als Metrikdatenbank unterstützt werden, finden Sie in den *VMware Cloud Director-Versionshinweise*. Sie können Cassandra unter <http://cassandra.apache.org/download/> herunterladen.
- Installieren und konfigurieren Sie den Cassandra-Cluster:
 - Der Cassandra-Cluster muss mindestens vier virtuelle Maschinen enthalten, die auf zwei oder mehr Hosts bereitgestellt werden.
 - Zwei Cassandra-Seed-Knoten sind erforderlich.
 - Aktivieren Sie Client-zu-Knoten-Verschlüsselung mit Cassandra. Weitere Informationen finden Sie unter <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html>.
 - Aktivieren Sie Cassandra-Benutzerauthentifizierung. Weitere Informationen finden Sie unter <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html>.
 - Aktivieren Sie Java Native Access (JNA) Version 3.2.7 oder höher auf jedem Cassandra-Cluster.
 - Knoten-zu-Knoten-Verschlüsselung mit Cassandra ist optional.
 - Verwendung von SSL mit Cassandra ist optional. Wenn Sie sich gegen die Aktivierung von SSL für Cassandra entscheiden, müssen Sie den Konfigurationsparameter `cassandra.use.ssl` in der Datei `global.properties` in jeder Zelle auf 0 setzen (`$VCLLOUD_HOME/etc/global.properties`)

Verfahren

- 1 Verwenden Sie das Dienstprogramm `cell-management-tool`, um eine Verbindung zwischen VMware Cloud Director und den Knoten im Cassandra-Cluster herzustellen.

Im folgenden Beispielbefehl sind `node1-ip`, `node2-ip`, `node3-ip` und `node4-ip` die IP-Adressen der Mitglieder des Cassandra-Clusters. Es wird der Standardport (9042) verwendet. Metrikdaten werden 15 Tage lang aufbewahrt.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --configure
--create-schema \ --cluster-nodes node1-ip,node2-ip,node3-ip, node4-ip \ --username admin
--password 'P@55w0rd' --ttl 15
```

Informationen zur Verwendung des Zellenverwaltungstools finden Sie unter [Kapitel 5 Überblick über das Zellenverwaltungstool](#).

- 2 (Optional) Wenn Sie ein Upgrade von VMware Cloud Director von Version 9.1 durchführen, verwenden Sie das Dienstprogramm `cell-management-tool`, um die Metrikdatenbank zum Speichern von mehrstufigen Metriken zu konfigurieren.

Führen Sie einen Befehl ähnlich dem folgenden Beispiel aus:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --add-
rollup \ --username admin --password 'P@55w0rd'
```

- 3 Starten Sie jede VMware Cloud Director-Zelle neu.

Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank

Nach dem Erstellen der VMware Cloud Director-Servergruppe können Sie die externe PostgreSQL-Datenbank so konfigurieren, dass SSL-Verbindungen aus den VMware Cloud Director-Zellen benötigt und bestimmte Datenbankparameter für optimale Leistung angepasst werden.

Die sichersten Verbindungen erfordern ein offiziell signiertes SSL-Zertifikat mit einer vollständigen Vertrauenskette, die auf einer vertrauenswürdigen öffentlichen Zertifizierungsstelle basiert. Alternativ können Sie ein selbstsigniertes SSL-Zertifikat oder ein SSL-Zertifikat verwenden, das von einer privaten Zertifizierungsstelle signiert wurde. Sie müssen dieses Zertifikat aber in den VMware Cloud Director-Truststore importieren.

Um optimale Leistung für Ihre Systemspezifikation und Ihre Anforderungen zu erzielen, können Sie die Datenbankkonfigurationen und Autovacuum-Parameter in der Konfigurationsdatei der Datenbank anpassen.

Verfahren

- 1 Konfigurieren Sie SSL-Verbindungen zwischen VMware Cloud Director und der PostgreSQL-Datenbank.

- a Wenn Sie ein selbstsigniertes oder privates Zertifikat für die externe PostgreSQL-Datenbank verwendet haben, führen Sie in jeder VMware Cloud Director-Zelle den Befehl zum Importieren des Datenbankzertifikats in den VMware Cloud Director-Truststore aus.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# cell-management-tool import-trusted-certificates --source path_to_self-signed_or_private_cert
```

- b Führen Sie den Befehl zum Aktivieren von SSL-Verbindungen zwischen VMware Cloud Director und PostgreSQL aus.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# cell-management-tool reconfigure-database --database-ssl true
```

Sie können den Befehl für alle Zellen in der Servergruppe ausführen, indem Sie die Option `--private-key-path` verwenden.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# cell-management-tool reconfigure-database --database-ssl true --private-key-path path_to_private_key
```

Weitere Informationen zur Verwendung des Zellenverwaltungstools finden Sie in [Kapitel 5 Überblick über das Zellenverwaltungstool](#).

- 2 Bearbeiten Sie die Datenbankkonfigurationen in der Datei `postgresql.conf` für Ihre Systemspezifikation.

Bei einem System mit 16 GB Arbeitsspeicher können Sie beispielsweise folgendes Fragment verwenden.

```
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 Bearbeiten Sie die Autovacuum-Parameter in der Datei `postgresql.conf` für Ihre Anforderungen.

Bei normalen VMware Cloud Director-Arbeitslasten können Sie das folgende Fragment verwenden.

```
autovacuum = on
track_counts = on
autovacuum_max_workers = 3
autovacuum_naptime = 1min
autovacuum_vacuum_cost_limit = 2400
```

Das System legt einen benutzerdefinierten `autovacuum_vacuum_scale_factor`-Wert für die Aktivität und die `activity_parameters`-Tabellen fest.

Nächste Schritte

Wenn Sie die Datei `postgresql.conf` bearbeitet haben, müssen Sie die Datenbank neu starten.

Installieren und Konfigurieren einer RabbitMQ AMQP Broker-Instanz

Wenn Sie blockierende Aufgaben, Benachrichtigungen oder VMware Cloud Director-API-Erweiterungen wie Container Service Extension (CSE) und VMware Cloud Director App Launchpad verwenden möchten, müssen Sie einen RabbitMQ AMQP Broker installieren und konfigurieren.

Advanced Message Queuing Protocol (AMQP) ist ein offener Standard für Nachrichtenwarteschlangen, der flexible Messaging-Funktionen für Unternehmenssysteme unterstützt. VMware Cloud Director verwendet RabbitMQ AMQP Broker zum Bereitstellen des Nachrichtenbuses, der von Erweiterungsdiensten, Objekterweiterungen und Benachrichtigungen verwendet wird.

Bei VMware Cloud Director kann beim Konfigurieren von Benachrichtigungen die Verwendung eines MQTT-Clients eine Alternative zu RabbitMQ AMQP Broker sein. Weitere Informationen finden Sie im [Abonnieren von Ereignissen, Aufgaben und Metriken mithilfe eines MQTT-Clients](#).

Verfahren

- 1 Laden Sie den RabbitMQ-Server von <https://www.rabbitmq.com/download.html> herunter.
Die Liste der unterstützten RabbitMQ-Versionen finden Sie in den *VMware Cloud Director-Versionshinweise*.
- 2 Befolgen Sie die Installationsanweisungen für RabbitMQ und installieren Sie die Software auf einem geeigneten Host.
Der RabbitMQ-Serverhost muss für jede VMware Cloud Director-Zelle im Netzwerk erreichbar sein.
- 3 Notieren Sie sich während der RabbitMQ-Installation folgende Werte, die Sie später beim Konfigurieren von VMware Cloud Director für die Zusammenarbeit mit dieser RabbitMQ-Installation bereitstellen müssen:
 - Den vollqualifizierten Domännennamen des RabbitMQ-Serverhosts, z. B. *amqp.example.com*.
 - Eine zur Authentifizierung mit RabbitMQ gültige Kombination aus Benutzername und Kennwort.
 - Den Port, über den der Broker Nachrichten empfängt. Der Standardwert lautet `5672` für nicht Nicht-SSL. Der Standardport für SSL/TLS lautet `5671`.
 - Das Kommunikationsprotokoll ist TCP.
 - Den virtuellen RabbitMQ-Host. Der Standardwert ist `"/`.

Nächste Schritte

Der AMQP-Dienst von VMware Cloud Director versendet standardmäßig unverschlüsselte Nachrichten. Sie können den AMQP-Dienst so konfigurieren, dass diese Nachrichten mit SSL verschlüsselt werden. Sie können den Dienst auch so konfigurieren, dass er das Broker-Zertifikat überprüft, indem Sie den standardmäßigen JCEKS Trust Store der Java-Laufzeitumgebung auf der VMware Cloud Director-Zelle verwenden, normalerweise unter `$VCLLOUD_HOME/jre/lib/security/cacerts`.

Informationen zum Aktivieren von SSL mit dem AMQP-Dienst von VMware Cloud Director finden Sie unter [Konfigurieren eines AMQP Brokers](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Abonnieren von Ereignissen, Aufgaben und Metriken mithilfe eines MQTT-Clients

Mithilfe eines MQTT-Clients können Sie Meldungen zu VMware Cloud Director-Ereignissen und -Aufgaben abonnieren.

MQTT ist ein schlankes, binäres Nachrichtentransportprotokoll. VMware Cloud Director verwendet MQTT, um Informationen zu Ereignissen und Aufgaben zu veröffentlichen, die Sie mithilfe eines MQTT-Clients abonnieren können. MQTT-Nachrichten durchlaufen einen MQTT-Broker, der Nachrichten auch speichern kann, falls die Clients nicht online sind.

Ab VMware Cloud Director 10.2.2 können Sie einen MQTT-Client zum Abonnieren von Metriken verwenden.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen MQTT-Client verfügen, der WebSocket unterstützt.
- Stellen Sie sicher, dass Sie einer von WebSocket aktualisierten Anforderung Kopfzeilen hinzufügen können.
- Wenn Sie Metriken abonnieren möchten, konfigurieren Sie die Metrikerfassung und aktivieren Sie die Veröffentlichung von Metriken. Weitere Informationen finden Sie im [Konfigurieren der Erfassung und Veröffentlichung von Metriken](#).

Verfahren

- 1 Melden Sie sich mithilfe des OpenAPI-Endpoints bei VMware Cloud Director an.

- Legen Sie zum Herstellen einer WebSocket-Verbindung die Eigenschaft „Sec-WebSocket-Protocol“ auf `mqtt` fest. Legen Sie weiterhin fest, dass der Client die Verbindung über den Pfad `/messaging/mqtt` herstellt, fügen Sie einen Autorisierungs-Header hinzu und befolgen Sie den standardmäßigen MQTT-Verbindungs-Flow.

Sie erhalten das JWT-Token über die standardmäßige Anmeldungsanforderung an VMware Cloud Director. Sie können den Benutzernamen und das Kennwort leer lassen.

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

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

- Nachdem die Verbindung hergestellt wurde, können Sie über den MQTT-Client Themen abonnieren.

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

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

Organisationsadministratoren können mithilfe von Platzhaltern auf alle organisationsbezogenen Themen zugreifen.

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

Systemadministratoren können mithilfe von Platzhaltern auf alle Themen zugreifen.

```
publish/#
```

- (Optional) Abonnieren Sie Metriken für VMware Cloud Director 10.2.2 oder höher.

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

Nur **Systemadministratoren** können auf das Metrikthema zugreifen.

Automatische Skalierungsgruppen

Ab VMware Cloud Director 10.2.2 können Sie Mandantenbenutzern die automatische Skalierung von Anwendungen in Abhängigkeit von der aktuellen CPU- und Speichernutzung ermöglichen.

Je nach den vordefinierten Kriterien für die CPU- und Arbeitsspeichernutzung können Mandanten VMware Cloud Director verwenden, um die Anzahl der VMs in einer ausgewählten Skalierungsgruppe automatisch hoch- oder herunterzuskalieren. Damit Mandanten Anwendungen automatisch skalieren können, müssen Sie die automatische Skalierungslösung konfigurieren, veröffentlichen und Zugriff darauf gewähren.

Zum Ausgleichen der Serverlast, die Sie zum Ausführen derselben Anwendung konfigurieren, können Sie VMware NSX Advanced Load Balancer (Avi Networks) verwenden.

Konfigurieren und Veröffentlichen des Plug-Ins für automatische Skalierung

Bevor Sie Mandanten Zugriff gewähren, müssen Sie die Lösung für die automatische Skalierung von Gruppen konfigurieren. Sie können die automatische Skalierung ab VMware Cloud Director 10.2.2 verwenden.

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem einer beliebigen Zelle im Cluster als **root** an.
- 2 Aktivieren Sie die Erfassung von Metrikdaten, indem Sie die Metrikerfassung in einer Cassandra-Datenbank einrichten oder Metriken ohne Metrikdatenpersistenz erfassen.

- [Installieren und Konfigurieren einer Cassandra-Datenbank zum Speichern von historischen Metrikdaten](#)
- Zum Erfassen von Metrikdaten ohne Datenpersistenz führen Sie die folgenden Befehle aus:

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

- 3 Aktivieren Sie die Veröffentlichung von Metriken.

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

- 4 Erstellen Sie eine Datei vom Typ `metrics.groovy` im Verzeichnis `/tmp` mit folgenden Inhalten.

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
        historicInterval=20
        entity="VM"
        instance=""
        minReportingInterval=300
        aggregator="AVERAGE"
    }
}
```

- 5 Importieren Sie die Datei.

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

- 6 Wenn Sie Cassandra zuvor konfiguriert haben, aktualisieren Sie das Cassandra-Schema, indem Sie die Adressen der Knoten, die Datenbankauthentifizierungsdetails sowie die Port- und Metriklebensdauer in Tagen korrekt angeben.

```
$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 Wenn Sie die Zelle mit einem von einer Zertifizierungsstelle signierten Zertifikat ausführen, verwenden Sie den folgenden Befehl zum Aktivieren der automatischen Skalierung.

```
$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>
```

Wenn Sie den Befehl über das Terminal ausführen, verwenden Sie als Escape-Zeichen für alle Sonderzeichen den umgekehrten Schrägstrich (\).

- 8 Starten Sie die Zelle neu.

```
service vmware-vcd restart
```

- 9 [Veröffentlichen des Rechtepakets für die automatische Skalierung](#)

Veröffentlichen des Rechtepakets für die automatische Skalierung

Wenn Mandanten Anwendungen automatisch skalieren sollen, müssen Sie das Rechtepaket für eine oder mehrere Organisationen in Ihrem System veröffentlichen. Sie können die automatische Skalierung ab VMware Cloud Director 10.2.2 verwenden.

Voraussetzungen

[Konfigurieren und Veröffentlichen des Plug-Ins für automatische Skalierung](#)

Verfahren

- 1 Wählen Sie in der oberen Navigationsleiste **Administration** aus.
- 2 Wählen Sie im linken Bereich unter **Zugriffssteuerung Mandant** die Option **Rechtepakete** aus.
- 3 Stellen Sie sicher, dass keine **Legacy-Rechtepakete** für die Mandantenorganisationen vorhanden sind, denen Zugriff auf die automatische Skalierung gewährt werden soll.
- 4 Wählen Sie das Paket **vmware:scalegroup Entitlement** aus und klicken Sie auf **Veröffentlichen**.
- 5 So veröffentlichen Sie das Paket:
 - a Wählen Sie **An Mandanten veröffentlichen**.
 - b Wählen Sie die Organisationen aus, für welche die Rolle veröffentlicht werden soll.
 - Wenn Sie das Paket für alle vorhandenen und neu erstellten Organisationen in Ihrem System veröffentlichen möchten, aktivieren Sie **An alle Mandanten veröffentlichen**.
 - Wenn Sie das Paket für bestimmte Organisationen in Ihrem System veröffentlichen möchten, wählen Sie die Organisationen einzeln aus.
- 6 Klicken Sie auf **Speichern**.

Nächste Schritte

Fügen Sie die notwendigen **VMWARE:SCALEGROUP**-Rechte zu den Mandantenrollen hinzu, die Skalierungsgruppen verwenden sollen. Weitere Informationen finden Sie unter [Anzeigen und Bearbeiten einer globalen Mandantenrolle](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Upgrade von VMware Cloud Director unter Linux

Für das Upgrade von VMware Cloud Director auf eine neue Version fahren Sie die VMware Cloud Director-Dienste in allen Zellen der Servergruppe herunter, installieren die neue Version auf allen Servern, aktualisieren die VMware Cloud Director-Datenbank und starten die VMware Cloud Director-Zellen neu.

Wenn Ihre vorhandene VMware Cloud Director-Servergruppe aus VMware Cloud Director-Installationen unter Linux besteht, können Sie das VMware Cloud Director-Installationsprogramm für Linux zum Aktualisieren Ihrer Umgebung verwenden.

Für VMware Cloud Director-Installationen unter Linux können Sie entweder ein abgestimmtes Upgrade durchführen oder VMware Cloud Director manuell aktualisieren. Weitere Informationen finden Sie in [Durchführen eines koordinierten Upgrades einer VMware Cloud Director-Installation](#) oder [Manuelles Upgrade einer VMware Cloud Director-Installation](#). Bei einem koordinierten Upgrade führen Sie einen einzelnen Befehl aus, mit dem alle Zellen in der Servergruppe und die Datenbank aktualisiert werden. Bei einem manuellen Upgrade aktualisieren Sie die einzelnen Zellen und die Datenbank der Reihe nach.

Ab VMware Cloud Director 9.5:

- Oracle-Datenbanken werden nicht unterstützt. Wenn Ihre vorhandene VMware Cloud Director-Installation eine Oracle-Datenbank verwendet, finden Sie weitere Informationen in der Tabelle [Upgrade-Pfade und -Workflows](#).
- Das Aktivieren und Deaktivieren von ESXi-Hosts wird nicht unterstützt. Bevor Sie das Upgrade starten, müssen Sie alle ESXi-Hosts aktivieren. Sie können die ESXi-Hosts unter Verwendung von vSphere Client in den Wartungsmodus versetzen.
- VMware Cloud Director verwendet Java mit verbesserter LDAP-Unterstützung. Um bei Verwendung eines LDAPS-Servers Fehler bei der LDAP-Anmeldung zu vermeiden, müssen Sie sich vergewissern, dass Sie über ein ordnungsgemäß erstelltes Zertifikat verfügen. Weitere Informationen finden Sie in den *Java 8-Versionsänderungen* unter <https://www.java.com>.

Ab VMware Cloud Director 10.0 werden Microsoft SQL Server-Datenbanken nicht mehr unterstützt.

Wenn Sie ein Upgrade von VMware Cloud Director durchführen, muss die neue Version mit den folgenden Komponenten Ihrer vorhandenen Installation kompatibel sein:

- Mit der Datenbanksoftware, die Sie derzeit für die VMware Cloud Director-Datenbank verwenden. Weitere Informationen finden Sie in der Tabelle „Upgrade- und Migrationspfade“.
- Mit der derzeit verwendeten VMware vSphere[®]-Version.

- Mit der derzeit verwendeten VMware NSX®-Version.
- Alle Drittanbieterkomponenten, die direkt mit VMware Cloud Director interagieren.

Informationen zur Kompatibilität von VMware Cloud Director mit anderen VMware-Produkten und mit Datenbanken von Drittanbietern finden Sie in den *VMware-Produkt-Interoperabilitätstabellen* unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. Wenn Sie vSphere- oder NSX-Komponenten als Teil des VMware Cloud Director-Upgrades aktualisieren möchten, müssen Sie diese Upgrades nach dem Upgrade von VMware Cloud Director durchführen. Weitere Informationen finden Sie unter [Nach dem Upgrade von VMware Cloud Director](#).

Nach dem Upgrade mindestens eines VMware Cloud Director-Servers können Sie die VMware Cloud Director-Datenbank aktualisieren. In der Datenbank werden Informationen über den Laufzeitstatus des Servers gespeichert. Dazu gehören auch die Status aller VMware Cloud Director-Aufgaben, die auf ihm ausgeführt werden. Um sicherzustellen, dass nach einem Upgrade keine ungültigen Aufgabeninformationen in der Datenbank verbleiben, müssen Sie sich vergewissern, dass auf keinem Server Aufgaben aktiv sind, bevor Sie mit dem Upgrade beginnen.

Das Upgrade behält die folgenden Artefakte bei, die nicht in der VMware Cloud Director-Datenbank gespeichert sind:

- Lokale und globale Eigenschaftendateien werden in die neue Installation kopiert.
- Zur Unterstützung der Gastanpassung verwendete Microsoft-Sysprep-Dateien werden in die neue Installation kopiert.

Damit alle Server in der Servergruppe und die Datenbank aktualisiert werden können, muss VMware Cloud Director für eine gewisse Zeit heruntergefahren werden. Wenn Sie einen Lastausgleichsdienst verwenden, kann dieser so konfiguriert werden, dass eine Meldung mit folgendem oder ähnlichem Inhalt angezeigt wird: `Das System steht wegen eines Upgrades nicht zur Verfügung.`

Ab Version 10.1 können Dienstanbieter und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Verweigerungsliste interner Hosts, die für Mandanten, die die VMware

Cloud Director-API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Verweigerungsliste, nachdem Sie die Installation oder das Upgrade von VMware Cloud Director durchgeführt haben und bevor Sie Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie im [Konfigurieren einer Negativliste für Testverbindungen](#).

Wichtig Nach dem Upgrade auf Version 10.1 und höher überprüft VMware Cloud Director immer die Zertifikate für alle mit ihm verbundenen Infrastruktur-Endpoints. Der Grund hierfür besteht darin, dass die Verwaltung von SSL-Zertifikaten durch VMware Cloud Director geändert wurde. Wenn Sie die Zertifikate vor dem Upgrade nicht in VMware Cloud Director importieren, kommt es in vCenter Server- und NSX-Verbindungen aufgrund von Problemen bei der SSL-Überprüfung möglicherweise zu fehlgeschlagenen Verbindungen. In diesem Fall haben Sie nach dem Upgrade zwei Möglichkeiten:

- 1 Führen Sie den Befehl `trust-infra-certs` des Zellenverwaltungstools aus, um automatisch alle Zertifikate in den zentralisierten Zertifikatspeicher zu importieren. Weitere Informationen finden Sie unter [Importieren von Endpoint-Zertifikaten aus vSphere-Ressourcen](#).
- 2 Wählen Sie in der Service Provider Admin Portal-Benutzeroberfläche jede vCenter Server- und NSX-Instanz aus und geben Sie die Anmeldedaten beim Akzeptieren des Zertifikats erneut ein.

Upgrade-Pfade und -Workflows

Quellumgebung	Zielumgebung
	VMware Cloud Director 10.2 unter Linux mit einer externen PostgreSQL-Datenbank
VMware Cloud Director 9.7 unter Linux mit einer externen Microsoft SQL Server-Datenbank	<ol style="list-style-type: none"> 1 Migrieren Sie die Microsoft SQL Server-Datenbank auf eine PostgreSQL-Datenbank. Weitere Informationen finden Sie unter PostgreSQL-Datenbank migrieren. 2 Aktualisieren Sie Ihre Umgebung auf VMware Cloud Director 10.2 unter Linux. Siehe Durchführen eines koordinierten Upgrades einer VMware Cloud Director-Installation oder Manuelles Upgrade einer VMware Cloud Director-Installation.
VMware Cloud Director 9.7, 10.0 oder 10.1 unter Linux mit einer externen PostgreSQL-Datenbank	Aktualisieren Sie Ihre Umgebung auf VMware Cloud Director 10.2 unter Linux. Siehe Durchführen eines koordinierten Upgrades einer VMware Cloud Director-Installation oder Manuelles Upgrade einer VMware Cloud Director-Installation .
VMware Cloud Director-Appliance 9.7, 10.0 oder 10.1 mit einer eingebetteten PostgreSQL-Datenbank	Nicht unterstützt

Durchführen eines koordinierten Upgrades einer VMware Cloud Director-Installation

Sie können alle Zellen in der Servergruppe mit der gemeinsam genutzten Datenbank aktualisieren, indem Sie das VMware Cloud Director-Installationsprogramm mit der Option `--private-key-path` ausführen.

Sie können das VMware Cloud Director-Installationsprogramm für Linux zur Aktualisierung einer VMware Cloud Director-Servergruppe verwenden, die aus VMware Cloud Director-Installationen auf einem unterstützten Linux-Betriebssystem besteht. Wenn die VMware Cloud Director-Servergruppe aus Bereitstellungen von VMware Cloud Director 9.5-Appliances besteht, verwenden Sie das VMware Cloud Director-Installationsprogramm für Linux, um die vorhandene Umgebung nur als Teil des Migrations-Workflows zu aktualisieren. Weitere Informationen finden Sie im [Upgrade und Migration der VMware Cloud Director-Appliance](#).

VMware Cloud Director für Linux wird als digital signierte ausführbare Datei mit einem Namen im Format `vmware-vcloud-director-distribution-v.verteilt.v.v-nnnnnn.bin` verteilt, wobei `v.v.v` die Produktversion und `nnnnnn` die Build-Nummer darstellt. Beispiel: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Durch Ausführen dieser ausführbaren Datei wird VMware Cloud Director installiert oder aktualisiert.

Wenn Sie das VMware Cloud Director-Installationsprogramm mit der Option `--private-key-path` ausführen, können Sie weitere Befehlsoptionen des `upgrade`-Dienstprogramms hinzufügen. Beispiel: `--maintenance-cell`. Informationen zu den Optionen des Datenbank-`upgrade`-Dienstprogramms finden Sie unter [Referenz zum Datenbank-Upgrade-Dienstprogramm](#).

Voraussetzungen

- Vergewissern Sie sich, dass Ihre VMware Cloud Director-Datenbank, die vSphere-Komponenten und die NSX-Komponenten mit der neuen Version von VMware Cloud Director kompatibel sind.

Wichtig Wenn bei Ihrer vorhandenen VMware Cloud Director-Installation eine Oracle- oder Microsoft SQL Server-Datenbank verwendet wird, stellen Sie sicher, dass Sie diese vor dem Upgrade zu einer PostgreSQL-Datenbank migriert haben. Die möglichen Upgrade-Pfade finden Sie unter [Upgrade von VMware Cloud Director unter Linux](#).

- Überprüfen Sie, ob Sie die für den Zielsystem benötigten Superuser-Anmeldeinformationen besitzen.
- Laden Sie den öffentlichen Schlüssel von VMware auf den Zielsystem herunter und installieren Sie ihn, wenn das Installationsprogramm die digitale Signatur der Installationsdatei überprüfen soll. Wenn Sie die digitale Signatur der Installationsdatei bereits überprüft haben, müssen Sie sie nicht erneut während der Installation überprüfen. Weitere Informationen finden Sie unter [Herunterladen und Installieren des öffentlichen Schlüssels von VMware](#).
- Vergewissern Sie sich, dass Sie über einen gültigen Lizenzschlüssel verfügen, um die Version der VMware Cloud Director-Software zu verwenden, auf die Sie ein Upgrade durchführen.

- Vergewissern Sie sich, dass alle Zellen SSH-Verbindungen vom Superuser ohne Eingabe eines Kennworts zulassen. Um eine Überprüfung durchzuführen, können Sie den folgenden Linux-Befehl ausführen:

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

In diesem Beispiel wird Ihre Identität auf `vcloud` festgelegt. Anschließend wird eine SSH-Verbindung mit der Zelle unter `cell-ip` als Root hergestellt, jedoch kein Root-Kennwort angegeben. Wenn der private Schlüssel in `private-key-path` in der lokalen Zelle vom Benutzer `vcloud.vcloud` gelesen werden kann und der entsprechende öffentliche Schlüssel in der Datei `authorized-keys` für den Root-Benutzer unter `cell-ip` vorhanden ist, wird der Befehl erfolgreich ausgeführt.

Hinweis Der Benutzer `vcloud`, die Gruppe `vcloud` und das Konto `vcloud.vcloud` werden vom VMware Cloud Director-Installationsprogramm zur Verwendung als Identität erstellt, mit der VMware Cloud Director-Prozesse ausgeführt werden. Der Benutzer `vcloud` hat kein Kennwort.

- Überprüfen Sie, ob alle ESXi-Hosts aktiviert sind. Deaktivierte ESXi-Hosts werden nicht unterstützt.
- Stellen Sie sicher, dass alle Server in der Servergruppe auf den freigegebenen Speicher des Übertragungsservers zugreifen können. Weitere Informationen finden Sie unter [Vorbereiten des Übertragungsserverspeichers für VMware Cloud Director unter Linux](#).
- Wenn Ihre VMware Cloud Director-Installation einen LDAPS-Server verwendet, stellen Sie sicher, dass Sie über ein korrekt erstelltes Zertifikat für Java 8 Update 181 verfügen, um LDAP-Anmeldefehler nach dem Upgrade zu vermeiden. Weitere Informationen finden Sie in den [Java 8-Versionsänderungen](#) unter <https://www.java.com>.

Verfahren

- 1 Melden Sie sich beim Zielsystem als **root** an.
- 2 Laden Sie die Installationsdatei auf den Zielsystem herunter.

Wenn Sie die Software auf einem Medium gekauft haben, kopieren Sie die Installationsdatei an einen Speicherort, auf den der Zielsystem zugreifen kann.

- 3 Überprüfen Sie, ob die Prüfsumme der heruntergeladenen Datei mit der auf der Downloadseite angezeigten Prüfsumme übereinstimmt.

Die Download-Seite stellt jeweils einen Wert für die MD5- und die SHA1-Prüfsumme zur Verfügung. Verwenden Sie das geeignete Tool, um zu überprüfen, ob die Prüfsumme der heruntergeladenen Installationsdatei mit der Prüfsumme der Downloadseite übereinstimmt. Ein Linux-Befehl mit dem folgenden Format zeigt die Prüfsumme für *Installationsdatei* an.

```
[root@cell11 /tmp]# md5sum installation-file
```

Der Befehl gibt die Prüfsumme der Installationsdatei zurück, die mit der MD5-Prüfsumme von der Downloadseite übereinstimmen muss.

4 Stellen Sie sicher, dass die Installationsdatei ausführbar ist.

Die Installationsdatei erfordert die Berechtigung **execute**. Um sicherzustellen, dass sie diese Berechtigung besitzt, öffnen Sie ein Konsolen-, Shell- oder Terminalfenster, und führen Sie den folgenden Linux-Befehl aus, wobei *installation-file* der vollständige Pfadname zur VMware Cloud Director-Installationsdatei ist.

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

5 Führen Sie in einem Konsolen-, Shell- oder Terminalfenster die Installationsdatei mit der Option `--private-key-path` und dem Pfadnamen des privaten Schlüssels der Zielzelle aus.

Sie können weitere Befehloptionen des Datenbank-upgrade-Dienstprogramms hinzufügen.

```
./installation-file --private-key-path /vcloud/.ssh/id_rsa
```

Hinweis Sie können die Installationsdatei nicht von einem Verzeichnis ausführen, dessen Pfadname Leerzeichen einschließt.

Das Installationsprogramm erkennt eine frühere Version von VMware Cloud Director und fordert Sie auf, das Upgrade zu bestätigen.

Wenn das Installationsprogramm eine Version von VMware Cloud Director erkennt, die identisch mit der Version der Installationsdatei oder neuer ist, zeigt es eine Fehlermeldung an und wird beendet.

6 Geben Sie **y** ein und drücken Sie die Eingabetaste, um das Upgrade zu bestätigen.

Ergebnisse

Das Installationsprogramm startet den folgenden Upgrade-Workflow für mehrere Zellen.

- 1 Es überprüft, ob der aktuelle Zellhost alle Anforderungen erfüllt.
- 2 Es entpackt das VMware Cloud Director-RPM-Paket.
- 3 Es führt ein Upgrade der VMware Cloud Director-Software auf der aktuellen Zelle aus.
- 4 Es aktualisiert die VMware Cloud Director-Datenbank.
- 5 Es aktualisiert VMware Cloud Director-Software in allen verbleibenden Zellen und startet dann VMware Cloud Director-Dienste in der Zelle neu.
- 6 Es startet die VMware Cloud Director-Dienste auf der aktuellen Zelle neu.

Nächste Schritte

Starten Sie die VMware Cloud Director-Dienste in allen Zellen in der Servergruppe.

Sie können jetzt das Verfahren [Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist](#) und anschließend das Verfahren [Upgrade von vCenter Server-Systemen, ESXi-Hosts und NSX Edges](#) durchführen.

Manuelles Upgrade einer VMware Cloud Director-Installation

Sie können eine einzelne Zelle durch Ausführen des Installationsprogramms von VMware Cloud Director ohne Befehlsoptionen aktualisieren. Bevor Sie eine aktualisierte Zelle neu starten, müssen Sie das Datenbankschema aktualisieren. Sie aktualisieren das Datenbankschema nach dem Upgrade von mindestens einer Zelle in der Servergruppe.

Sie können das VMware Cloud Director-Installationsprogramm für Linux zur Aktualisierung einer VMware Cloud Director-Servergruppe verwenden, die aus VMware Cloud Director-Installationen auf einem unterstützten Linux-Betriebssystem besteht. Wenn die VMware Cloud Director-Servergruppe aus Bereitstellungen von VMware Cloud Director 9.5-Appliances besteht, verwenden Sie das VMware Cloud Director-Installationsprogramm für Linux, um die vorhandene Umgebung nur als Teil des Migrations-Workflows zu aktualisieren. Weitere Informationen finden Sie im [Upgrade und Migration der VMware Cloud Director-Appliance](#).

Statt die einzelnen Zellen und die Datenbank der Reihe nach manuell zu aktualisieren, können Sie bei einer VMware Cloud Director-Installation mit mehreren Zellen ein abgestimmtes Upgrade der VMware Cloud Director-Installation vornehmen. Weitere Informationen finden Sie unter [Durchführen eines koordinierten Upgrades einer VMware Cloud Director-Installation](#).

Voraussetzungen

- Vergewissern Sie sich, dass Ihre VMware Cloud Director-Datenbank, die vSphere-Komponenten und die NSX-Komponenten mit der neuen Version von VMware Cloud Director kompatibel sind.

Wichtig Wenn bei Ihrer vorhandenen VMware Cloud Director-Installation eine Oracle- oder Microsoft SQL Server-Datenbank verwendet wird, stellen Sie sicher, dass Sie diese vor dem Upgrade zu einer PostgreSQL-Datenbank migriert haben. Die möglichen Upgrade-Pfade finden Sie unter [Upgrade von VMware Cloud Director unter Linux](#).

- Vergewissern Sie sich, dass Sie über Superuser-Anmeldeinformationen für die Server in Ihrer VMware Cloud Director-Servergruppe verfügen.
- Laden Sie den öffentlichen Schlüssel von VMware auf den Zielsystem herunter und installieren Sie ihn, wenn das Installationsprogramm die digitale Signatur der Installationsdatei überprüfen soll. Wenn Sie die digitale Signatur der Installationsdatei bereits überprüft haben, müssen Sie sie nicht erneut während der Installation überprüfen. Weitere Informationen finden Sie unter [Herunterladen und Installieren des öffentlichen Schlüssels von VMware](#).
- Vergewissern Sie sich, dass Sie über einen gültigen Lizenzschlüssel verfügen, um die Version der VMware Cloud Director-Software zu verwenden, auf die Sie ein Upgrade durchführen.

- Überprüfen Sie, ob alle ESXi-Hosts aktiviert sind. Deaktivierte ESXi-Hosts werden nicht unterstützt.

Verfahren

1 Upgrade einer VMware Cloud Director-Zelle

Das VMware Cloud Director-Installationsprogramm überprüft, ob der Zielserver alle Upgrade-Voraussetzungen erfüllt, und aktualisiert die VMware Cloud Director-Software auf dem Server.

2 Aktualisieren der VMware Cloud Director-Datenbank

Auf einem aktualisierten VMware Cloud Director-Server können Sie ein Tool ausführen, mit dem die VMware Cloud Director-Datenbank aktualisiert wird. Aktualisierte VMware Cloud Director-Server dürfen nicht neu gestartet werden, bevor die gemeinsam genutzte Datenbank aktualisiert wurde.

Nächste Schritte

- Nachdem Sie alle VMware Cloud Director-Server in der Servergruppe und die Datenbank aktualisiert haben, können Sie die VMware Cloud Director-Dienste für alle Zellen starten.
- [Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist](#)
- Nach dem Upgrade der einzelnen NSX Manager können Sie die vCenter Server-Systeme, -Hosts und NSX-Edges aktualisieren. Weitere Informationen finden Sie unter [Upgrade von vCenter Server-Systemen, ESXi-Hosts und NSX Edges](#).

Upgrade einer VMware Cloud Director-Zelle

Das VMware Cloud Director-Installationsprogramm überprüft, ob der Zielserver alle Upgrade-Voraussetzungen erfüllt, und aktualisiert die VMware Cloud Director-Software auf dem Server.

VMware Cloud Director für Linux wird als digital signierte ausführbare Datei mit einem Namen im Format `vmware-vccloud-director-distribution-v.v.v-nnnnnn.bin` verteilt, wobei `v.v.v` die Produktversion und `nnnnnn` die Build-Nummer darstellt. Beispiel: `vmware-vccloud-director-distribution-8.10.0-3698331.bin`. Durch Ausführen dieser ausführbaren Datei wird VMware Cloud Director installiert oder aktualisiert.

Bei einer VMware Cloud Director-Installation mit mehreren Zellen müssen Sie das VMware Cloud Director-Installationsprogramm für jedes Mitglied der VMware Cloud Director-Servergruppe ausführen.

Verfahren

- 1 Melden Sie sich beim Zielserver als **root** an.
- 2 Laden Sie die Installationsdatei auf den Zielserver herunter.

Wenn Sie die Software auf einem Medium gekauft haben, kopieren Sie die Installationsdatei an einen Speicherort, auf den der Zielserver zugreifen kann.

- 3 Überprüfen Sie, ob die Prüfsumme der heruntergeladenen Datei mit der auf der Downloadseite angezeigten Prüfsumme übereinstimmt.

Die Download-Seite stellt jeweils einen Wert für die MD5- und die SHA1-Prüfsumme zur Verfügung. Verwenden Sie das geeignete Tool, um zu überprüfen, ob die Prüfsumme der heruntergeladenen Installationsdatei mit der Prüfsumme der Downloadseite übereinstimmt. Ein Linux-Befehl mit dem folgenden Format zeigt die Prüfsumme für *Installationsdatei* an.

```
[root@cell11 /tmp]# md5sum installation-file
```

Der Befehl gibt die Prüfsumme der Installationsdatei zurück, die mit der MD5-Prüfsumme von der Downloadseite übereinstimmen muss.

- 4 Stellen Sie sicher, dass die Installationsdatei ausführbar ist.

Die Installationsdatei erfordert die Berechtigung **execute**. Um sicherzustellen, dass sie diese Berechtigung besitzt, öffnen Sie ein Konsolen-, Shell- oder Terminalfenster, und führen Sie den folgenden Linux-Befehl aus, wobei *installation-file* der vollständige Pfadname zur VMware Cloud Director-Installationsdatei ist.

```
[root@cell11 /tmp]# chmod u+x installation-file
```

- 5 Führen Sie die Installationsdatei aus.

Um die Installationsdatei auszuführen, geben Sie den vollständigen Pfadnamen ein, z. B.:

```
[root@cell11 /tmp]# ./Installationdatei
```

Diese Datei enthält ein Installationsskript und ein eingebettetes RPM-Paket.

Hinweis Sie können die Installationsdatei nicht von einem Verzeichnis ausführen, dessen Pfadname Leerzeichen einschließt.

Wenn das Installationsprogramm eine Version von VMware Cloud Director erkennt, die identisch mit der Version der Installationsdatei oder neuer ist, zeigt es eine Fehlermeldung an und wird beendet.

Wenn das Installationsprogramm eine frühere Version von VMware Cloud Director erkennt, werden Sie aufgefordert, das Upgrade zu bestätigen.

- 6 Geben Sie **y** ein und drücken Sie die Eingabetaste, um das Upgrade zu bestätigen.

Das Installationsprogramm startet den folgenden Upgrade-Workflow.

- a Es überprüft, ob der Host alle Anforderungen erfüllt.
- b Es entpackt das VMware Cloud Director-RPM-Paket.
- c Nachdem alle aktiven VMware Cloud Director-Aufgaben auf der Zelle abgeschlossen sind, beendet es die VMware Cloud Director-Dienste auf dem Server und aktualisiert die installierte VMware Cloud Director-Software.

Wenn Sie den öffentlichen Schlüssel von VMware nicht auf dem Zielsystem installiert haben, zeigt das Installationsprogramm eine Warnung der folgenden Art an:

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

Wenn Sie die vorhandene `global.properties`-Datei auf dem Zielsystem ändern, zeigt das Installationsprogramm eine Warnung der folgenden Art an:

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-director/etc/global.properties.rpmnew
```

Hinweis Wenn Sie die vorhandene `global.properties`-Datei zuvor aktualisiert haben, können Sie die Änderungen aus `global.properties.rpmnew` abrufen.

7 (Optional) Aktualisieren Sie die Protokollierungseigenschaften.

Nach einer Aktualisierung werden neue Protokollierungseigenschaften in die Datei `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` geschrieben.

Option	Aktion
Wenn Sie vorhandene Protokollierungseigenschaften nicht geändert haben	Kopieren Sie diese Datei in <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> .
Wenn Sie Protokollierungseigenschaften geändert haben	Um Ihre Änderungen beizubehalten, führen Sie <code>/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew</code> mit der vorhandenen Datei <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> zusammen.

Ergebnisse

Wenn das VMware Cloud Director-Upgrade abgeschlossen ist, zeigt das Installationsprogramm eine Meldung mit Informationen zum Speicherort der alten Konfigurationsdateien an. Das Installationsprogramm fordert Sie dann auf, das Datenbank-Upgrade-Tool auszuführen.

Nächste Schritte

Sofern sie noch nicht aktualisiert wurde, können Sie die VMware Cloud Director-Datenbank aktualisieren.

Wiederholen Sie diesen Vorgang für jede VMware Cloud Director-Zelle in der Servergruppe.

Wichtig Starten Sie die VMware Cloud Director-Dienste erst, wenn alle Zellen in der Servergruppe und der Datenbank aktualisiert wurden.

Aktualisieren der VMware Cloud Director-Datenbank

Auf einem aktualisierten VMware Cloud Director-Server können Sie ein Tool ausführen, mit dem die VMware Cloud Director-Datenbank aktualisiert wird. Aktualisierte VMware Cloud Director-

Server dürfen nicht neu gestartet werden, bevor die gemeinsam genutzte Datenbank aktualisiert wurde.

Informationen über alle ausgeführten und kürzlich abgeschlossenen Aufgaben werden in der VMware Cloud Director-Datenbank gespeichert. Da ein Datenbank-Upgrade diese Aufgabeninformationen ungültig macht, stellt das Datenbank-Upgrade-Dienstprogramm sicher, dass keine Aufgaben ausgeführt werden, wenn der Upgrade-Vorgang beginnt.

Alle Zellen in einer VMware Cloud Director-Servergruppe nutzen dieselbe Datenbank. Unabhängig davon, wie viele Zellen Sie aktualisieren, die Datenbank wird nur einmal aktualisiert. Nach dem Upgrade der Datenbank können nicht aktualisierte VMware Cloud Director-Zellen keine Verbindung zur Datenbank herstellen. Sie müssen ein Upgrade aller Zellen durchführen, um eine Verbindung mit der aktualisierten Datenbank herstellen zu können.

Voraussetzungen

- Sichern Sie Ihre vorhandene Datenbank. Gehen Sie dabei nach den Empfehlungen des Datenbanksoftwareherstellers vor.
- Überprüfen Sie, ob alle VMware Cloud Director-Zellen in der Servergruppe beendet wurden. Während des Aktualisierungsvorgangs werden die aktualisierten Zellen beendet. Wenn noch nicht aktualisierte VMware Cloud Director-Server vorhanden sind, können sie mit dem Zellenverwaltungstool stillgelegt und ihre Dienste heruntergefahren werden. Weitere Informationen zum Verwalten einer Zelle mithilfe des Zellenverwaltungstools finden Sie unter [Kapitel 5 Überblick über das Zellenverwaltungstool](#).
- Gehen Sie das Thema [Referenz zum Datenbank-Upgrade-Dienstprogramm](#) durch.

Verfahren

- 1 Führen Sie das `upgrade` -Dienstprogramm der Datenbank mit oder ohne Optionen aus.

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

Wenn das Datenbank-Upgrade-Dienstprogramm eine nicht kompatible Version von NSX Manager erkennt, wird eine Warnmeldung angezeigt und das Upgrade abgebrochen.

- 2 Geben Sie in der Eingabeaufforderung `y` ein und drücken Sie die Eingabetaste, um das Upgrade der Datenbank zu bestätigen.

- 3 Geben Sie in der Eingabeaufforderung `y` ein und drücken Sie die Eingabetaste, um zu bestätigen, dass Sie die Datenbank gesichert haben.

Wenn Sie die Option `--backup-completed` verwendet haben, überspringt das Dienstprogramm diese Eingabeaufforderung.

- 4 Wenn das Dienstprogramm eine aktive Zelle erkennt, geben Sie in der nächsten Eingabeaufforderung `n` ein, um die Shell zu beenden. Stellen Sie dann sicher, dass keine Zellen ausgeführt werden, und wiederholen Sie das Upgrade aus [Schritt 1](#).

Ergebnisse

Das Datenbank-Upgrade-Tool wird ausgeführt und zeigt Statusmeldungen an. Wenn das Upgrade abgeschlossen ist, werden Sie aufgefordert, den VMware Cloud Director-Dienst auf dem aktuellen Server zu starten.

Nächste Schritte

Geben Sie `y` ein und drücken Sie die Eingabetaste oder starten Sie den Dienst zu einem späteren Zeitpunkt durch Ausführen des Befehls `service vmware-vcd start`.

Sie können die Dienste der aktualisierten VMware Cloud Director-Server starten.

Sie können die restlichen VMware Cloud Director-Mitglieder der Servergruppe aktualisieren und ihre Dienste starten. Weitere Informationen finden Sie unter [Upgrade einer VMware Cloud Director-Zelle](#).

Referenz zum Datenbank-Upgrade-Dienstprogramm

Wenn Sie das Dienstprogramm `upgrade` ausführen, geben Sie die Setup-Informationen in der Befehlszeile als Optionen und Argumente an.

Der Speicherort des `upgrade`-Dienstprogramms ist `/opt/vmware/vcloud-director/bin/`.

Tabelle 4-3. Optionen und Argumente des Datenbank-Upgrade-Dienstprogramms

Option	Argument	Beschreibung
<code>--backup-completed</code>	Keines	Gibt an, dass Sie eine Sicherungskopie von VMware Cloud Director abgeschlossen haben. Wenn Sie diese Option hinzufügen, werden Sie vom Upgrade-Dienstprogramm nicht aufgefordert, die Datenbank zu sichern.
<code>--ceip-user</code>	Der Benutzername für das CEIP-Dienstkonto.	Wenn ein Benutzer mit diesem Benutzernamen bereits in der Systemorganisation vorhanden ist, schlägt das Upgrade fehl. Standard: <code>phone-home-system-account</code> .

Tabelle 4-3. Optionen und Argumente des Datenbank-Upgrade-Dienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
<code>--enable-ceip</code>	<p>Wählen Sie einen Typ aus:</p> <ul style="list-style-type: none"> ■ true ■ false 	<p>Gibt an, ob diese Installation am Programm zur Verbesserung der Kundenzufriedenheit (CEIP) von VMware teilnimmt. Wird, wenn nicht bereitgestellt, standardmäßig auf „true“ und nicht auf „false“ in der aktuellen Konfiguration festgelegt. Das Programm zur Verbesserung der Kundenzufriedenheit (CEIP) von VMware stellt zusätzliche Informationen in Bezug auf die durch CEIP erfassten Daten und die Zwecke, für die sie von VMware verwendet werden, bereit. Diese sind im Trust & Assurance Center unter http://www.vmware.com/trustvmware/ceip.html festgelegt. Mit dem Zellenverwaltungstool können Sie dem CEIP von VMware für dieses Produkt jederzeit beitreten bzw. dieses verlassen. Weitere Informationen finden Sie im Kapitel 5 Überblick über das Zellenverwaltungstool.</p>
<code>--installer-path</code>	<p>Vollständiger Pfadname der VMware Cloud Director-Installationsdatei. Die Installationsdatei und das Verzeichnis, in dem sie gespeichert ist, müssen für den Benutzer „vcloud.vcloud“ lesbar sein.</p>	<p>Erfordert die Option <code>--private-key-path</code> .</p>
<code>--maintenance-cell</code>	<p>IP-Adresse</p>	<p>Die IP-Adresse einer Zelle, damit das Upgrade-Dienstprogramm während des Upgrades im Wartungsmodus ausgeführt wird. Diese Zelle wechselt in den Wartungsmodus, bevor die anderen Zellen heruntergefahren werden, und bleibt im Wartungsmodus, während die anderen Zellen aktualisiert werden. Nachdem die anderen Zellen aktualisiert wurden und mindestens eine der Zeilen neu gestartet wurde, wird diese Zelle heruntergefahren und aktualisiert. Erfordert die Option <code>--private-key-path</code> .</p>

Tabelle 4-3. Optionen und Argumente des Datenbank-Upgrade-Dienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
<code>--multisite-user</code>	Der Benutzername für das Multi-Site-Systemkonto.	Dieses Konto wird von der VMware Cloud Director Multi-Site-Funktion verwendet. Wenn ein Benutzer mit diesem Benutzernamen bereits in der Systemorganisation vorhanden ist, schlägt das Upgrade fehl. Standard: <code>multisite-system-account</code> .
<code>--private-key-path</code>	Pfadname	Der vollständige Pfadname des privaten Schlüssels der Zelle. Wenn Sie diese Option verwenden, werden alle Zellen in der Servergruppe normal heruntergefahren, aktualisiert und neu gestartet, nachdem die Datenbank aktualisiert wurde. Unter Durchführen eines koordinierten Upgrades einer VMware Cloud Director-Installation finden Sie weitere Informationen zu diesem Upgrade-Workflow.
<code>--unattended-upgrade</code>	Keines	Gibt ein unbeaufsichtigtes Upgrade an

Wenn Sie die Option `--private-key-path` verwenden, müssen alle Zellen so konfiguriert sein, dass sie `ssh`-Verbindungen vom Superuser ohne die Eingabe eines Kennworts ermöglichen. Sie können eine Linux-Befehlszeile wie hier gezeigt verwenden, um dies zu überprüfen. In diesem Beispiel wird Ihre Identität auf `vcloud` festgelegt, dann wird eine `ssh`-Verbindung zur Zelle unter `cell-ip` als `root` hergestellt, jedoch kein Root-Kennwort angegeben.

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

Wenn der private Schlüssel in `private-key-path` auf der lokalen Zelle vom Benutzer `vcloud.vcloud` gelesen werden kann und der entsprechende öffentliche Schlüssel zur Datei `authorized-keys` für den Root-Benutzer unter `cell-ip` hinzugefügt wurde, ist der Befehl erfolgreich.

Hinweis Der Benutzer `vcloud`, die Gruppe `vcloud` und das Konto `vcloud.vcloud` werden vom VMware Cloud Director-Installationsprogramm zur Verwendung als Identität erstellt, mit der VMware Cloud Director-Prozesse ausgeführt werden. Der Benutzer `vcloud` hat kein Kennwort.

Nach dem Upgrade von VMware Cloud Director

Nach dem Upgrade aller VMware Cloud Director-Server und der gemeinsam genutzten Datenbank können Sie die NSX Manager-Instanzen aktualisieren, die Netzwerkdienste für Ihre

Cloud bereitstellen. Danach können Sie die ESXi-Hosts und die vCenter Server-Instanzen aktualisieren, die bei Ihrer VMware Cloud Director-Installation registriert sind.

Wichtig VMware Cloud Director unterstützt nur erweiterte Edge-Gateways. Sie müssen jedes ältere, nicht erweiterte Edge-Gateway in ein erweitertes Gateway konvertieren. Weitere Informationen finden Sie unter <https://kb.vmware.com/kb/66767>.

Ab Version 10.1 können Dienstanbieter und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen. Um VMware Cloud Director-Netzwerkverbindungen zu schützen, konfigurieren Sie eine Verweigerungsliste interner Hosts, die für Mandanten, die die VMware Cloud Director-API für Verbindungstests verwenden, nicht erreichbar sind. Konfigurieren Sie die Verweigerungsliste, nachdem Sie die Installation oder das Upgrade von VMware Cloud Director durchgeführt haben und bevor Sie Mandanten Zugriff auf VMware Cloud Director gewähren. Weitere Informationen finden Sie im [Konfigurieren einer Negativliste für Testverbindungen](#).

Wichtig Nach dem Upgrade auf Version 10.1 und höher überprüft VMware Cloud Director immer die Zertifikate für alle mit ihm verbundenen Infrastruktur-Endpoints. Der Grund hierfür besteht darin, dass die Verwaltung von SSL-Zertifikaten durch VMware Cloud Director geändert wurde. Wenn Sie die Zertifikate vor dem Upgrade nicht in VMware Cloud Director importieren, kommt es in vCenter Server- und NSX-Verbindungen aufgrund von Problemen bei der SSL-Überprüfung möglicherweise zu fehlgeschlagenen Verbindungen. In diesem Fall haben Sie nach dem Upgrade zwei Möglichkeiten:

- 1 Führen Sie den Befehl `trust-infra-certs` des Zellenverwaltungstools aus, um automatisch alle Zertifikate in den zentralisierten Zertifikatspeicher zu importieren. Weitere Informationen finden Sie unter [Importieren von Endpoint-Zertifikaten aus vSphere-Ressourcen](#).
- 2 Wählen Sie in der Service Provider Admin Portal-Benutzeroberfläche jede vCenter Server- und NSX-Instanz aus und geben Sie die Anmeldedaten beim Akzeptieren des Zertifikats erneut ein.

Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist

Bevor Sie ein Upgrade eines vCenter Server- und ESXi-Hosts durchführen, die bei VMware Cloud Director registriert sind, müssen Sie ein Upgrade einer jeden NSX Manager-Instanz durchführen, die mit diesem vCenter Server verbunden ist.

Durch das Durchführen eines Upgrades von NSX Manager wird der Zugriff auf administrative NSX-Funktionen unterbrochen, es werden jedoch keine Netzwerkdienste unterbrochen. Sie können ein Upgrade von NSX Manager durchführen, bevor oder nachdem Sie ein Upgrade von VMware Cloud Director durchgeführt haben. Dies ist unabhängig davon, ob VMware Cloud Director-Zellen ausgeführt werden.

Informationen zum Durchführen eines Upgrades von NSX finden Sie in der NSX for vSphere-Dokumentation unter <https://docs.vmware.com>.

Verfahren

- 1 Führen Sie ein Upgrade des NSX Manager durch, der mit jedem vCenter Server verknüpft ist, der bei der VMware Cloud Director-Installation registriert ist.
- 2 Nach dem Upgrade aller NSX Manager können Sie ein Upgrade der registrierten vCenter Server-Systeme und ESXi-Hosts durchführen.

Upgrade von vCenter Server-Systemen, ESXi-Hosts und NSX Edges

Nach dem Upgrade von VMware Cloud Director und NSX Manager müssen Sie das Upgrade der vCenter Server-Systeme und ESXi-Hosts durchführen, die bei VMware Cloud Director registriert sind. Nach dem Upgrade aller verbundenen vCenter Server-Systeme und ESXi-Hosts können Sie das Upgrade der NSX Edges durchführen.

Voraussetzungen

Stellen Sie sicher, dass Sie bereits ein Upgrade eines jeden NSX Manager durchgeführt haben, der den mit Ihrer Cloud verbundenen vCenter Server-Systemen zugeordnet ist. Weitere Informationen finden Sie unter [Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist](#).

Verfahren

- 1 Deaktivieren Sie die vCenter Server-Instanz.
 - a Wählen Sie in der oberen Navigationsleiste des VMware Cloud Director Service Provider Admin Portal unter **Ressourcen** die Option **vSphere-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **vCenter Server-Instanzen**.
 - c Wählen Sie das Optionsfeld neben der vCenter Server-Instanz aus, die Sie deaktivieren möchten, und klicken Sie auf **Deaktivieren**.
 - d Klicken Sie auf **OK**.
- 2 Führen Sie ein Upgrade des vCenter Server-Systems durch.

Informationen dazu finden Sie unter *Upgrade von vCenter Server*.
- 3 Verifizieren Sie alle öffentlichen VMware Cloud Director-URLs und Zertifikatsketten.
 - a Wählen Sie in der oberen Navigationsleiste **Administration** aus.
 - b Klicken Sie im linken Bereich unter **Einstellungen** auf **Öffentliche Adressen**.
 - c Überprüfen Sie alle öffentlichen Adressen.
- 4 Aktualisieren Sie die Registrierung von vCenter Server bei VMware Cloud Director.
 - a Wählen Sie in der oberen Navigationsleiste des VMware Cloud Director Service Provider Admin Portal unter **Ressourcen** die Option **vSphere-Ressourcen** aus.
 - b Klicken Sie im linken Bereich auf **vCenter Server-Instanzen**.

- c Wählen Sie das Optionsfeld neben dem gewünschten vCenter Server und klicken Sie auf **Erneut verbinden**.
 - d Klicken Sie auf **OK**.
- 5 Führen Sie ein Upgrade jedes ESXi-Hosts durch, den das aktualisierte vCenter Server-System unterstützt.

Weitere Informationen finden Sie unter *VMware ESXi-Upgrade*.

Wichtig Um sicherzustellen, dass Sie über ausreichend Hostkapazität zur Unterstützung der virtuellen Maschinen in Ihrer Cloud verfügen, aktualisieren Sie die Hosts jeweils in kleinen Gruppen. Bei diesem Vorgehen kann die Aktualisierung der Hostagenten rechtzeitig abgeschlossen werden, um eine Migration der virtuellen Maschinen zurück zum aktualisierten Host zu ermöglichen.

- a Verwenden Sie das vCenter Server-System, um den Host in den Wartungsmodus zu versetzen und zu ermöglichen, dass alle virtuellen Maschinen auf diesem Host auf einen anderen Host migriert werden.
 - b Aktualisieren Sie den Host.
 - c Verwenden Sie das vCenter Server-System, um die Verbindung zum Host wiederherzustellen.
 - d Verwenden Sie das vCenter Server-System, um den Wartungsmodus für den Host zu beenden.
- 6 (Optional) Führen Sie ein Upgrade der NSX Edges durch, die vom vCenter Server Manager verwaltet werden, der mit dem aktualisierten NSX-System verbunden ist.

Aktualisierte NSX Edges bieten bessere Leistung und Integration. Sie können entweder NSX Manager oder VMware Cloud Director für das Upgrade von NSX Edges verwenden.

- Informationen zur Verwendung von NSX Manager für das Upgrade von NSX Edges finden Sie in der NSX für vSphere-Dokumentation unter <https://docs.vmware.com/de/>.
- Um VMware Cloud Director für das Upgrade eines NSX-Edge-Gateways zu verwenden, müssen Sie das durch das Edge unterstützte VMware Cloud Director-Netzwerkobjekt verwenden:
 - Ein entsprechendes Upgrade eines Edge-Gateways findet automatisch statt, wenn Sie entweder VMware Cloud Director oder die VMware Cloud Director-API zum Zurücksetzen eines vom Edge-Gateway unterstützten Netzwerks verwenden.
 - Durch das erneute Bereitstellen eines Edge-Gateways wird ein Upgrade der zugeordneten NSX Edge-Appliance durchgeführt.

Hinweis Die erneute Bereitstellung wird nur für NSX Data Center for vSphere-Edge-Gateways unterstützt.

- Durch das Zurücksetzen eines vApp-Netzwerks von innerhalb des Kontexts der vApp wird ein Upgrade der diesem Netzwerk zugeordneten NSX Edge-Appliance durchgeführt. Um ein vApp-Netzwerk innerhalb des Kontexts einer vApp zurückzusetzen, navigieren Sie zur Registerkarte **Netzwerke** für die vApp, zeigen Sie die Netzwerkdetails an, klicken Sie auf das Optionsfeld neben dem Namen des vApp-Netzwerks und klicken Sie auf **Zurücksetzen**.

Weitere Informationen zum erneuten Bereitstellen von Edge-Gateways und zum Zurücksetzen von vApp-Netzwerken finden Sie im *VMware Cloud Director API-Programmierhandbuch*.

Nächste Schritte

Wiederholen Sie diesen Vorgang für die anderen vCenter Server-Systeme, die bei Ihrer VMware Cloud Director-Installation registriert sind.

Überblick über das Zellenverwaltungstool

5

Das Zellenverwaltungstool ist ein Befehlszeilendienstprogramm, mit dem Sie eine VMware Cloud Director-Zelle oder -Datenbank verwalten können. Für die meisten Vorgänge sind Superuser- oder Systemadministrator-Anmeldeinformationen erforderlich.

Das Zellenverwaltungstool ist unter `/opt/vmware/vcloud-director/bin/` installiert. Sie können es zur Ausführung eines Einzelbefehls oder als eine interaktive Shell verwenden.

Auflisten der verfügbaren Befehle

Wenn Sie die für das Zellenverwaltungstool verfügbaren Befehle auflisten möchten, verwenden Sie die folgende Befehlszeile:

```
./cell-management-tool -h
```

Verwenden des Shell-Modus

Sie können das Zellenverwaltungstool als eine interaktive Shell ausführen, indem Sie es wie im Folgenden gezeigt ohne Argumente aufrufen.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool
Cell Management Tool v8.14.0.4146350 Type "help" for available subcommands. cmt>
```

Im Shell-Modus können Sie an der Eingabeaufforderung `cmt>` wie im folgenden Beispiel verdeutlicht jeden beliebigen Befehl des Zellenverwaltungstools eingeben.

```
cmt>cell -h
usage: cell [options] -a,--application-states display the state of each application on
the cell [DEPRECATED - use the cell-application command instead] -h,--help print this
message -i,--pid <arg> the process id of the cell [REQUIRED if username is not specified]
-m,--maintenance <arg> gracefully enter maintenance mode on the cell -p,--password <arg>
administrator password [OPTIONAL] -q,--quiesce <arg> quiesce activity on the cell -s,--
shutdown gracefully shutdown the cell -t,--status display activity on the cell -tt,--
status-verbose display a verbose description of activity on the cell -u,--username <arg>
administrator username [REQUIRED if pid is not specified] Note: You will be prompted for
administrator password if not entered in command line. cmt>
```

Nach Ausführung des Befehls wird erneut die Eingabeaufforderung `cmt>` angezeigt. Um den Shell-Modus zu verlassen, geben Sie **exit** an der Eingabeaufforderung `cmt>` ein.

Beispiel: Hilfe zur Nutzung des Zellenverwaltungstools

In diesem Beispiel wird ein nicht interaktiver Einzelbefehl ausgeführt, mit dem verfügbare Befehle des Shell-Verwaltungstools aufgelistet werden.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
usage: cell-management-tool -h,--help print this message Available commands: cell -
Manipulates the Cell and core components certificates - Reconfigures the SSL certificates for
the cell . . . For command specific help: cell-management-tool <commandName> -h
```

- [Konfigurieren einer VMware Cloud Director-Installation](#)

Verwenden Sie den Befehl `system-setup` des Zellenverwaltungsprogramms, um die Datenbank der Servergruppe mit einem Systemadministratorkonto und zugehörigen Informationen zu initialisieren.

- [Deaktivieren des Dienstanbieterzugriffs auf den Legacy-API-Endpoint](#)

Ab VMware Cloud Director 10.0 können Sie separate VMware Cloud Director OpenAPI-Anmelde-Endpoints für den Dienstanbieter- und den Mandantenzugriff auf VMware Cloud Director verwenden.

- [Verwalten einer Zelle](#)

Mit dem Unterbefehl `cell` des Zellenverwaltungstools können Sie das Aufgabenplanungstool anhalten, damit keine neuen Aufgaben gestartet werden können, den Status aller aktiven Aufgaben anzeigen, den Zellenwartungsmodus steuern sowie die Zelle ordnungsgemäß herunterfahren.

- [Verwalten von Zellenanwendungen](#)

Verwenden Sie den Befehl `cell-application` des Zellenverwaltungstools zum Steuern des Satzes von Anwendungen, die die Zelle beim Starten ausführt.

- [Aktualisieren der Datenbankverbindungseigenschaften](#)

Sie können die Verbindungseigenschaften für die VMware Cloud Director-Datenbank mithilfe des Unterbefehls `reconfigure-database` des Zellenverwaltungstools aktualisieren.

- [Erkennen und Reparieren von beschädigten Scheduler-Daten](#)

VMware Cloud Director verwendet das Auftragsplanungstool Quartz zum Koordinieren von asynchronen Vorgängen (Aufträgen), die auf dem System ausgeführt werden. Wenn die Datenbank des Planungstools Quartz beschädigt wird, können Sie das System möglicherweise nicht erfolgreich stilllegen. Verwenden Sie den Befehl `fix-scheduler-data` des Zellenverwaltungstools zum Durchsuchen der Datenbank nach beschädigten Scheduler-Daten und reparieren Sie die Daten nach Bedarf.

- [Generieren von selbstsignierten Zertifikaten für die HTTPS- und Konsolenproxy-Endpoints](#)

Verwenden Sie den Befehl `generate-certs` des Zellenverwaltungstools, um selbstsignierte SSL-Zertifikate für die HTTPS- und Konsolenproxy-Endpoints zu generieren.

- **Ersetzen der Zertifikate für die HTTPS- und Konsolenproxy-Endpoints**

Verwenden Sie den Befehl `certificates` des Zellenverwaltungstools, um SSL-Zertifikate für die HTTPS- und Konsolenproxy-Endpoints zu ersetzen.
- **Importieren von SSL-Zertifikaten aus externen Diensten**

Verwenden Sie den Befehl `import-trusted-certificates` des Zellenverwaltungstools, um Zertifikate für den Aufbau sicherer Verbindungen zu externen Diensten wie AMQP und der VMware Cloud Director-Datenbank zu importieren.
- **Importieren von Endpoint-Zertifikaten aus vSphere-Ressourcen**

Verwenden Sie nach dem Upgrade den Befehl `trust-infra-certs` des Zellenverwaltungstools, um Zertifikate aus den vSphere-Ressourcen in der Umgebung zu erfassen und in die VMware Cloud Director-Datenbank zu importieren.
- **Konfigurieren einer Negativliste für Testverbindungen**

Verwenden Sie nach der Installation oder dem Upgrade den Befehl `manage-test-connection-blacklist` des Zellenverwaltungstools, um den Zugriff auf interne Hosts zu blockieren, bevor Sie Mandantenzugriff auf das VMware Cloud Director-Netzwerk gewähren.
- **Anzeigen des FIPS-Status aller aktiven Zellen**

Ab VMware Cloud Director 10.2.2 können Sie zum Sicherstellen des FIPS-Status aller aktiven VMware Cloud Director-Zellen den Befehl `fips-status` verwenden. Der Befehl zeigt nicht den FIPS-Status der VMware Cloud Director-Appliance an.
- **Verwalten der Liste zulässiger SSL-Verschlüsselungen**

Mit dem Befehl `ciphers` im Zellenverwaltungstool können Sie den Satz von Verschlüsselungsverfahren konfigurieren, den die Zelle während des SSL-Handshake-Vorgangs bereitstellt.
- **Verwalten der Liste der zulässigen SSL-Protokolle**

Um den Satz von SSL-Protokollen zu konfigurieren, die die Zelle während des SSL-Handshake-Vorgangs bietet, verwenden Sie den Befehl `ssl-protocols` des Zellenverwaltungstools.
- **Konfigurieren der Erfassung und Veröffentlichung von Metriken**

Sie können den Befehl `configure-metrics` des Zellenverwaltungstools verwenden, um den zu erfassenden Metriksatz zu konfigurieren.
- **Konfigurieren einer Cassandra-Metrikendatenbank**

Mit dem Befehl `cassandra` des Zellenverwaltungstools können Sie die Zelle mit einer optionalen Metrikdatenbank verbinden.
- **Wiederherstellen des Kennworts für den Systemadministrator**

Wenn Sie den Benutzernamen und das Kennwort für die VMware Cloud Director-Datenbank kennen, können Sie den Befehl `recover-password` des Zellenverwaltungstools verwenden, um das Kennwort des VMware Cloud Director-Systemadministrators wiederherzustellen.

- **Aktualisieren des Fehlerstatus einer Aufgabe**

Verwenden Sie den Befehl `fail-tasks` im Zellenverwaltungstool, um den Abschlussstatus zu aktualisieren, der mit Aufgaben verknüpft ist, die beim absichtlichen Herunterfahren der Zelle ausgeführt wurden. Sie können den Befehl `fail-tasks` nur verwenden, wenn alle Zellen heruntergefahren wurden.

- **Konfigurieren der Behandlung von Überwachungsmeldungen**

Verwenden Sie den Befehl `configure-audit-syslog` des Zellenverwaltungstools zum Konfigurieren der Art und Weise, wie das System Überwachungsmeldungen protokolliert.

- **Konfigurieren von E-Mail-Vorlagen**

Um die Vorlagen zu verwalten, die das System beim Erstellen von E-Mail-Warnungen verwendet, können Sie den Befehl `manage-email` des Zellenverwaltungstools verwenden.

- **Finden von verwaisten VMs**

Verwenden Sie den Befehl `find-orphan-vm` des Zellenverwaltungstools, um Verweise auf virtuelle Maschinen zu finden, die in der vCenter-Datenbank, jedoch nicht in der VMware Cloud Director-Datenbank vorhanden sind.

- **Beitreten zum Programm zur Verbesserung der Kundenzufriedenheit von VMware bzw. Verlassen dieses Programms**

Um dem Programm zur Verbesserung der Kundenzufriedenheit (CEIP) beizutreten oder es zu verlassen, können Sie den Unterbefehl `configure-ceip` des Zellenverwaltungstools verwenden.

- **Aktualisieren von Anwendungskonfigurationseinstellungen**

Mit dem Unterbefehl `manage-config` des Zellenverwaltungstools können Sie verschiedene Anwendungskonfigurationseinstellungen aktualisieren, wie z. B. Katalogdrosselungsaktivitäten.

- **Konfigurieren von Katalogsynchronisierungsdrosselung**

Um bei einer Vielzahl von Katalogelementen, die für andere Organisationen veröffentlicht oder von diesen abonniert werden, während der Katalogsynchronisierung eine Überlastung des Systems zu vermeiden, können Sie Katalogsynchronisierungsdrosselung konfigurieren. Sie können den Unterbefehl `manage-config` des Zellenverwaltungstools verwenden, um Katalogsynchronisierungsdrosselung zu konfigurieren, indem Sie die Anzahl der Bibliothekselemente begrenzen, die gleichzeitig synchronisiert werden können.

- **Fehlerbehebung bei fehlgeschlagenem Zugriff auf die VMware Cloud Director-Benutzeroberfläche**

Um die gültigen IP-Adressen und DNS-Einträge für die VMware Cloud Director-Zellen in Ihrer VMware Cloud Director-Umgebung anzuzeigen und zu aktualisieren, können Sie den Unterbefehl `manage-config` des Zellenverwaltungstools verwenden.

- [Debuggen der vCenter-VM-Erkennung](#)

Mithilfe des Unterbefehls `debug-auto-import` des Zellenverwaltungstools können Sie untersuchen, warum der Mechanismus zum Auffinden von vApps eine oder mehrere vCenter-VMs überspringt.

- [Erneutes Erzeugen von MAC-Adressen für ausgeweitete Multisite-Netzwerke](#)

Wenn Sie zwei VMware Cloud Director-Sites verknüpfen, die mit derselben Installations-ID konfiguriert sind, kommt es in ausgeweiteten Netzwerken für diese Sites möglicherweise zu Konflikten bei MAC-Adressen. Zur Vermeidung solcher Konflikte müssen Sie die MAC-Adressen an einem dieser Sites auf Basis eines benutzerdefinierten Ausgangswerts, der sich von der Installations-ID unterscheidet, erneut erzeugen.

- [Aktualisieren der Datenbank-IP-Adressen auf VMware Cloud Director-Zellen](#)

Um die IP-Adressen der VMware Cloud Director-Zellen in einem Datenbank-Hochverfügbarkeits-Cluster zu aktualisieren, können Sie das Zellenverwaltungstool verwenden.

Konfigurieren einer VMware Cloud Director-Installation

Verwenden Sie den Befehl `system-setup` des Zellenverwaltungsprogramms, um die Datenbank der Servergruppe mit einem Systemadministratorkonto und zugehörigen Informationen zu initialisieren.

Nachdem Sie alle Server in der VMware Cloud Director-Servergruppe konfiguriert und sie mit der Datenbank verbunden haben, können Sie das anfängliche Systemadministratorkonto erstellen und die VMware Cloud Director-Datenbank mit zugehörigen Informationen mithilfe einer Befehlszeile im folgenden Format initialisieren:

```
cell-management-tool system-setup Optionen
```

Sie können diesen Befehl nicht in einem bereits konfigurierten System ausführen. Alle Optionen mit Ausnahme von `--unattended` und `--password` müssen angegeben werden.

Tabelle 5-1. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `system-setup`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--email</code>	Die zu erstellende E-Mail-Adresse für den Systemadministrator.	Die E-Mail-Adresse des Systemadministrators ist in der VMware Cloud Director-Datenbank gespeichert.

Tabelle 5-1. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `system-setup` (Fortsetzung)

Option	Argument	Beschreibung
<code>--full-name</code>	Der zu erstellende vollständige Name des Systemadministrators	Der vollständige Name des Systemadministrators ist in der VMware Cloud Director-Datenbank gespeichert.
<code>--installation-id</code>	Eine Ganzzahl im Bereich von 1 bis 63	Die Installations-ID für diese Installation von VMware Cloud Director. Das System verwendet die Installations-ID beim Generieren von MAC-Adressen für virtuelle Netzwerkadapter. Hinweis Wenn Sie ausgeweitete Netzwerke für VMware Cloud Director-Installationen in einer Multisite-Bereitstellung erstellen möchten, richten Sie eine eindeutige Installations-ID für jede VMware Cloud Director-Installation ein.
<code>--password</code>	Das zu erstellende Kennwort für den Systemadministrator. Erforderlich, wenn Sie die <code>--unattended</code> -Option verwenden. Wenn Sie die Option <code>--unattended</code> nicht verwenden, werden Sie zur Eingabe dieses Kennworts aufgefordert, falls Sie es nicht in der Befehlszeile eingeben.	Der Systemadministrator gibt dieses Kennwort bei der Authentifizierung bei VMware Cloud Director ein.
<code>--serial-number</code>	Die Seriennummer (Lizenzschlüssel) für diese Installation.	Optional. Muss eine gültige VMware Cloud Director-Seriennummer sein.
<code>--system-name</code>	Der zu verwendende Name ist ein Name für den VMware Cloud Director vCenter Server-Ordner.	Diese VMware Cloud Director-Installation wird durch einen Ordner mit diesem Namen in jedem vCenter Server, bei dem sie registriert ist, dargestellt.

Tabelle 5-1. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `system-setup` (Fortsetzung)

Option	Argument	Beschreibung
<code>--unattended</code>	Keine	Optional. Beim Aufruf mit dieser Option erfolgt keine weitere Eingabeaufforderung.
<code>--user</code>	Der zu erstellende Benutzername des Systemadministrators	Der Systemadministrator gibt diesen Benutzernamen bei der Authentifizierung bei VMware Cloud Director ein.

Beispiel: VMware Cloud Director-Systemeinstellungen angeben

Dieser Befehl gibt alle Systemeinstellungen für eine neue VMware Cloud Director-Installation an. Da `--unattended` und `--password` nicht angegeben sind, werden Sie aufgefordert, das für den Systemadministrator zu erstellende Kennwort einzugeben und zu bestätigen.

```
[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.
```

Deaktivieren des Dienstanbieterzugriffs auf den Legacy-API-Endpoint

Ab VMware Cloud Director 10.0 können Sie separate VMware Cloud Director OpenAPI-Anmelde-Endpoints für den Dienstanbieter- und den Mandantenzugriff auf VMware Cloud Director verwenden.

Sie können zwei neue OpenAPI-Endpoints verwenden, um durch Beschränkung des Zugriffs auf VMware Cloud Director die Sicherheit zu erhöhen.

- `/cloudapi/1.0.0/sessions/provider` – OpenAPI-Endpoint für die Dienstanbieteranmeldung. Mandanten können nicht unter Verwendung dieses Endpoints auf VMware Cloud Director zugreifen.

- `/cloudapi/1.0.0/sessions/` – OpenAPI-Endpoint für die Mandantenanmeldung. Dienstanbieter können nicht unter Verwendung dieses Endpoints auf VMware Cloud Director zugreifen.

Standardmäßig können Anbieteradministratoren und Organisationsbenutzer auf VMware Cloud Director zugreifen, indem sie sich beim `/api/sessions`-API-Endpoint anmelden.

Mithilfe des Unterbefehls `manage-config` des Zellenverwaltungstools können Sie den Dienstanbieterzugriff auf den `/api/sessions`-API-Endpoint deaktivieren und dadurch die Anbieteranmeldung auf den neuen OpenAPI-Endpoint `/cloudapi/1.0.0/sessions/provider` begrenzen, auf den nur Dienstanbieter zugreifen können.

Hinweis Wenn Sie den Dienstanbieterzugriff auf den API-Endpoint `/api/sessions` deaktivieren, schlagen Dienstanbieteranfragen, die nur ein SAML-Token im Autorisierungsheader bereitstellen, für alle veralteten API-Endpoints fehl.

Verfahren

- 1 Melden Sie sich, bei Bedarf mithilfe von SSH, als `root` beim Betriebssystem einer der VMware Cloud Director-Zellen an.
- 2 Um den Anbieterzugriff auf den API-Endpoint `/api/sessions` zu blockieren, verwenden Sie das Zellenverwaltungstool und führen Sie den folgenden Befehl aus:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v true
```

Ergebnisse

Dienstanbieter können nicht mehr auf den API-Endpoint `/api/sessions` zugreifen. Dienstanbieter können den neuen OpenAPI-Endpoint `/cloudapi/1.0.0/sessions/provider` verwenden, um auf VMware Cloud Director zuzugreifen. Mandanten können auf VMware Cloud Director zugreifen, indem sie sowohl den API-Endpoint `/api/sessions` als auch den neuen OpenAPI-Endpoint `/cloudapi/1.0.0/sessions/` verwenden.

Nächste Schritte

Um den Anbieterzugriff auf den API-Endpoint `/api/sessions` zu aktivieren, führen Sie den folgenden Befehl aus:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v false
```

Verwalten einer Zelle

Mit dem Unterbefehl `cell` des Zellenverwaltungstools können Sie das Aufgabenplanungstool anhalten, damit keine neuen Aufgaben gestartet werden können, den Status aller aktiven

Aufgaben anzeigen, den Zellenwartungsmodus steuern sowie die Zelle ordnungsgemäß herunterfahren.

Verwenden Sie zum Verwalten einer Zelle eine Befehlszeile im folgenden Format:

```
cell-management-toolcell-usysadmin-username -p sysadmin-passwordoption
```

wobei *sysadmin-username* und *sysadmin-password* der Benutzername und das Kennwort des **Systemadministrators** sind.

Hinweis Aus Sicherheitsgründen können Sie das Kennwort auslassen. In diesem Fall fordert Sie der Befehl zur Eingabe des Kennworts auf, ohne es auf dem Bildschirm anzuzeigen.

Alternativ zum Angeben der Anmeldeinformationen des **Systemadministrators** können Sie die Option `--pid` verwenden und die Prozess-ID des Zellenprozesses angeben. Um die Prozess-ID der Zelle zu finden, verwenden Sie einen Befehl wie den folgenden:

```
cat /var/run/vmware-vcd-cell.pid
```

Tabelle 5-2. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `cell`

Option	Argument	Beschreibung
<code>--help</code> (-h)	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--pid</code> (-i)	Prozess-ID des Zellenprozesses	Sie können diese Option anstelle von <code>-username</code> verwenden.
<code>--maintenance</code> (-m)	<code>true</code> oder <code>false</code>	Richtet die Zelle im Wartungsmodus ein. Das Argument <code>true</code> legt die Aktivität der Zelle still und versetzt die Zelle in den Wartungsmodus. Mit dem Argument <code>false</code> wird der Wartungsmodus für die Zelle beendet.
<code>--password</code> (-p)	Kennwort des VMware Cloud Director- Systemadministrators	Optional, wenn die Option <code>-username</code> verwendet wird. Wenn Sie diese Option auslassen, werden Sie vom Befehl zur Eingabe des Kennworts aufgefordert, ohne dass dieses auf dem Bildschirm angezeigt wird.

Tabelle 5-2. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `cell` (Fortsetzung)

Option	Argument	Beschreibung
<code>--quiesce</code> (-q)	true oder false	Legt die Aktivität auf der Zelle still. Mit dem Argument <code>true</code> wird das Planungstool angehalten. Mit dem Argument <code>false</code> wird die Ausführung des Planungstools neu gestartet.
<code>--shutdown</code> (-s)	Keines	Führt die VMware Cloud Director-Dienste auf dem Server ordnungsgemäß herunter.
<code>--status</code> (-t)	Keines	Zeigt Informationen über die Anzahl der Aufgaben, die auf der Zelle ausgeführt werden, und den Status der Zelle an.
<code>--status-verbose</code> (-tt)	Keines	Zeigt ausführliche Informationen über die Aufgaben, die auf der Zelle ausgeführt werden, sowie über den Status der Zelle an.
<code>--username</code> (-u)	Benutzername des VMware Cloud Director-Systemadministrators.	Sie können diese Option anstelle von <code>-pid</code> verwenden.

Verwalten von Zellenanwendungen

Verwenden Sie den Befehl `cell-application` des Zellenverwaltungstools zum Steuern des Satzes von Anwendungen, die die Zelle beim Starten ausführt.

Eine VMware Cloud Director-Instanz führt eine Reihe von Anwendungen aus, die von VMware Cloud Director-Clients benötigte Dienste bereitstellen. Die Zelle startet standardmäßig eine Teilmenge dieser Anwendungen. Üblicherweise müssen alle Mitglieder dieser Teilmenge eine VMware Cloud Director-Installation unterstützen.

Verwenden Sie zum Anzeigen oder Ändern der Liste der Anwendungen, die beim Start der Zelle ausgeführt werden, eine Befehlszeile im folgenden Format:

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell-application command
```

sysadmin-username

Der Benutzername eines VMware Cloud Director-Systemadministrators.

sysadmin-password

Das Kennwort des VMware Cloud Director-Systemadministrators. Sie müssen das Kennwort in Anführungszeichen setzen, wenn es Sonderzeichen enthält.

Hinweis Sie können das Kennwort für den VMware Cloud Director-Systemadministrator in der Befehlszeile von `cell-management-tool` angeben. Es ist jedoch sicherer, das Kennwort wegzulassen. Damit werden Sie von `cell-management-tool` aufgefordert, das Kennwort anzugeben, das während der Eingabe nicht auf dem Bildschirm angezeigt wird.

Alternativ zum Angeben der Anmeldeinformationen des Systemadministrators können Sie die Option `--pid` verwenden und die Prozess-ID des Zellenprozesses angeben. Um die Prozess-ID der Zelle zu finden, verwenden Sie einen Befehl wie den folgenden:

```
cat /var/run/vmware-vcd-cell.pid
```

command

`cell-application`-Unterbefehl.

Tabelle 5-3. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `cell-application`

Befehl	Argument	Beschreibung
<code>--help (-h)</code>	Keine	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--application-states</code>	Keine	Listet die Zellenanwendungen und den jeweils zugehörigen aktuellen Status auf.
<code>--disable</code>	Anwendungs-ID	Verhindert, dass diese Zellenanwendung beim Start der Zelle ausgeführt wird.
<code>--enable</code>	Anwendungs-ID	Aktiviert die Ausführung dieser Zellenanwendung beim Start der Zelle.
<code>--pid (-i)</code>	Prozess-ID des Zellenprozesses	Sie können diese Option anstelle von <code>-u</code> oder <code>-u</code> und <code>-p</code> verwenden.
<code>--list</code>	Keine	Listet alle Zellenanwendungen auf und zeigt an, ob sie für die Ausführung beim Start der Zelle aktiviert sind.
<code>--password (-p)</code>	VMware Cloud Director-Administratorkennwort	Optional. Der Befehl fordert zur Eingabe eines Kennworts auf, wenn Sie dieses nicht in der Befehlszeile angeben.
<code>--set</code>	Durch Semikolon getrennte Liste von Anwendungs-IDs.	Gibt den Satz von Zellenanwendungen an, die beim Start der Zelle ausgeführt werden. Dieser Befehl überschreibt den vorhandenen Satz an Zellenanwendungen, die beim Start der Zelle ausgeführt werden. Verwenden Sie <code>--enable</code> oder <code>--disable</code> , um den Startstatus einzelner Anwendungen zu ändern.
<code>--username (-u)</code>	Benutzername des VMware Cloud Director-Administrators.	Dieser ist erforderlich, wenn <code>--pid</code> nicht angegeben wird.

Beispiel: Auflisten von Zellenanwendungen und ihres jeweiligen Startstatus

Die folgende Befehlszeile von `cell-management-tool` erfordert Anmeldeinformationen eines Systemadministrators und gibt die Liste der Zellenanwendungen und ihres jeweiligen Startstatus zurück.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell-
application --list
Please enter the administrator password:

name                id                enabled
description

Networking           com.vmware.vc... true           Exposes NSX api endpoints directly from
vCD.
Console Proxy       com.vmware.vc... true           Proxies VM console data
connection...
Cloud Proxy         com.vmware.vc... true           Proxies TCP connections from a tenant
site.
Compute Service Broker com.vmware.vc... true           Allows registering with a service
control...
Maintenance Application com.vmware.vc... false          Indicates to users the cell is
undergo ...
Core Cell Application com.vmware.vc... true           Main cell application, Flex UI and REST
API.
```

Aktualisieren der Datenbankverbindungseigenschaften

Sie können die Verbindungseigenschaften für die VMware Cloud Director-Datenbank mithilfe des Unterbefehls `reconfigure-database` des Zellenverwaltungstools aktualisieren.

Während des VMware Cloud Director-Installations- oder VMware Cloud Director-Appliance-Bereitstellungsvorgangs konfigurieren Sie den Datenbanktyp und die Datenbankverbindungseigenschaften. Weitere Informationen finden Sie unter [Installieren von VMware Cloud Director unter Linux](#) und [Bereitstellung und anfängliche Konfiguration der VMware Cloud Director-Appliance](#).

Nach dem Konfigurieren der VMware Cloud Director-Datenbank können Sie die Datenbankverbindungen mithilfe des Unterbefehls `reconfigure-database` aktualisieren. Sie können die vorhandene VMware Cloud Director-Datenbank auf einen neuen Host verschieben, den Benutzernamen und das Kennwort für die Datenbank ändern oder eine SSL-Verbindung zu einer PostgreSQL-Datenbank herstellen.

```
cell-management-tool reconfigure-database options
```

Wichtig Die Änderungen, die Sie durch Ausführen des Befehls `reconfigure-database` vornehmen, werden in die globale Konfigurationsdatei `global.properties` und die Antwortdatei `responses.properties` der Zelle geschrieben. Stellen Sie vor dem Ausführen des Befehls sicher, dass die Antwortdatei unter `/opt/vmware/vcloud-director/etc/responses.properties` verfügbar und beschreibbar ist. Informationen zum Schützen und Wiederverwenden der Antwortdatei finden Sie unter [Installieren von VMware Cloud Director unter Linux](#).

Wenn Sie die Option „`--pid`“ nicht verwenden, müssen Sie die Zelle neu starten, damit die Änderungen übernommen werden.

Tabelle 5-4. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `reconfigure-database`

Option	Argument	Beschreibung
<code>--help</code> (-h)	Keines	Stellt eine Zusammenfassung der verfügbaren Optionen in dieser Kategorie bereit.
<code>--database-host</code> (-dbhost)	IP-Adresse oder vollqualifizierter Domänenname des VMware Cloud Director-Datenbankhosts	Aktualisiert den Wert der Eigenschaft <code>database.jdbcUrl</code> . Wichtig Der Befehl überprüft nur das Wertformat.
<code>--database-instance</code> (-dbinstance)	SQL Server-Datenbank-Instanz.	Optional. Wird verwendet, wenn der Datenbanktyp <code>sqlserver</code> ist. Wichtig Wenn Sie diese Option hinzufügen, müssen Sie denselben Wert eingeben, den Sie bei der erstmaligen Konfiguration der Datenbank angegeben haben.
<code>--database-name</code> (-dbname)	Der Datenbankdienstname.	Aktualisiert den Wert der Eigenschaft <code>database.jdbcUrl</code> .
<code>--database-password</code> (-dbpassword)	Kennwort für den Datenbankbenutzer.	Aktualisiert den Wert der Eigenschaft <code>database.password</code> . Das eingegebene Kennwort wird verschlüsselt, bevor es als Eigenschaftswert gespeichert wird.

Tabelle 5-4. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl reconfigure-database (Fortsetzung)

Option	Argument	Beschreibung
<code>--database-port</code> (<code>-dbport</code>)	Portnummer, die vom Datenbankdienst auf dem Datenbank-Host verwendet wird.	Aktualisiert den Wert für die Eigenschaft <code>database.jdbcUrl</code> . Wichtig Der Befehl überprüft nur das Wertformat.
<code>--database-type</code> (<code>-dbtype</code>)	Der Datenbanktyp. Dazu gehören: <ul style="list-style-type: none"> ■ <code>sqlserver</code> ■ <code>postgres</code> 	Aktualisiert den Wert der Eigenschaft <code>database.jdbcUrl</code> .
<code>--database-user</code> (<code>-dbuser</code>)	Benutzername des Datenbankbenutzers.	Aktualisiert den Wert der Eigenschaft <code>database.user</code> .
<code>--database-ssl</code>	<code>true</code> oder <code>false</code>	Wird verwendet, wenn der Datenbanktyp <code>postgres</code> ist. Konfiguriert die PostgreSQL-Datenbank, um eine SSL-Verbindung von VMware Cloud Director anzufordern.
<code>--pid</code> (<code>-i</code>)	Die Prozess-ID der Zelle.	Optional. Führt eine Neukonfiguration einer VMware Cloud Director-Zelle im laufenden Betrieb aus. Erfordert keinen Neustart der Zelle. Bei Verwendung mit <code>--private-key-path</code> können Sie den Befehl auf lokalen und Remote-Zellen sofort ausführen.
<code>--private-key-path</code>	Pfadname des privaten Schlüssels der Zelle.	Optional. Alle Zellen in der Servergruppe werden ordnungsgemäß heruntergefahren. Aktualisieren Sie die zugehörigen Datenbankeigenschaften und führen Sie einen Neustart durch. Wichtig Alle Zellen müssen SSH-Verbindungen vom Superuser ohne Eingabe eines Kennworts zulassen.
<code>--remote-sudo-user</code>	Ein Benutzername mit sudo-Rechten.	Wird mit der Option <code>--private-key-path</code> verwendet, wenn der Remotebenutzer nicht root ist. Für die Appliance können Sie diese Option für den postgres -Benutzer verwenden, z. B. <code>--remote-sudo-user=postgres</code> .

Bei Verwendung der Optionen `--database-host` und `--database-port` validiert der Befehl das Format der Argumente, überprüft aber die Kombination aus Host und Port weder auf Netzwerkzugriff noch auf das Vorhandensein einer ausgeführten Datenbank vom angegebenen Typ.

Wenn Sie die Option `--private-key-path` verwenden, müssen alle Zellen so konfiguriert werden, dass sie SSH-Verbindungen vom Superuser ohne Eingabe eines Kennworts zulassen. Um eine Überprüfung durchzuführen, können Sie beispielsweise den folgenden Linux-Befehl ausführen:

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

In diesem Beispiel wird Ihre Identität auf `vcloud` festgelegt. Anschließend wird eine SSH-Verbindung mit der Zelle unter `cell-ip` als Root hergestellt, jedoch kein Root-Kennwort angegeben. Wenn der private Schlüssel in `private-key-path` in der lokalen Zelle vom Benutzer `vcloud.vcloud` gelesen werden kann und der entsprechende öffentliche Schlüssel in der Datei `authorized-keys` für den Root-Benutzer unter `cell-ip` vorhanden ist, wird der Befehl erfolgreich ausgeführt.

Hinweis Der Benutzer `vcloud`, die Gruppe `vcloud` und das Konto `vcloud.vcloud` werden vom VMware Cloud Director-Installationsprogramm zur Verwendung als Identität erstellt, mit der VMware Cloud Director-Prozesse ausgeführt werden. Der Benutzer `vcloud` hat kein Kennwort.

Beispiel: Ändern Sie den Benutzernamen und das Kennwort für die VMware Cloud Director-Datenbank.

Zum Ändern des Benutzernamens und Kennworts für die VMware Cloud Director-Datenbank unter Beibehaltung der ursprünglichen Konfiguration aller anderen Verbindungseigenschaften können Sie den folgenden Befehl ausführen:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \  
-dbuser vcd-dba -dbpassword P@55w0rd
```

Beispiel: Aktualisieren der IP-Adresse der VMware Cloud Director-Datenbank durch Neukonfiguration aller Zellen bei laufendem Betrieb

Wenn Sie kein root-Benutzer mit sudo-Rechten sind, können Sie den folgenden Befehl ausführen, um die IP-Adresse der VMware Cloud Director-Datenbank in allen Zellen sofort zu ändern:

```
[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
```

Erkennen und Reparieren von beschädigten Scheduler-Daten

VMware Cloud Director verwendet das Auftragsplanungstool Quartz zum Koordinieren von asynchronen Vorgängen (Aufträgen), die auf dem System ausgeführt werden. Wenn die Datenbank des Planungstools Quartz beschädigt wird, können Sie das System möglicherweise nicht erfolgreich stilllegen. Verwenden Sie den Befehl `fix-scheduler-data` des Zellenverwaltungstools zum Durchsuchen der Datenbank nach beschädigten Scheduler-Daten und reparieren Sie die Daten nach Bedarf.

Verwenden Sie zum Durchsuchen der Datenbank nach beschädigten Scheduler-Daten einen Befehl im folgenden Format:

```
cell-management-toolfix-scheduler-dataOptionen
```

Tabelle 5-5. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `fix-scheduler-data`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keine	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--dbuser</code>	Der Benutzername des VMware Cloud Director-Datenbankbenutzers.	Muss in der Befehlszeile angegeben werden.
<code>--dbpassword</code>	Das Kennwort des VMware Cloud Director-Datenbankbenutzers.	Wird vom Benutzer abgefragt, falls es nicht angegeben ist.

Generieren von selbstsignierten Zertifikaten für die HTTPS- und Konsolenproxy-Endpoints

Verwenden Sie den Befehl `generate-certs` des Zellenverwaltungstools, um selbstsignierte SSL-Zertifikate für die HTTPS- und Konsolenproxy-Endpoints zu generieren.

Jede VMware Cloud Director-Servergruppe muss zwei SSL-Endpoints unterstützen: einen für den HTTPS-Dienst und einen weiteren für den Konsolenproxydienst. Der Endpoint des HTTPS-Diensts unterstützt das VMware Cloud Director Service Provider Admin Portal, das VMware Cloud Director Tenant Portal und die VMware Cloud Director-API. Der Remote-Konsolen-Proxy-Endpoint unterstützt VMRC-Verbindungen mit vApps und VMs.

Mit dem Befehl `generate-certs` im Zellenverwaltungstool wird das in [Erstellen von selbstsignierten SSL-Zertifikaten für VMware Cloud Director unter Linux](#) beschriebene Verfahren automatisiert.

Wenn Sie neue selbstsignierte SSL-Zertifikate generieren und diese einem neuen oder vorhandenen Keystore hinzufügen möchten, verwenden Sie eine Befehlszeile im folgenden Format:

```
cell-management-tool generate-certs Optionen
```

Tabelle 5-6. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl generate-certs

Option	Argument	Beschreibung
--help (-h)	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
--expiration (-x)	<i>days-until-expiration</i>	Die Anzahl der Tage bis zum Ablauf der Zertifikate. Standardmäßig 365.
--issuer (-i)	<i>name= value</i> [, <i>name= value, ...</i>]	X.509-DN (Distinguished Name) des Zertifikatsherausgebers. Die Standardeinstellung lautet <i>CN=FQDN</i> . Dabei ist <i>FQDN</i> der vollqualifizierte Domänenname der Zelle bzw. ihre IP-Adresse, falls kein vollqualifizierter Domänenname vorliegt. Wenn Sie mehrere Attribut-Wert-Paare angeben, trennen Sie sie durch Komma und schließen Sie das gesamte Argument in Anführungszeichen ein.
--httpcert (-j)	Keines	Generieren Sie ein Zertifikat für den HTTPS-Endpoint.
--type (-t)	<i>keystore-type</i>	Format des Keystores. Der Standardwert ist <i>PKCS12</i> . Sie können auch einen <i>JCEKS</i> -Keystore erstellen.
--key-size (-s)	<i>key-size</i>	Die Größe des Schlüsselpaars als Ganzzahlwert der Bits. Die Standardeinstellung lautet 2048. Schlüssel mit einer Länge von weniger als 1024 werden entsprechend NIST Special Publication 800-131A nicht mehr unterstützt.
--keystore-pwd (-w)	<i>keystore-password</i>	Das Kennwort für den Keystore auf diesem Host.

Tabelle 5-6. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `generate-certs` (Fortsetzung)

Option	Argument	Beschreibung
<code>--out (-o)</code>	<i>keystore-pathname</i>	Der vollständige Pfadname des Keystores auf diesem Host.
<code>--consoleproxycert (-p)</code>	Keines	Generieren Sie ein Zertifikat für den Konsolen-Proxy-Endpunkt.

Hinweis Um die Kompatibilität mit vorherigen Versionen dieses Unterbefehls zu sichern, führen sowohl das Auslassen von `-j` und `-p` als auch das Angeben von `-j` und `-p` zu denselben Ergebnissen.

Beispiel: Erstellen selbstsignierter Zertifikate

In diesen beiden Beispielen wird von einem Keystore unter `/tmp/cell.ks` mit dem Kennwort `kspw` ausgegangen. Dieser Keystore wird erstellt, wenn er nicht bereits vorhanden ist.

In diesem Beispiel werden die neuen Zertifikate mit den Standardwerten erstellt. Der Name des Ausstellers wird auf `CN=Unknown` festgelegt. Für das Zertifikat wird die Standardschlüssellänge von 2048-Bit verwendet und das Zertifikat läuft ein Jahr nach der Erstellung ab.

```
[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.
```

In diesem Beispiel wird ein neues Zertifikat nur für den HTTPS-Endpoint erstellt. Zudem werden auch benutzerdefinierte Werte für die Schlüssellänge und den Namen des Ausstellers verwendet. Der Name des Ausstellers wird auf `CN=Test, L=London, C=GB` festgelegt. Das neue Zertifikat für die HTTPS-Verbindung hat einen 4096 Bit umfassenden Schlüssel und läuft 90 Tage nach seiner Erstellung ab. Das vorhandene Zertifikat für den Konsolen-Proxy-Endpunkt bleibt davon unberührt.

```
[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.
```

Wichtig Die Keystore-Datei und das Verzeichnis, in dem sie sich befindet, muss von der Benutzer-`vcloud.vcloud` lesbar sein. Das Installationsprogramm von VMware Cloud Director erstellt diesen Benutzer und diese Gruppe.

Ersetzen der Zertifikate für die HTTPS- und Konsolenproxy-Endpoints

Verwenden Sie den Befehl `certificates` des Zellenverwaltungstools, um SSL-Zertifikate für die HTTPS- und Konsolenproxy-Endpoints zu ersetzen.

Mit dem Befehl `certificates` des Zellenverwaltungstools wird der Vorgang zum Ersetzen vorhandener Zertifikate durch neue Zertifikate automatisiert, die in einem mit PKCS12 oder JCEKS formatierten Keystore gespeichert wurden. Verwenden Sie den Befehl `certificates`, um selbstsignierte Zertifikate durch signierte Zertifikate oder ablaufende Zertifikate durch neue Zertifikate zu ersetzen. Informationen zum Erstellen eines Keystores mit signierten Zertifikaten finden Sie unter [Erstellen von selbstsignierten SSL-Zertifikaten für VMware Cloud Director unter Linux](#).

Verwenden Sie einen Befehl im folgenden Format, um SSL-Zertifikate für einen oder beide Endpoints zu ersetzen:

```
cell-management-tool certificates Optionen
```

Tabelle 5-7. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `certificates`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--config (-c)</code>	Vollständiger Pfadname zur Datei <code>global.properties</code> der Zelle.	Standardmäßig <code>\$VCLLOUD_HOME/etc/global.properties</code> .
<code>--https (-j)</code>	Keines	Ersetzen Sie die Keystore-Datei mit dem Namen <code>certificates</code> , die vom HTTP-Endpoint verwendet wird.
<code>--consoleproxy (-p)</code>	Keines	Ersetzen Sie die Keystore-Datei mit dem Namen <code>proxycertificates</code> , die vom Konsolen-Proxy-Endpoint verwendet wird.
<code>--responses (-r)</code>	Vollständiger Pfadname zur Datei <code>responses.properties</code> der Zelle.	Standardmäßig <code>\$VCLLOUD_HOME/etc/responses.properties</code> .
<code>--keystore (-k)</code>	<i>keystore-pathname</i>	Der vollständige Pfadname zu einem mit PKCS12 oder JCEKS formatierten Keystore, der signierte Zertifikate enthält. Auslaufende <code>-s</code> -Kurzform ersetzt durch <code>-k</code> .
<code>--keystore-password (-w)</code>	<i>keystore-password</i>	Das Kennwort für den mit PKCS12 oder JCEKS formatierten Keystore, auf den mit der Option <code>--keystore</code> verwiesen wird. Ersetzt auslaufende <code>-kspassword-</code> und <code>--kestorepwd-</code> Optionen.

Beispiel: Ersetzen von Zertifikaten

Sie können die Optionen `--config` und `--responses` auslassen, sofern diese Dateien nicht aus den Standardpfaden verschoben wurden. In diesem Beispiel hat ein Keystore unter `/tmp/my-new-certs.ks` das Kennwort `kspw`. In diesem Beispiel wird das vorhandene HTTP-Endpunkt-Zertifikat der Zelle durch das Zertifikat `/tmp/my-new-certs.ks` ersetzt.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool certificates -j -k /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

Hinweis Sie müssen die Zelle nach dem Ersetzen der Zertifikate neu starten.

Importieren von SSL-Zertifikaten aus externen Diensten

Verwenden Sie den Befehl `import-trusted-certificates` des Zellenverwaltungstools, um Zertifikate für den Aufbau sicherer Verbindungen zu externen Diensten wie AMQP und der VMware Cloud Director-Datenbank zu importieren.

Bevor eine sichere Verbindung zu einem externen Dienst aufgebaut werden kann, muss VMware Cloud Director durch den Import der Zertifikate dieses Dienstes in seinen eigenen Truststore eine gültige Vertrauenskette für diesen Dienst einrichten. Um vertrauenswürdige Zertifikate in den Truststore der Zelle zu importieren, verwenden Sie einen Befehl im folgenden Format:

```
cell-management-tool import-trusted-certificates Optionen
```

Tabelle 5-8. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `import-trusted-certificates`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--destination</code>	Pfadname	Vollständiger Pfad zum Ziel-Truststore. Ist standardmäßig <code>/opt/vmware/vcloud-director/etc/certificates</code> , sofern nicht in der Befehlszeile angegeben.
<code>--destination-password</code>	Zeichenfolge	Kennwort für den Ziel-Truststore. Die Standardeinstellung ist der Wert von <code>vcloud.ssl.truststore.password</code> , wenn nicht in der Befehlszeile angegeben.

Tabelle 5-8. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `import-trusted-certificates` (Fortsetzung)

Option	Argument	Beschreibung
<code>--destination-type</code>	Typ des Keystores	Keystore-Typ des Ziel-Truststore. JKS oder JCEKS möglich. Die Standardeinstellung lautet JCEKS.
<code>--force</code>	Keines	Überschreibt die vorhandenen Zertifikate im Ziel-Truststore.
<code>--source</code>	Pfadname	Vollständiger Pfad zur quellseitigen PEM-Datei.

Beispiel: Importieren von vertrauenswürdigen Zertifikaten

In diesem Beispiel werden die Zertifikate aus `/tmp/demo.pem` in den lokalen Keystore von VMware Cloud Director unter `/opt/vmware/vcloud-director/etc/certificates` importiert. VMware Cloud Director speichert das Keystore-Kennwort in einem verschlüsselten Format, das der Befehl `import-trusted-certificates` entschlüsselt.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool import-trusted-certificates --source /tmp/demo.pem
```

Importieren von Endpoint-Zertifikaten aus vSphere-Ressourcen

Verwenden Sie nach dem Upgrade den Befehl `trust-infra-certs` des Zellenverwaltungstools, um Zertifikate aus den vSphere-Ressourcen in der Umgebung zu erfassen und in die VMware Cloud Director-Datenbank zu importieren.

Der Befehl `trust-infra-certs` des Zellenverwaltungstools erfasst automatisch die SSL-Zertifikate aus den vSphere-Ressourcen in der Umgebung und importiert sie in die VMware Cloud Director-Datenbank.

Voraussetzungen

Vergewissern Sie sich, dass die vCenter Server- und NSX Manager-Instanzen, für die Sie Endpoints importieren möchten, bereit sind und ausgeführt werden.

Verfahren

- 1 Melden Sie sich, bei Bedarf mithilfe von SSH, als „root“ beim Betriebssystem einer der VMware Cloud Director-Zellen an.
- 2 Führen Sie den Befehl im folgenden Format aus.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs Optionen
```

Tabelle 5-9. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl trust-infra-certs

Option	Argument	Beschreibung
--help (-h)	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
--vsphere	Keines	Fordert Sie auf, den Zertifikaten für alle registrierten vCenter Server-, NSX Data Center for vSphere- und NSX-T Data Center-Instanzen in dieser Installation zu vertrauen.
--trust	Keines	Optional. Fügt dem VMware Cloud Director-Truststore Zertifikate hinzu.
--inspect	Optional. Dateipfad.	Optional. Zeigt die Zertifikate in einer Datei an.
--unattended	Keines	Optional. Beim Aufruf mit dieser Option erfolgt keine weitere Eingabeaufforderung. Alle Infrastrukturzertifikate werden automatisch als vertrauenswürdig eingestuft.

Beispiel: Einstufen aller Zertifikate aus vSphere-Ressourcen-Endpoints als vertrauenswürdig und Importieren dieser Zertifikate

Wenn Sie die Zertifikate aus den vSphere-Ressourcen-Endpoints ohne weitere Eingabeaufforderungen als vertrauenswürdig einstufen und sie importieren möchten, führen Sie den Befehl mit den folgenden Optionen aus.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs --vsphere --unattended
```

Konfigurieren einer Negativliste für Testverbindungen

Verwenden Sie nach der Installation oder dem Upgrade den Befehl `manage-test-connection-blacklist` des Zellenverwaltungstools, um den Zugriff auf interne Hosts zu blockieren, bevor Sie Mandantenzugriff auf das VMware Cloud Director-Netzwerk gewähren.

Ab VMware Cloud Director 10.1 können Dienstanbieter und Mandanten die VMware Cloud Director-API verwenden, um Verbindungen mit Remoteservern zu testen und die Serveridentität als Teil eines SSL-Handshake zu überprüfen.

Um das interne Netzwerk, in dem eine VMware Cloud Director-Instanz bereitgestellt wird, vor böswilligen Angriffen zu schützen, können Systemanbieter eine Negativliste interner Hosts konfigurieren, die für Mandanten nicht erreichbar sind.

Wenn ein böswilliger Angreifer mit Mandantenzugriff versucht, die VMware Cloud Director-API für Verbindungstests zu verwenden, um das Netzwerk, in dem VMware Cloud Director installiert ist, zuzuordnen, kann er keine Verbindung zu den internen Hosts in der Negativliste herstellen.

Verwenden Sie nach der Installation oder dem Upgrade, und bevor Sie Mandanten den Zugriff auf das VMware Cloud Director-Netzwerk ermöglichen, den Befehl `manage-test-connection-blacklist` des Zellenverwaltungstools, um den Mandantenzugriff auf interne Hosts zu blockieren.

Verfahren

- 1 Melden Sie sich, bei Bedarf mithilfe von SSH, als „root“ beim Betriebssystem einer der VMware Cloud Director-Zellen an.
- 2 Führen Sie den Befehl aus, um der Negativliste einen Eintrag hinzuzufügen.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-test-connection-blacklist
option
```

Tabelle 5-10. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `manage-test-connection-blacklist`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--add-ip</code>	IPv4- oder IPv6-Adresse	Fügt der Negativliste eine IP-Adresse hinzu.
<code>--add-name</code>	Eine Unterdomäne oder ein vollqualifizierter Domänenname für einen Host	Fügt der Negativliste eine Unterdomäne oder einen Domännennamen hinzu.
<code>--add-range</code>	IPv4- oder IPv6-Adressbereich im CIDR- oder Bindestrichformat	Fügt der Negativliste einen IP-Adressbereich hinzu.
<code>--list</code>	Keines	Listet alle vorhandenen Einträge mit verweigertem Zugriff auf.

Anzeigen des FIPS-Status aller aktiven Zellen

Ab VMware Cloud Director 10.2.2 können Sie zum Sicherstellen des FIPS-Status aller aktiven VMware Cloud Director-Zellen den Befehl `fips-status` verwenden. Der Befehl zeigt nicht den FIPS-Status der VMware Cloud Director-Appliance an.

Weitere Informationen zum Aktivieren des FIPS-Modus für VMware Cloud Director unter Linux finden Sie unter [Aktivieren des FIPS-Modus](#) im *VMware Cloud Director Service Provider Admin Portal-Handbuch*.

Der Befehl `fips-status` zeigt die FIPS-Statusinformationen für alle aktiven Zellen an, einschließlich des Zellennamens, der UUID, der IP-Adresse und des FIPS-Status.

Informationen zum FIPS-Modus der Appliance finden Sie unter [Anzeigen des FIPS-Modus der VMware Cloud Director-Appliance](#).

Um die Daten im JSON-Format zu empfangen, können Sie das Flag `--json` angeben.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem der VMware Cloud Director-Zelle als **root** an.
- 2 Zeigen Sie den FIPS-Status aller aktiven Zellen an.

```
/opt/vmware/vcloud-director/bin/cell-management-tool fips-status
```

Tabelle 5-11. Optionen und Argumente des Zellenverwaltungstools, Befehl `fips-status`

Befehl	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--json</code>	Keines	Zeigt die Informationen im JSON-Format an.

Verwalten der Liste zulässiger SSL-Verschlüsselungen

Mit dem Befehl `ciphers` im Zellenverwaltungstool können Sie den Satz von Verschlüsselungsverfahren konfigurieren, den die Zelle während des SSL-Handshake-Vorgangs bereitstellt.

Hinweis Der Befehl `ciphers` gilt nur für den Satz von Zertifikaten, den VMware Cloud Director für die HTTPS- und Konsolen-Proxy-Kommunikation verwendet, und nicht für die Zertifikate, die die VMware Cloud Director-Appliance für ihre Appliance-Verwaltungsbenutzeroberfläche und -API verwendet.

Wenn ein Client eine SSL-Verbindung mit einer VMware Cloud Director-Zelle herstellt, bietet die Zelle nur diejenigen Verschlüsselungen an, die auf ihre Standardliste von zulässigen Verschlüsselungen konfiguriert sind. Mehrere Verschlüsselungen befinden sich nicht in dieser Liste, da sie entweder nicht stark genug sind, um die Verbindung zu sichern, oder zu SSL-Verbindungsfehlern beitragen.

Wenn Sie VMware Cloud Director installieren oder aktualisieren, überprüft das Installations- bzw. Upgrade-Skript die Zertifikate der Zelle. Wenn eines oder mehrere der Zertifikate mit einer Verschlüsselung verschlüsselt ist, die nicht in der Liste der zulässigen Verschlüsselungen enthalten ist, schlägt die Installation oder das Upgrade fehl. Sie können die folgenden Schritte ausführen, um die Zertifikate zu ersetzen und die Liste der zulässigen Verschlüsselungen neu zu konfigurieren:

- 1 Erstellen Sie Zertifikate, die keine der unzulässigen Verschlüsselungen verwenden. Sie können `cell-management-tool ciphers -a` wie im nachstehenden Beispiel beschrieben verwenden, um alle Verschlüsselungen aufzulisten, die in der Standardkonfiguration zulässig sind.
- 2 Mit dem Befehl `cell-management-tool certificates` können Sie die vorhandenen Zertifikate der Zelle durch die neuen Zertifikate ersetzen.
- 3 Mit dem Befehl `cell-management-tool ciphers` können Sie die Liste der zulässigen Verschlüsselungen neu konfigurieren und alle erforderlichen Verschlüsselungen einschließen, die in Verbindung mit den neuen Zertifikaten verwendet werden sollen.

Wichtig Da die VMRC-Konsole die Verwendung der AES256-SHA- und AES128-SHA-Verschlüsselungen erfordert, können Sie sie nicht verbieten, wenn Ihre VMware Cloud Director-Clients die VMRC-Konsole verwenden.

Verwenden Sie zum Verwalten der Liste der zulässigen SSL-Verschlüsselungen eine Befehlszeile im folgenden Format:

```
cell-management-tool ciphers options
```

Tabelle 5-12. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `ciphers`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--all-allowed (-a)</code>	Keines	Listet alle Verschlüsselungen auf, die VMware Cloud Director unterstützt.
<code>--compatible-reset (-c)</code> (veraltet)	Keines	Veraltet. Verwenden Sie die Option <code>--reset</code> , um die Liste der zulässigen Verschlüsselungen auf die Standardliste zurückzusetzen.

Tabelle 5-12. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `ciphers` (Fortsetzung)

Option	Argument	Beschreibung
<code>--disallow (-d)</code>	Durch Kommata getrennte Liste mit Verschlüsselungsnamen.	<p>Untersagt die Verwendung der Verschlüsselungen in der angegebenen kommagetrennten Liste. Bei jeder Ausführung dieser Option müssen Sie die vollständige Liste der Verschlüsselungen angeben, die Sie deaktivieren möchten, da die Ausführung der Option die vorherige Einstellung überschreibt.</p> <hr/> <p>Wichtig Wenn Sie die Option ohne Werte ausführen, werden alle Verschlüsselungen aktiviert.</p> <hr/> <p>Um alle möglichen Verschlüsselungen anzuzeigen, führen Sie die Option <code>-a</code> aus.</p> <hr/> <p>Wichtig Sie müssen die Zelle nach der Ausführung von <code>ciphers --disallow</code> neu starten.</p>
<code>--list (-l)</code>	Keines	Listet die zulässigen Verschlüsselungen auf, die derzeit verwendet werden.
<code>--reset (-r)</code>	Keines	<p>Setzt die Liste der zulässigen Verschlüsselungen auf die Standardliste zurück. Wenn die Zertifikate dieser Zelle unzulässige Verschlüsselungen verwenden, können Sie erst dann eine SSL-Verbindung mit der Zelle herstellen, wenn Sie die neuen Zertifikate installiert haben, die eine zulässige Verschlüsselung verwenden.</p> <hr/> <p>Wichtig Sie müssen die Zelle nach der Ausführung von <code>ciphers --reset</code> neu starten.</p>

Beispiel: Untersagen der Verwendung von zwei Verschlüsselungen

VMware Cloud Director enthält eine vorkonfigurierte Liste aktivierter Verschlüsselungen.

In diesem Beispiel wird gezeigt, wie Sie zusätzliche Verschlüsselungen aus der Liste der zulässigen Verschlüsselungen aktivieren und die Zulassung von Verschlüsselungen, die Sie nicht verwenden möchten, aufheben können.

- 1 Rufen Sie die Liste der standardmäßig aktivierten Verschlüsselungen ab.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -l
```

Die Ausgabe des Befehls gibt die Liste der aktivierten Verschlüsselungen zurück.

```
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 Rufen Sie eine Liste aller Verschlüsselungen ab, die die Zelle während eines SSL-Handshakes anbieten kann.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
```

Die Ausgabe des Befehls gibt die Liste der zulässigen Verschlüsselungen zurück.

```
# ./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 Geben Sie an, welche Verschlüsselungen deaktiviert werden sollen.

Wenn Sie den Befehl ausführen und eine Verschlüsselung nicht explizit deaktivieren, wird sie aktiviert.

```
[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 Führen Sie den Befehl aus, um die Liste der aktivierten Verschlüsselungen zu überprüfen. Jede Verschlüsselung, die in der Liste nicht vorhanden ist, wird deaktiviert.

```
root@bos1-vcd-static-211-90 [ /opt/vmware/vcloud-director/bin ]# ./cell-management-tool
ciphers -l
```

Die Ausgabe gibt eine Liste aller derzeit aktivierten Verschlüsselungen zurück.

```
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
```

Verwalten der Liste der zulässigen SSL-Protokolle

Um den Satz von SSL-Protokollen zu konfigurieren, die die Zelle während des SSL-Handshake-Vorgangs bietet, verwenden Sie den Befehl `ssl-protocols` des Zellenverwaltungstools.

Wenn ein Client eine SSL-Verbindung mit einer VMware Cloud Director-Zelle herstellt, bietet die Zelle nur die Protokolle an, die in ihrer Standardliste von zulässigen SSL-Protokollen konfiguriert sind. Mehrere Protokolle, einschließlich TLSv1, SSLv3 und SSLv2Hello, sind nicht in der Standardliste enthalten, weil bekannt ist, dass sie erhebliche Sicherheitsprobleme aufweisen.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem der VMware Cloud Director-Zelle als **root** an.

2 Führen Sie den Befehl aus, um die Liste der zulässigen SSL-Protokolle zu verwalten.

```
cell-management-tool ssl-protocols options
```

Tabelle 5-13. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `ssl-protocols`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--all-allowed (-a)</code>	Keines	Listet alle SSL-Protokolle auf, die VMware Cloud Director unterstützt.
<code>--disallow (-d)</code>	Durch Kommata getrennte Liste mit SSL-Protokollnamen.	<p>Konfiguriert die Liste der nicht zulässigen SSL-Protokolle neu, indem die in der Liste angegebenen Protokolle verwendet werden. Bei jeder Ausführung dieser Option müssen Sie die vollständige Liste der SSL-Protokolle angeben, die Sie deaktivieren möchten, da die Ausführung der Option die vorherige Einstellung überschreibt.</p> <p>Wichtig Wenn Sie die Option ohne Werte ausführen, werden alle SSL-Protokolle aktiviert.</p> <p>Um alle möglichen SSL-Protokolle anzuzeigen, führen Sie die Option <code>-a</code> aus.</p> <p>Wichtig Sie müssen die Zelle nach der Ausführung von <code>ssl-protocols --disallow</code> neu starten.</p>
<code>--list (-l)</code>	Keines	Listet die zulässigen SSL-Protokolle auf, die derzeit verwendet werden.
<code>--reset (-r)</code>	Keines	<p>Setzt die Liste der konfigurierten SSL-Protokolle auf die Standardeinstellung zurück.</p> <p>Wichtig Sie müssen die Zelle nach der Ausführung von <code>ssl-protocols --reset</code> neu starten.</p>

Beispiel: Listet zulässige und konfigurierte SSL-Protokolle auf und konfiguriert die Liste der nicht zulässigen SSL-Protokolle neu

Verwenden Sie die Option `--all-allowed (-a)`, um alle SSL-Protokolle aufzulisten, die die Zelle während des SSL-Handshake-Vorgangs bereitstellen darf.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

* TLSv1.2
* TLSv1.1
* TLSv1
* SSLv3
* SSLv2Hello
```

Diese Liste ist typischerweise eine Übermenge der SSL-Protokolle, für deren Unterstützung die Zelle konfiguriert ist. Um diese SSL-Protokolle aufzulisten, verwenden Sie die Option `--list (-l)`.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

* TLSv1.2
* TLSv1.1
```

Um die Liste der nicht zulässigen SSL-Protokolle neu zu konfigurieren, verwenden Sie die Option `--disallow (-d)`. Für diese Option ist eine durch Komma getrennte Liste der Teilmenge zulässiger von `ssl-protocols -a` erzeugter Protokolle erforderlich.

In diesem Beispiel wird die Liste der zulässigen SSL-Protokolle aktualisiert, sodass sie TLSv1 enthält. vCenter Server-Versionen vor 5.5 Update 3e erfordern TLSv1.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -d
SSLv3,SSLv2Hello
```

Sie müssen die Zelle nach Ausführung dieses Befehls neu starten.

Konfigurieren der Erfassung und Veröffentlichung von Metriken

Sie können den Befehl `configure-metrics` des Zellenverwaltungstools verwenden, um den zu erfassenden Metriksatz zu konfigurieren.

VMware Cloud Director kann Metriken mit aktuellen und historischen Informationen über die Leistung der virtuellen Maschine und den Ressourcenverbrauch erfassen. Verwenden Sie diesen Unterbefehl, um die Metriken zu konfigurieren, die VMware Cloud Director erfasst. Verwenden Sie den Unterbefehl `cell-management-tool cassandra`, um eine Apache Cassandra-Datenbank für die Verwendung als VMware Cloud Director-Metrik-Repository zu konfigurieren. Weitere Informationen finden Sie unter [Konfigurieren einer Cassandra-Metrikendatenbank](#).

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem der VMware Cloud Director-Zelle als **root** an.
- 2 Konfigurieren Sie die Metriken, die von VMware Cloud Director erfasst werden.

```
/opt/vmware/vcloud-director/bin/cell-management-tool configure-metrics --metrics-config
pathname
```

Tabelle 5-14. Optionen und Argumente des Zellenverwaltungstools, Unterbefehl `configure-metrics`

Befehl	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--repository-host</code> (Veraltet)	Hostname oder IP-Adresse des KairosDB-Hosts	Veraltet. Verwenden Sie die Option <code>--cluster-nodes</code> des Unterbefehls <code>cell-management-tool cassandra</code> , um eine Apache Cassandra-Datenbank für die Verwendung als VMware Cloud Director-Metrik-Repository zu konfigurieren.
<code>--repository-port</code> (Veraltet)	Zu verwendender KairosDB-Port	Veraltet. Verwenden Sie die Option <code>--port</code> des Unterbefehls <code>cell-management-tool cassandra</code> , um eine Apache Cassandra-Datenbank für die Verwendung als VMware Cloud Director-Metrik-Repository zu konfigurieren.
<code>--metrics-config</code>	Pfadname	Pfad der Metrikkonfigurationsdatei

- 3 Bei Verwendung von VMware Cloud Director 10.2.2 oder höher können Sie die Metrikveröffentlichung aktivieren, indem Sie folgenden Befehl ausführen.

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

Ab VMware Cloud Director 10.2.2 ist die Metrikveröffentlichung standardmäßig deaktiviert.

Beispiel: Konfigurieren der Verbindung einer Metrikendatenbank

In diesem Beispiel wird die Metrikerfassung wie in der Datei `/tmp/metrics.groovy` angegeben konfiguriert.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool configure-metrics --
metrics-config /tmp/metrics.groovy
```

Der Metrikerfassungsdienst von VMware Cloud Director implementiert eine Teilmenge der vomvSphere-Leistungs-Manager erfassten Metriken. Weitere Informationen zu Metrikenamen und Erfassungsparametern erhalten Sie in der Dokumentation zum vSphere-Leistungs-Manager. Die `metrics-config`-Datei zitiert einen oder mehrere Metrikenamen und bietet Erfassungsparameter für jede zitierte Metrik. Beispiel:

```
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"
  }
}
```

Die folgenden Metrikenamen werden unterstützt.

Tabelle 5-15. Metrikenamen

Metrikname	Beschreibung
<code>cpu.usage.average</code>	Hostansicht der durchschnittlich aktiv genutzten CPU dieser virtuellen Maschine als Prozentsatz der verfügbaren Gesamtmenge. Umfasst alle Kerne in allen Sockets.
<code>cpu.usagemhz.average</code>	Hostansicht der durchschnittlich aktiv genutzten CPU dieser virtuellen Maschine als Rohmessung. Umfasst alle Kerne in allen Sockets.
<code>cpu.usage.maximum</code>	Hostansicht der maximal aktiv genutzten CPU dieser virtuellen Maschine als Prozentsatz der verfügbaren Gesamtmenge. Umfasst alle Kerne in allen Sockets.
<code>mem.usage.average</code>	Arbeitsspeicher, der von dieser virtuellen Maschine als Prozentsatz des konfigurierten Gesamtarbeitsspeichers verwendet wird.
<code>disk.provisioned.latest</code>	Speicherplatz, der dieser virtuellen Festplatte im enthaltenen virtuellen Datacenter der Organisation zugewiesen wird.
<code>disk.used.latest</code>	Speicher, der von allen virtuellen Festplatten verwendet wird.

Tabelle 5-15. Metriknamen (Fortsetzung)

Metrikname	Beschreibung
<code>disk.read.average</code>	Die durchschnittliche Leserate für alle virtuellen Festplatten.
<code>disk.write.average</code>	Die durchschnittliche Schreibrate für alle virtuellen Festplatten.

Hinweis Wenn eine virtuelle Maschine über mehrere Festplatten verfügt, meldet VMware Cloud Director Metriken als Aggregat für alle Festplatten. CPU-Metriken sind ein Aggregat aller Kerne und Sockets.

Sie können für jede benannte Metrik die folgenden Erfassungsparameter angeben.

Tabelle 5-16. Metrik-Erfassungsparameter

Parametername	Wert	Beschreibung
<code>currentInterval</code>	Ganzzahl in Sekunden	Das Intervall in Sekunden, das bei der Abfrage nach den aktuell verfügbaren Metrikwerten für aktuelle Metrikabfragen verwendet werden soll. Der Standardwert ist 20. VMware Cloud Director unterstützt Werte größer als 20 nur für Metriken der Ebene 1, wie durch den vSphere-Leistungs-Manager definiert.
<code>historicInterval</code>	Ganzzahl in Sekunden	Das Intervall in Sekunden, das bei der Abfrage von Verlaufs-Metrik-Werten verwendet werden soll. Der Standardwert ist 20. VMware Cloud Director unterstützt Werte größer als 20 nur für Metriken der Ebene 1, wie durch den vSphere-Leistungs-Manager definiert.
<code>entity</code>	Einer der folgenden: HOST, VM	Der Typ des VC-Objekts, für das die Metrik verfügbar ist. Der Standardwert ist VM. Nicht alle Metriken sind für alle Elemente verfügbar.
<code>instance</code>	Ein vSphere-Leistungs-Manager mit <code>PerfMetricId</code> -Instanzbezeichner	Gibt an, ob Daten für einzelne Instanzen einer Metrik (z. B. einzelne CPU-Kerne), ein Aggregat aller Instanzen oder beides abgerufen werden soll. Bei einem Wert von "*" werden alle Metriken, die Instanz und das Aggregat erfasst. Bei einer leeren Zeichenfolge "" werden nur die Aggregatdaten erfasst. Bei einer bestimmten Zeichenfolge wie "DISKFILE" werden Daten nur für diese Instanz erfasst. Der Standardwert ist "*".
<code>minReportingInterval</code>	Ganzzahl in Sekunden	Gibt ein Standard-Aggregationsintervall in Sekunden an, das bei der Berichterstellung von Zeitreihendaten verwendet werden soll. Bietet weitere Kontrolle über die Berichterstellungsgranularität, wenn die Granularität des Erfassungsintervalls nicht ausreicht. Der Standardwert ist 0, d. h. kein dediziertes Berichtsintervall.
<code>aggregator</code>	Einer der folgenden: AVERAGE, MINIMUM, MAXIMUM, SUMMATION	Der Typ der Aggregation, die während des <code>minReportingInterval</code> durchzuführen ist. Der Standardwert ist AVERAGE.

Konfigurieren einer Cassandra-Metriken Datenbank

Mit dem Befehl `cassandra` des Zellenverwaltungstools können Sie die Zelle mit einer optionalen Metriken Datenbank verbinden.

VMware Cloud Director kann Metriken mit aktuellen und historischen Informationen über die Leistung der virtuellen Maschine und den Ressourcenverbrauch erfassen. Verwenden Sie diesen Unterbefehl, um eine Apache Cassandra-Datenbank für die Verwendung als VMware Cloud Director-Metrik-Repository zu konfigurieren. Verwenden Sie den Unterbefehl `cell-management-tool configure-metrics` zum Konfigurieren des zu erfassenden Metriksatzes. Weitere Informationen finden Sie unter [Konfigurieren der Erfassung und Veröffentlichung von Metriken](#).

Daten für historische Metriken werden in einer Apache-Cassandra-Datenbank gespeichert. Weitere Informationen zur Konfiguration optionaler Datenbanksoftware zum Speichern und Abrufen von Leistungsmetriken finden Sie unter [Installieren und Konfigurieren einer Cassandra-Datenbank zum Speichern von historischen Metrikdaten](#).

Um eine Verbindung zwischen VMware Cloud Director und einer Apache-Cassandra-Datenbank zu erstellen, verwenden Sie eine Befehlszeile im folgenden Format:

```
cell-management-tool cassandra Optionen
```

Tabelle 5-17. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `cassandra`

Befehl	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Optionen für diesen Befehl bereit.
<code>--add-rollback</code>	Keines	Aktualisiert das Metrikschema, um mehrstufige Metriken einzubeziehen. Weitere Informationen finden Sie im Installieren und Konfigurieren einer Cassandra-Datenbank zum Speichern von historischen Metrikdaten .
<code>--cluster-nodes</code>	<i>Adresse</i> [, <i>Adresse</i> ...]	Durch Kommas getrennte Liste der Cassandra-Cluster-Knoten für VMware Cloud Director-Metriken.
<code>--clean</code>	Keines	Entfernen Sie Cassandra-Konfigurationseinstellungen aus der VMware Cloud Director-Datenbank.
<code>--configure</code>	Keines	Konfigurieren Sie VMware Cloud Director für die Verwendung mit einem vorhandenen Cassandra-Cluster.

Tabelle 5-17. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `cassandra` (Fortsetzung)

Befehl	Argument	Beschreibung
<code>--dump</code>	Keines	Verwerfen Sie die aktuelle Verbindungskonfiguration.
<code>--keyspace</code>	Zeichenfolge	Legen Sie für VMware Cloud Director-Schlüsselraumnamen in Cassandra <i>string</i> fest. Standardmäßig <code>vcloud_metrics</code> .
<code>--offline</code>	Keines	Konfigurieren Sie Cassandra für die Verwendung mit VMware Cloud Director. Testen Sie die Konfiguration jedoch nicht durch eine Verbindung zu VMware Cloud Director.
<code>--password</code>	Zeichenfolge	Kennwort des Benutzers der Cassandra-Datenbank
<code>--port</code>	Ganzzahl	Verbindungsport an jedem Clusterknoten. Die Standardeinstellung lautet 9042.
<code>--ttl</code>	Ganzzahl	Behalten Sie die Metrikdaten für <i>Ganzzahl</i> /Tage bei. Setzen Sie <i>Ganzzahl</i> auf 0, um die Metrikdaten für immer beizubehalten.
<code>--update-schema</code>	Keines	Initialisiert das Cassandra-Schema zum Speichern von VMware Cloud Director-Metrikdaten.
<code>--username</code>	Zeichenfolge	Benutzername des Benutzers der Cassandra-Datenbank.

Beispiel: Konfigurieren einer Cassandra-Datenbankverbindung

Verwenden Sie einen Befehl wie diesen, wobei `node1-ip`, `node2-ip`, `node3-ip` und `node4-ip` die IP-Adressen der Mitglieder des Cassandra-Clusters darstellen. Es wird der Standardport (9042) verwendet. Metrikdaten werden 15 Tage lang aufbewahrt.

```
[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
```

Sie müssen die Zelle nach Ausführung dieses Befehls neu starten.

Wiederherstellen des Kennworts für den Systemadministrator

Wenn Sie den Benutzernamen und das Kennwort für die VMware Cloud Director-Datenbank kennen, können Sie den Befehl `recover-password` des Zellenverwaltungstools verwenden, um das Kennwort des VMware Cloud Director-Systemadministrators wiederherzustellen.

Mit dem Befehl `recover-password` des Zellenverwaltungstools kann ein Benutzer, der den Benutzernamen und das Kennwort der VMware Cloud Director-Datenbank kennt, das Kennwort des VMware Cloud Director-Systemadministrators wiederherstellen.

Verwenden Sie zum Wiederherstellen des Systemadministratorkennworts eine Befehlszeile im folgenden Format:

```
cell-management-tool recover-password Optionen
```

Tabelle 5-18. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `recover-password`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keine	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--dbuser</code>	Der Benutzername des VMware Cloud Director-Datenbankbenutzers.	Muss in der Befehlszeile angegeben werden.
<code>--dbpassword</code>	Das Kennwort des VMware Cloud Director-Datenbankbenutzers.	Wird vom Benutzer abgefragt, falls es nicht angegeben ist.

Aktualisieren des Fehlerstatus einer Aufgabe

Verwenden Sie den Befehl `fail-tasks` im Zellenverwaltungstool, um den Abschlussstatus zu aktualisieren, der mit Aufgaben verknüpft ist, die beim absichtlichen Herunterfahren der Zelle ausgeführt wurden. Sie können den Befehl `fail-tasks` nur verwenden, wenn alle Zellen heruntergefahren wurden.

Wenn Sie eine Zelle mit dem Befehl „`cell-management-tool -q`“ stilllegen, werden in der Regel die aufgeführten Aufgaben innerhalb von wenigen Minuten ordnungsgemäß beendet. Wenn Aufgaben weiterhin für eine stillgelegte Zelle ausgeführt werden, kann der Superuser die Zelle herunterfahren, wodurch alle laufenden Aufgaben fehlschlagen. Nach dem Herunterfahren und dem damit verbundenen zwangsläufigen Fehlschlagen der Aufgaben kann der Superuser `cell-management-tool fail-tasks` ausführen, um den Abschlussstatus für diese Aufgaben zu aktualisieren. Diese Art der Aktualisierung des Abschlussstatus ist optional. Sie trägt jedoch zur Unterstützung der Wartung der Integrität der Systemprotokolle bei, indem die durch eine administrative Aktion verursachten Fehler eindeutig ermittelt werden.

Um eine Liste mit Aufgaben zu erzeugen, die nach wie vor für eine stillgelegte Zelle ausgeführt werden, verwenden Sie eine Befehlszeile im folgenden Format:

```
cell-management-tool -u sysadmin-username cell --status-verbose
```

Tabelle 5-19. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `fail-tasks`

Befehl	Argument	Beschreibung
<code>--help (-h)</code>	Keine	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--message (-m)</code>	Meldungstext	Der Meldungstext, der als Beendigungsstatus verwendet werden soll.

Beispiel: Erzwungenes Beenden von auf einer Zelle aufgeführten Aufgaben

In diesem Beispiel wird der Aufgabenabschlussstatus aktualisiert, der mit einer Aufgabe verknüpft ist, die auch dann ausgeführt wird, wenn die Zelle bereits heruntergefahren wurde.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool fail-tasks -m
"administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system,
Organization: org1
Would you like to fail the tasks listed above?
```

Geben Sie **y** ein, um die Aufgabe mit einem Abschlussstatus von **administrative shutdown** zu aktualisieren. Geben Sie **n** ein, wenn die Aufgabe weiter ausgeführt werden soll.

Hinweis Wenn in der Antwort mehrere Aufgaben zurückgegeben werden, müssen Sie entweder alle von ihnen abbrechen oder nichts unternehmen. Sie können keine Untermenge der Aufgaben abbrechen.

Konfigurieren der Behandlung von Überwachungsmeldungen

Verwenden Sie den Befehl `configure-audit-syslog` des Zellenverwaltungstools zum Konfigurieren der Art und Weise, wie das System Überwachungsmeldungen protokolliert.

Dienste in den einzelnen VMware Cloud Director-Zellen protokollieren Überwachungsmeldungen an die VMware Cloud Director-Datenbank, in der diese 90 Tage aufbewahrt werden. Um Überwachungsmeldungen länger aufzubewahren, können Sie VMware Cloud Director-Dienste konfigurieren, damit Überwachungsmeldungen zusätzlich zur VMware Cloud Director-Datenbank auch an das Linux `syslog`-Dienstprogramm gesendet werden.

Mit dem Systemkonfigurationsskript können Sie angeben, wie Überwachungsmeldungen behandelt werden. Weitere Informationen finden Sie unter „Konfigurieren der Netzwerk- und Datenbankverbindungen“ im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*. Die bei der Systemkonfiguration angegebenen Protokollierungsoptionen sind in zwei Dateien gespeichert: `global.properties` und `responses.properties`. Sie können die Konfiguration der Protokollierung von Überwachungsmeldungen in beiden Dateien mit einer Zellenverwaltungstool-Befehlszeile folgenden Formats ändern:

```
cell-management-toolconfigure-audit-syslog options
```

Alle Änderungen, die Sie mit diesem Unterbefehl des Zellenverwaltungstools vornehmen, bleiben in den Dateien `global.properties` und `responses.properties` der Zelle erhalten. Änderungen werden erst nach dem Neustart der Zelle wirksam.

Tabelle 5-20. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `configure-audit-syslog`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--disable (-d)</code>	Keines	Deaktivieren Sie die Protokollierung von Überwachungsereignissen in <code>syslog</code> . Überwachungsereignisse werden nur in der VMware Cloud Director-Datenbank protokolliert. Mit dieser Option werden die Werte der Eigenschaften <code>audit.syslog.host</code> und <code>audit.syslog.port</code> in <code>global.properties</code> und <code>responses.properties</code> zurückgesetzt.
<code>--syslog-host (-loghost)</code>	IP-Adresse oder vollqualifizierter Domänenname des Syslog-Server-Hosts	Mit dieser Option wird der Wert der <code>audit.syslog.host</code> -Eigenschaft auf die angegebene Adresse oder den vollqualifizierten Domännennamen festgelegt.
<code>--syslog-port (-logport)</code>	Ganzzahl im Bereich 0 bis 65535	Mit dieser Option wird der Wert der <code>audit.syslog.port</code> -Eigenschaft auf die angegebene Ganzzahl festgelegt.

Wenn Sie einen Wert für `--syslog-host` und/oder `--syslog-port` angeben, wird mit dem Befehl überprüft, ob der angegebene Wert das richtige Format aufweist. Die Kombination aus Host und Port für den Netzwerkzugriff oder das Vorhandensein eines ausgeführten `syslog`-Dienstes wird jedoch nicht getestet.

Beispiel: Ändern des Hostnamens des Syslog-Servers

Wichtig Mit diesem Befehl vorgenommene Änderungen werden in die globale Konfigurationsdatei und in die Antwortdatei geschrieben. Vergewissern Sie sich vor Verwendung dieses Befehls, dass sich die Antwortdatei am richtigen Speicherort befindet (in `/opt/vmware/vcloud-director/etc/responses.properties`) und beschreibbar ist. Weitere Informationen dazu finden Sie unter „Schützen und Wiederverwenden der Antwortdatei“ im *Installations-, Konfigurations- und Upgrade-Handbuch zu VMware Cloud Director*.

Um den Host zu ändern, an den `syslog`-Meldungen gesendet werden, verwenden Sie einen Befehl wie den folgenden:

```
[root@cell11 /opt/vmware/vcloud-director/bin]# cell-management-tool configure-audit-syslog
-loghost syslog.example.com
Using default port 514
```

Bei diesem Beispiel wird davon ausgegangen, dass der neue Host `syslog`-Meldungen am Standardport überwacht.

Mit dem Befehl werden `global.properties` und `responses.properties` aktualisiert, aber die Änderungen werden erst nach dem Neustart der Zelle wirksam.

Konfigurieren von E-Mail-Vorlagen

Um die Vorlagen zu verwalten, die das System beim Erstellen von E-Mail-Warnungen verwendet, können Sie den Befehl `manage-email` des Zellenverwaltungstools verwenden.

Das System sendet standardmäßig E-Mail-Warnungen, mit denen Systemadministratoren bei Ereignissen und Zuständen benachrichtigt werden, die wahrscheinlich ihr Eingreifen erfordern. Die Liste der E-Mail-Empfänger kann unter Verwendung der VMware Cloud Director-API oder der Webkonsole aktualisiert werden. Sie können den standardmäßigen E-Mail-Inhalt für jede Art von Warnungen überschreiben, indem Sie eine Zellenverwaltungstool-Befehlszeile im folgenden Format verwenden:

```
cell-management-tool manage-email options
```

Tabelle 5-21. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `manage-email`

Option	Argument	Beschreibung
<code>--help</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--delete</code>	Vorlagenname	Der Name der zu löschenden Vorlage.
<code>--lookup</code>	Vorlagenname	Dieses Argument ist optional. Wenn Sie es nicht eingeben, gibt der Befehl eine Liste aller Vorlagenamen zurück.
<code>--locale</code>	Das Gebietsschema der Vorlage	Standardmäßig wird dieser Befehl für Vorlagen mit dem Gebietsschema en-US verwendet. Verwenden Sie diese Option, um ein anderes Gebietsschema anzugeben.
<code>--set-template</code>	Pfadname zu einer Datei, die eine aktualisierte E-Mail-Vorlage enthält	Diese Datei muss auf dem lokalen Host zugänglich und vom Benutzer <code>vcloud.vcloud</code> lesbar sein. Beispiel: <code>/tmp/my-email-template.txt</code>

Es gibt unterschiedliche zulässige Vorlagenamen, die Sie für verschiedene E-Mail-Benachrichtigungen verwenden können.

Tabelle 5-22. Namen für VMware Cloud Director-E-Mail-Benachrichtigungen

Name	Beschreibung	Zeitpunkt, zu dem die E-Mail gesendet wird	Empfänger
<code>VAPP_UNDEPLOY_NOTIFICATION_DEFAULT</code>	Warnung , wenn die vApp-Laufzeit-Lease in Kürze abläuft. Wenn die Lease abläuft, hält VMware Cloud Director die vApp an oder schaltet sie aus.	Bevor die Laufzeit-Lease einer vApp abläuft, je nach konfigurierter Bereitstellung und Warnzeit für Speicher-Lease.	Der Besitzer der vApp; wenn es sich bei dem Besitzer um einen Systemadministrator handelt, erhalten die Organisationsadministratoren die Benachrichtigung.
<code>VAPP_STORAGE_NOTIFICATION_DEFAULT</code>	Warnung , wenn die vApp-Speicher-Lease in Kürze abläuft. Wenn die Lease abläuft, löscht VMware Cloud Director die vApp.	Bevor die Speicher-Lease einer vApp abläuft, je nach konfigurierter Bereitstellung und Warnzeit für Speicher-Lease.	Der Besitzer der vApp; wenn es sich bei dem Besitzer um einen Systemadministrator handelt, erhalten die Organisationsadministratoren die Benachrichtigung.
<code>VAPP_STORAGE_NOTIFICATION_FLEXIBLE</code>	Warnung , wenn die vApp-Speicher-Lease in Kürze abläuft. Wenn die Lease abläuft, kennzeichnet	Bevor die Speicher-Lease einer vApp abläuft, je nach konfigurierter Bereitstellung und Warnzeit für Speicher-Lease.	Der Besitzer der vApp; wenn es sich bei dem Besitzer um einen Systemadministrator handelt, erhalten die

Tabelle 5-22. Namen für VMware Cloud Director-E-Mail-Benachrichtigungen (Fortsetzung)

Name	Beschreibung	Zeitpunkt, zu dem die E-Mail gesendet wird	Empfänger
VAPP_STORAGE_NOTIFICATION_BODY	VMware Cloud Director die vApp als abgelaufen.		Organisationsadministratoren die Benachrichtigung.
VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY	Warnung, wenn die Speicher-Lease der vApp-Vorlage in Kürze abläuft. Wenn die Lease abläuft, löscht VMware Cloud Director die vApp-Vorlage.	Bevor die Speicher-Lease einer vApp-Vorlage abläuft, je nach konfigurierter Bereitstellung und Warnzeit für Speicher-Lease.	Der Besitzer der vApp-Vorlage; wenn es sich bei dem Besitzer um einen Systemadministrator handelt, erhalten die Organisationsadministratoren die Benachrichtigung.
VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY	Warnung, wenn die Speicher-Lease der vApp-Vorlage in Kürze abläuft. Wenn die Lease abläuft, kennzeichnet VMware Cloud Director die vApp-Vorlage als abgelaufen.	Bevor die Speicher-Lease einer vApp-Vorlage abläuft, je nach konfigurierter Bereitstellung und Warnzeit für Speicher-Lease.	Der Besitzer der vApp-Vorlage; wenn es sich bei dem Besitzer um einen Systemadministrator handelt, erhalten die Organisationsadministratoren die Benachrichtigung.
DISK_STORAGE_ALERT	Festplattenspeicherwarnung (rote Warnung)	Wenn auf dem Datenspeicher wenig Festplattenspeicher vorhanden ist und er den roten Schwellenwert erreicht.	Systemadministratoren
DISK_STORAGE_ALERT_VDCS	Festplattenspeicherwarnung für Provider-VDCs. Die E-Mail enthält eine Liste der Provider-VDCs, die den Datenspeicher verwenden, für den aufgrund geringen Festplattenspeichers eine rote Warnung angezeigt wird.	Wenn auf dem Datenspeicher wenig Festplattenspeicher vorhanden ist und er den roten Schwellenwert erreicht.	Systemadministratoren
VM_HW_UPGRADE_INVALID_POWER_STATE	Eine Benachrichtigung über den Betriebszustand einer VM.	Wenn ein Benutzer versucht, ein Upgrade der Hardwareversion einer VM durchzuführen.	Der Besitzer der VM; wenn es sich bei dem Besitzer um einen Systemadministrator handelt, erhalten die Organisationsadministratoren die Benachrichtigung.
VM_UPDATE_NESTED_HV_INVALID_POWER_STATE	Um ein Upgrade der virtuellen Hardware durchzuführen, müssen Sie die VM ausschalten.	Wenn ein Benutzer versucht, ein Upgrade der Hardwareversion einer VM durchzuführen.	Der Besitzer der VM; wenn es sich bei dem Besitzer um einen Systemadministrator handelt, erhalten die Organisationsadministratoren die Benachrichtigung.
FEDERATION_CERTIFICATE_SUCCESS	Die Benachrichtigung zum Ablauf des Verbundzertifikats wird an alle Organisationsadministratoren gesendet, wenn ein Zertifikat für einen externen SSO-Server in Kürze abläuft. Die Organisationsadministratoren werden dazu	Wenn ein Verbundzertifikat innerhalb von 7 Tagen ab dem aktuellen Datum abläuft.	Organisationsadministratoren

Tabelle 5-22. Namen für VMware Cloud Director-E-Mail-Benachrichtigungen (Fortsetzung)

Name	Beschreibung	Zeitpunkt, zu dem die E-Mail gesendet wird	Empfänger
FEDERATION_CERTIFICATE_SUCCESS	fordert, ein neues Zertifikat vom SSO-Server herunterzuladen und VMware Cloud Director zu aktualisieren.		
IPSEC_VPN_TUNNEL_ERROR IPSEC_VPN_TUNNEL_ERROR_SUMMARY	VPN-Tunnelfehler (rote Warnung)	Wenn der VPN-Tunnel nicht betriebsbereit ist.	Systemadministratoren
IPSEC_VPN_TUNNEL_ENABLED IPSEC_VPN_TUNNEL_ENABLED_SUMMARY	VPN-Tunnel aktiviert (grüne Warnung)	Wenn der VPN-Tunnel wieder funktioniert, nachdem er nicht betriebsbereit war.	Systemadministratoren

Tabelle 5-23. Nicht anpassbare E-Mail-Vorlagen

Benachrichtigung	Zeitpunkt, zu dem die E-Mail gesendet wird	Empfänger
E-Mail-Warnung zu erneut verbundenem vCenter Server	Wenn ein vCenter Server erneut verbunden wird.	Systemadministratoren
E-Mail-Warnung zu getrennter Verbindung von vCenter Server. In der E-Mail wird angegeben, ob ein Fehler oder eine Benutzeranforderung die Trennung der Verbindung von vCenter Server verursacht hat.	Wenn die Verbindung eines vCenter Server getrennt wird.	Systemadministratoren
E-Mail-Warnung zu verloren gegangener AMQP-Verbindung. Warnung, dass VMware Cloud Director vom AMQP-Server getrennt wurde.	Wenn RabbitMQ nicht mehr funktioniert.	Systemadministratoren
E-Mail-Warnung zu unterbrochener Datenbankverbindung	Wenn VMware Cloud Director von der Datenbank getrennt wird.	Systemadministratoren
E-Mail-Warnung zu wiederhergestellter Datenbankverbindung	Wenn VMware Cloud Director erneut mit der Datenbank verbunden wird.	Systemadministratoren
E-Mail-Warnung zu vom Switch getrenntem Host	Wenn ein Host von den verfügbaren Switches getrennt wird.	Systemadministratoren
E-Mail-Warnung zu vom Distributed Virtual Switch getrenntem Host	Wenn ein Host von den verfügbaren Distributed Virtual Switches getrennt wird.	Systemadministratoren
E-Mail-Warnung zu LDAP-Fehler	Während der Synchronisierung mit LDAP.	Systemadministratoren

Tabelle 5-23. Nicht anpassbare E-Mail-Vorlagen (Fortsetzung)

Benachrichtigung	Zeitpunkt, zu dem die E-Mail gesendet wird	Empfänger
E-Mail-Warnung zur LDAP-Benutzersynchronisierung	Während der Umbenennung eines LDAP-Benutzers.	Systemadministratoren
E-Mail-Warnung zur Änderung von Sitezuordnungen	Die Sites haben kürzlich die Verbindung verloren, die Verbindung wurde wiederhergestellt oder sie sind weiterhin inaktiv.	Systemadministratoren

Beispiel: Aktualisieren einer E-Mail-Vorlage

Der folgende Befehl ersetzt die aktuellen Inhalte der `DISK_STORAGE_ALERT_VDCS`-E-Mail-Vorlage durch einen Inhalt, den Sie in einer Datei mit dem Namen `/tmp/DISK_STORAGE_ALERT_VDCS-new.txt` erstellt haben.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-email --set-template DISK_STORAGE_ALERT_VDCS /tmp/DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s):
$pvdcList
"
Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from
$productName The $datastore is used by the followingProvider VDC(s): $pvdcList
"

VCD Email notification details:
name                : DISK_STORAGE_ALERT_VDCS
description          : Alert when used disk storage exceeds threshold
config key           : email.template.DISK_STORAGE_ALERT_VDCS.en-US
template placeholders : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcList]
template content     : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcList
```

Finden von verwaisten VMs

Verwenden Sie den Befehl `find-orphan-vm`s des Zellenverwaltungstools, um Verweise auf virtuelle Maschinen zu finden, die in der vCenter-Datenbank, jedoch nicht in der VMware Cloud Director-Datenbank vorhanden sind.

Virtuelle Maschinen, auf die in der vCenter-Datenbank, jedoch nicht in der VMware Cloud Director-Datenbank verwiesen wird, werden als verwaiste VMs betrachtet, da VMware Cloud Director nicht auf diese zugreifen kann, obwohl sie möglicherweise Computing- und Speicherressourcen verbrauchen. Diese Art der Nichtübereinstimmung von Verweisen kann aus einer Reihe von Gründen auftreten, einschließlich Arbeitslasten mit einem hohen Volumen, Datenbankfehlern und administrativen Aktionen. Mit dem Befehl `find-orphan-vm`s kann ein

Administrator diese VMs auflisten, sodass sie entfernt oder erneut in VMware Cloud Director importiert werden können. Dieser Befehl ermöglicht die Angabe eines alternativen Trust Store, der möglicherweise benötigt wird, wenn Sie mit VMware Cloud Director- oder vCenter-Installationen arbeiten, die selbstsignierte Zertifikate verwenden.

Verwenden Sie einen Befehl folgenden Formats:

```
cell-management-tool find-orphan-vm options
```

Tabelle 5-24. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `find-orphan-vm`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--enableVerifyHostname</code>	Keines	Aktiviert die Komponente zur Hostnamenverifizierung des SSL-Handshakes.
<code>--host</code>	Erforderlich	IP-Adresse oder vollqualifizierter Domänenname der VMware Cloud Director-Installation für die Suche nach verwaisten VMs.
<code>--output-file</code>	Pfadname oder -	Vollständiger Pfadname der Datei, in die die Liste der verwaisten VMs geschrieben werden soll. Geben Sie den Pfadnamen - an, um die Liste in die Standardausgabe zu schreiben.
<code>--password (-p)</code>	Erforderlich	Kennwort für den VMware Cloud Director-Systemadministrator.
<code>--port</code>	VMware Cloud Director-HTTPS-Port.	Geben Sie dies nur an, wenn für diesen Befehl nicht der standardmäßige VMware Cloud Director-HTTPS-Port verwendet werden soll.
<code>--trustStore</code>	Vollständiger Pfadname zu einer Java-Trust Store-Datei.	Geben Sie dies nur an, wenn für diesen Befehl nicht die standardmäßige VMware Cloud Director-Trust Store-Datei verwendet werden soll.
<code>--trustStorePassword</code>	Kennwort für angegebenen <code>--trustStore</code>	Nur erforderlich, wenn Sie <code>--trustStore</code> zum Angeben einer alternativen Trust Store-Datei verwenden.

Tabelle 5-24. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `find-orphan-vm` (Fortsetzung)

Option	Argument	Beschreibung
<code>--trustStoreType</code>	Der Typ des angegebenen <code>--trustStore</code> (PKCS12, JCEKS ...)	Nur erforderlich, wenn Sie <code>--trustStore</code> zum Angeben einer alternativen Trust Store-Datei verwenden.
<code>--user (-u)</code>	Erforderlich	Benutzername des VMware Cloud Director-Systemadministrators.
<code>--vc-name</code>	Erforderlich	vCenter-Name für die Suche nach verwaisten VMs.
<code>--vc-password</code>	Erforderlich	Kennwort des vCenter-Administrators.
<code>--vc-user</code>	Erforderlich	Benutzername des vCenter-Administrators.

Beispiel: Finden von verwaisten VMs

In diesem Beispiel wird eine einzelne vCenter Server-Instanz abgefragt. Da `--output-file` als - angegeben ist, werden Ergebnisse in der Standardausgabe wiedergegeben.

```
[root@cell1 /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")
```

Beitreten zum Programm zur Verbesserung der Kundenzufriedenheit von VMware bzw. Verlassen dieses Programms

Um dem Programm zur Verbesserung der Kundenzufriedenheit (CEIP) beizutreten oder es zu verlassen, können Sie den Unterbefehl `configure-ceip` des Zellenverwaltungstools verwenden.

Dieses Produkt nimmt am Programm zur Verbesserung der Kundenzufriedenheit („CEIP“) von VMware teil. Einzelheiten im Hinblick auf die über CEIP gesammelten Daten und die Zwecke, für die diese von VMware verwendet werden, finden Sie im Trust & Assurance Center unter <http://www.vmware.com/trustvmware/ceip.html>. Mit dem Zellenverwaltungstool können Sie dem CEIP von VMware für dieses Produkt jederzeit beitreten bzw. dieses verlassen.

```
cell-management-tool
configure-ceip
Optionen
```

Wenn Sie nicht am CEIP von VMware für dieses Produkt teilnehmen möchten, führen Sie diesen Befehl mit der Option `--disable` aus.

Tabelle 5-25. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `configure-ceip`

Option	Argument	Beschreibung
<code>--help</code> (-h)	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--disable</code>	Keines	Das Programm zur Verbesserung der Benutzerfreundlichkeit von VMware verlassen
<code>--enable</code>	Keines	Am Programm zur Verbesserung der Benutzerfreundlichkeit von VMware teilnehmen
<code>--status</code>	Keine	Zeigt den aktuellen Teilnahmestatus dieses Produkts am Programm zur Verbesserung der Kundenzufriedenheit von VMware an.

Beispiel: Das Programm zur Verbesserung der Kundenzufriedenheit von VMware verlassen

Um das Programm zur Verbesserung der Kundenzufriedenheit von VMware zu verlassen, verwenden Sie einen Befehl wie den folgenden:

```
[root@cell11 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
disableParticipation disabled
```

Nach dem Ausführen dieses Befehls sendet das System keine Informationen mehr an das Programm zur Verbesserung der Kundenzufriedenheit von VMware.

Um den aktuellen Teilnahmestatus am Programm zur Verbesserung der Kundenzufriedenheit von VMware zu bestätigen, verwenden Sie einen Befehl wie den folgenden:

```
[root@cell11 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
statusParticipation disabled
```

Aktualisieren von Anwendungskonfigurationseinstellungen

Mit dem Unterbefehl `manage-config` des Zellenverwaltungstools können Sie verschiedene Anwendungskonfigurationseinstellungen aktualisieren, wie z. B. Katalogdrosselungsaktivitäten.

Tabelle 5-26. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `manage-config`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keines	Stellt eine Zusammenfassung der verfügbaren Optionen für diesen Unterbefehl bereit.
<code>--delete (-d)</code>	Keines	Entfernt die Konfigurationseinstellung für das Ziel.
<code>--lookup (-l)</code>	Keines	Suchen Sie nach dem Wert der Konfigurationseinstellung für das Ziel.
<code>--name (-n)</code>	Name der Konfigurationseinstellung	Der Name der Konfigurationseinstellung für das Ziel. Erforderlich mit Optionen <code>-d</code> , <code>-l</code> und <code>-v</code>
<code>--value (-v)</code>	Wert der Konfigurationseinstellung	Fügt den Wert für die Konfigurationseinstellung des Ziels hinzu oder aktualisiert diesen.

Sie können beispielsweise den Unterbefehl `manage-config` für [Konfigurieren von Katalogsynchronisierungsdrosselung](#) verwenden.

Konfigurieren von Katalogsynchronisierungsdrosselung

Um bei einer Vielzahl von Katalogelementen, die für andere Organisationen veröffentlicht oder von diesen abonniert werden, während der Katalogsynchronisierung eine Überlastung des Systems zu vermeiden, können Sie Katalogsynchronisierungsdrosselung konfigurieren. Sie können den Unterbefehl `manage-config` des Zellenverwaltungstools verwenden, um Katalogsynchronisierungsdrosselung zu konfigurieren, indem Sie die Anzahl der Bibliothekselemente begrenzen, die gleichzeitig synchronisiert werden können.

Wenn ein abonnierter Katalog Katalogsynchronisierung initiiert, lädt der veröffentlichte Katalog zuerst die Bibliothekselemente aus dem vCenter Server-Repository in den Speicher des VMware Cloud Director-Übertragungsdiensts herunter und erstellt dann Download-Links für den abonnierten Katalog. Sie können die Anzahl der Bibliothekselemente beschränken, die gleichzeitig

von allen veröffentlichten Katalogen heruntergeladen werden können. Sie können die Anzahl der Bibliothekselemente beschränken, die gleichzeitig von allen abonnierten Katalogen synchronisiert werden können. Sie können die Anzahl der Bibliothekselemente beschränken, die gleichzeitig von einem abonnierten Katalog synchronisiert werden können.

Sie können den Unterbefehl `manage-config` des Zellenverwaltungstools verwenden, um die Konfigurationseinstellungen für die Katalogdrosselung zu aktualisieren. Informationen zur Verwendung des Unterbefehls `manage-config` finden Sie unter [Aktualisieren von Anwendungskonfigurationseinstellungen](#).

Tabelle 5-27. Konfigurationseinstellungen für Katalogdrosselung

Konfigurationseinstellung	Standardwert	Beschreibung
<code>vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit</code>	30	<p>Die maximale Anzahl an Bibliothekselementen, die alle veröffentlichten Kataloge in der VMware Cloud Director-Instanz gleichzeitig von vCenter Server auf VMware Cloud Director herunterladen können.</p> <p>Wenn die Gesamtzahl der veröffentlichten Bibliothekselemente, die über die VMware Cloud Director-Instanz heruntergeladen werden, diesen Grenzwert überschreitet, werden die Bibliothekselemente entsprechend dem Grenzwert aufgeteilt und nacheinander heruntergeladen.</p>
<code>vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit</code>	30	<p>Die maximale Anzahl an Bibliothekselementen, die alle abonnierten Kataloge in einer VMware Cloud Director-Instanz gleichzeitig synchronisieren können.</p> <p>Wenn die Gesamtzahl der abonnierten Bibliothekselemente, die über die VMware Cloud Director-Instanz synchronisiert werden, diesen Grenzwert überschreitet, werden die Elemente entsprechend dem Grenzwert aufgeteilt und nacheinander synchronisiert.</p>
<code>contentLibrary.item.sync.batch.size</code>	10	<p>Die maximale Anzahl an Bibliothekselementen, die ein einzelner abonniertes Katalog gleichzeitig synchronisieren kann.</p> <p>Wenn ein abonniertes Katalog versucht, eine Anzahl von Bibliothekselementen zu synchronisieren, die diesen Grenzwert überschreitet, werden die Elemente entsprechend dem Grenzwert aufgeteilt und nacheinander synchronisiert.</p>

Beispiel: Konfigurieren von Synchronisierungsdrosselung für abonnierte Kataloge

Mit dem folgenden Befehl werden maximal fünf Bibliothekselemente festgelegt, die von einem einzelnen abonnierten Katalog gleichzeitig synchronisiert werden können.

```
[root@cell11 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n contentLibrary.item.sync.batch.size -v 5
```

Wenn ein abonnierter Katalog 13 Bibliothekselemente enthält, wird der Katalog in drei aufeinanderfolgenden Teilen synchronisiert. Der erste Teil enthält fünf Elemente, der zweite Teil die nächsten fünf Elemente und der letzte Teil die verbleibenden drei Elemente.

Fehlerbehebung bei fehlgeschlagenem Zugriff auf die VMware Cloud Director-Benutzeroberfläche

Um die gültigen IP-Adressen und DNS-Einträge für die VMware Cloud Director-Zellen in Ihrer VMware Cloud Director-Umgebung anzuzeigen und zu aktualisieren, können Sie den Unterbefehl `manage-config` des Zellenverwaltungstools verwenden.

Problem

Nach einer erfolgreichen Anmeldung können Sie nicht auf das VMware Cloud Director Service Provider Admin Portal oder das VMware Cloud Director Tenant Portal zugreifen.

Nachdem Sie Ihre Anmeldedaten in den Anmeldebildschirm eingegeben haben, wird die folgende Fehlermeldung angezeigt: `Start fehlgeschlagen. Während der Initialisierung trat ein Fehler auf. Die Ursache hierfür kann ein Zugriff auf die Anwendung über eine nicht unterstützte öffentliche URL oder eine schlechte Verbindung sein.`

Ursache

VMware Cloud Director verwendet eine Implementierung des CORS-Filters (Cross-Origin Resource Sharing, Ressourcenfreigabe zwischen verschiedenen Ursprüngen) zum Verwalten einer Liste aller gültigen Endpoints, die Sie für den Zugriff auf das Service Provider Admin Portal und das VMware Cloud Director Tenant Portal verwenden können.

Die CORS-Filterliste wird während der Zellenkonfiguration aufgefüllt und aktualisiert. Sie enthält HTTP- und HTTPS-Einträge mit IP-Adressen und DNS-Namen für alle Zellen in der Servergruppe. Sie enthält auch eine öffentliche IP-Adresse, die vom Lastausgleichsdienst verwendet wird, der der VMware Cloud Director-Servergruppe voransteht.

Während der Zellenkonfiguration von Appliance-Bereitstellungen wird die Liste nicht mit den DNS-Namen der VMware Cloud Director-Zellen aktualisiert, und Sie können für den Zugriff auf eine Zelle nicht deren DNS-Namen verwenden.

Lösung

- 1 Melden Sie sich, bei Bedarf mithilfe von SSH, als **root** bei einer der Zellen in der Servergruppe an.
- 2 Führen Sie die folgende Befehlszeile aus, um die gültigen URLs aufzulisten, die Sie für den Zugriff auf die VMware Cloud Director-Zellen in Ihrer Umgebung verwenden können.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
webapp.allowed.origins -l
```

Die Systemausgabe ist eine Liste, die HTTP- und HTTPS-Einträge mit IP-Adressen und DNS-Namen für alle Zellen in der Servergruppe enthält. Sie enthält auch eine öffentliche IP-Adresse, die vom Lastausgleichsdienst verwendet wird, der der VMware Cloud Director-Servergruppe voransteht.

Die Liste ist eine kommagetrennte Zeichenfolge, ohne Leerzeichen zwischen den Einträgen.

- 3 (Optional) Führen Sie die folgende Befehlszeile aus, um die Konfigurationseinstellung `webapp.allowed.origins` zu aktualisieren. In der Befehlszeile ist der Wertparameter der Einstellung eine Liste von IP-Adressen und DNS-Namen in einer kommagetrennten Zeichenfolge ohne Leerzeichen zwischen den Einträgen.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
webapp.allowed.origins -v "comma_separated_list_of_URLs_without_spaces"
```

Debuggen der vCenter-VM-Erkennung

Mithilfe des Unterbefehls `debug-auto-import` des Zellenverwaltungstools können Sie untersuchen, warum der Mechanismus zum Auffinden von vApps eine oder mehrere vCenter-VMs überspringt.

In der Standardkonfiguration erkennt ein Organisations-VDC automatisch vCenter-VMs, die in den Ressourcenpools erstellt werden, die dem VDC zugrunde liegen. Informationen zum Ermitteln und Übernehmen von vApps finden Sie im *VMware Cloud Director Service Provider Admin Portal-Handbuch*. Wenn eine vCenter-VM in einer erkannten vApp nicht angezeigt wird, können Sie den Unterbefehl `debug-auto-import` für diese VM oder das VDC ausführen.

```
cell-management-tool debug-auto-import Optionen
```

Der Unterbefehl `debug-auto-import` gibt eine Liste von vCenter-VMs und Informationen über die möglichen Gründe dafür aus, dass sie durch den Ermittlungsmechanismus übersprungen wurden. Die Liste enthält auch vCenter-VMs, die erkannt wurden, aber nicht in das Organisations-VDC importiert werden konnten.

Tabelle 5-28. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `debug-auto-import`

Option	Argument	Beschreibung
<code>--help</code> (-h)	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--org</code>	Name der Organisation	Optional. Listet Informationen zu den übersprungenen VMs für die angegebene Organisation auf.
<code>--vm</code>	VM-Name oder Teil eines VM-Namens	Listet Informationen zu den übersprungenen VMs auf, die den angegebenen VM-Namen enthalten. Optional, wenn die Option <code>--org</code> verwendet wird.

Beispiel: Debuggen der vCenter-VM-Erkennung nach dem VM-Namen `test`

Der folgende Befehl gibt Informationen über übersprungene vCenter-VMs für alle Organisationen zurück.

```
[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

In diesem Beispiel gibt die Systemausgabe Informationen zu drei vCenter-VMs zurück, die durch den Ermittlungsmechanismus übersprungen werden und deren Namen die Zeichenfolge `test` enthalten. VM `import-test3` ist ein Beispiel für eine virtuelle Maschine, die erkannt wurde, aber nicht in das VDC importiert werden konnte.

Erneutes Erzeugen von MAC-Adressen für ausgeweitete Multisite-Netzwerke

Wenn Sie zwei VMware Cloud Director-Sites verknüpfen, die mit derselben Installations-ID konfiguriert sind, kommt es in ausgeweiteten Netzwerken für diese Sites möglicherweise zu Konflikten bei MAC-Adressen. Zur Vermeidung solcher Konflikte müssen Sie die MAC-Adressen

an einem dieser Sites auf Basis eines benutzerdefinierten Ausgangswerts, der sich von der Installations-ID unterscheidet, erneut erzeugen.

Legen Sie während der erstmaligen Einrichtung von VMware Cloud Director eine Installations-ID fest. VMware Cloud Director verwendet die Installations-ID zum Erzeugen von MAC-Adressen für die Netzwerkschnittstellen der virtuellen Maschine. Zwei VMware Cloud Director-Installationen, die mit derselben Installations-ID konfiguriert werden, erzeugen möglicherweise identische MAC-Adressen. Doppelte MAC-Adressen können Konflikte in ausgeweiteten Netzwerken zwischen zwei verknüpften Sites hervorrufen.

Vor dem Erstellen von ausgeweiteten Netzwerken zwischen verknüpften Sites, die mit derselben Installations-ID konfiguriert sind, müssen Sie die MAC-Adressen an einer der Sites mithilfe des Unterbefehls `mac-address-management` des Zellenverwaltungstools erneut erzeugen.

```
cell-management-tool mac-address-management options
```

Richten Sie zum erneuten Erzeugen von MAC-Adressen einen benutzerdefinierten Ausgangswert ein, der sich von der Installations-ID unterscheidet. Die Installations-ID wird nicht vom Ausgangswert überschrieben, die Datenbank speichert jedoch den letzten Ausgangswert als zweiten Konfigurationsparameter, der die Installations-ID überschreibt.

Sie führen den Unterbefehl `mac-address-management` über ein beliebiges VMware Cloud Director-Mitglied der Servergruppe aus. Der Befehl wird für die VMware Cloud Director-Datenbank ausgeführt, d. h., der Befehl wird einmal für eine Servergruppe ausgeführt.

Wichtig Für die erneute Erzeugung von MAC-Adressen muss VMware Cloud Director zeitweilig heruntergefahren werden. Vor dem Starten der erneuten Erzeugung müssen Sie die Aktivitäten für alle Zellen in der Servergruppe stilllegen.

Tabelle 5-29. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `mac-address-management`

Option	Argument	Beschreibung
<code>--help</code> (-h)	Keines	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--regenerate</code>	Keines	Löscht alle MAC-Adressen, die nicht verwendet werden, und erzeugt neue MAC-Adressen auf Basis des aktuellen Ausgangswerts. Wurde zuvor kein Ausgangswert eingerichtet, werden die MAC-Adressen auf Basis der Installations-ID neu erzeugt. Die verwendeten MAC-Adressen werden beibehalten. Hinweis Alle Zellen in der Servergruppe müssen inaktiv sein. Informationen zum Stilllegen der Aktivitäten in einer Zelle finden Sie unter Verwalten einer Zelle .
<code>--regenerate-with-seed</code>	Ein Ausgangswert zwischen 0 und 63	Legt einen neuen benutzerdefinierten Ausgangswert in der Datenbank fest, löscht alle nicht verwendeten MAC-Adressen und erzeugt neue MAC-Adressen auf Basis des neu festgelegten Ausgangswerts. Die verwendeten MAC-Adressen werden beibehalten. Hinweis Alle Zellen in der Servergruppe müssen inaktiv sein. Informationen zum Stilllegen der Aktivitäten in einer Zelle finden Sie unter Verwalten einer Zelle .
<code>--show-seed</code>	Keines	Gibt den aktuellen Ausgangswert und die Anzahl der MAC-Adressen an, die für jeden Ausgangswert verwendet werden.

Wichtig Die verwendeten MAC-Adressen werden beibehalten. Zum Ändern einer verwendeten MAC-Adresse in eine neu erzeugte MAC-Adresse müssen Sie die MAC-Adresse der Netzwerkschnittstelle zurücksetzen. Informationen zum Bearbeiten von VM-Eigenschaften finden Sie im *Handbuch für das VMware Cloud Director Mandantenportal*.

Beispiel: Erneutes Erzeugen von MAC-Adressen auf Basis eines neuen benutzerdefinierten Ausgangswerts

Mit dem folgenden Befehl wird der aktuelle Ausgangswert auf *9* gesetzt und alle nicht verwendeten MAC-Adressen auf Basis des neu festgelegten Ausgangswerts neu erzeugt:

```
[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.
```

Beispiel: Anzeigen des aktuellen Ausgangswerts sowie der Anzahl der verwendeten MAC-Adressen für jeden Ausgangswert

Der folgende Befehl gibt Informationen über den aktuellen Ausgangswert und die Anzahl der MAC-Adressen pro Ausgangswert zurück:

```
[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
```

In diesem Beispiel zeigt die Systemausgabe, dass 9 als aktueller Ausgangswert verwendet wird, auf dem 12 MAC-Adressen basieren. Darüber hinaus gibt es eine MAC-Adresse, die auf einem vorherigen Ausgangswert oder einer Installations-ID von 1 basiert.

Aktualisieren der Datenbank-IP-Adressen auf VMware Cloud Director-Zellen

Um die IP-Adressen der VMware Cloud Director-Zellen in einem Datenbank-Hochverfügbarkeits-Cluster zu aktualisieren, können Sie das Zellenverwaltungstool verwenden.

Voraussetzungen

Um die IP-Adressen der Zellen in einem Datenbank-Hochverfügbarkeits-Cluster zu aktualisieren, müssen Sie die IP-Adresse des aktuellen primären Knotens angeben. Um die IP-Adresse zu finden, müssen Sie mithilfe der VMware Cloud Director-Appliance-API die Knoten-IDs der Standby-Knoten im Cluster notieren. Weitere Informationen finden Sie in der *API-Schema-Referenz für VMware Cloud Director-Appliance* unter <http://code.vmware.com>.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem einer beliebigen Zelle im Cluster als **root** an.
- 2 Überprüfen Sie, ob die Zelle auf diesem Knoten ausgeführt wird.

```
service vmware-vcd pid cell
```

Wenn die Zellenprozess-ID nicht NULL ist, wird die VMware Cloud Director-Zelle ausgeführt, und Sie können die IP-Adresse der Datenbank ändern, ohne die VMware Cloud Director-Zelle neu zu starten.

- 3 Führen Sie den folgenden Befehl aus, um die IP-Adressen in allen Zellen in der Servergruppe zu aktualisieren:

```
/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
```

Die Systemausgabe zeigt die erfolgreiche Neukonfiguration an.

- 4 (Optional) Überprüfen Sie, ob jede VMware Cloud Director-Zelle auf die richtige Datenbank-IP-Adresse verweist.

```
grep "database.jdbcUrl" /opt/vmware/vcloud-director/etc/global.properties
```

Die Systemausgabe gibt an, dass die Zelle aktualisiert wurde.

- 5 Wenn eine der Zellen nicht aktualisiert wurde, führen Sie den Befehl aus, um sie neu zu konfigurieren.

- Wenn die Zelle nicht ausgeführt wird, führen Sie den folgenden Befehl aus:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-
host primary node IP address
```

- Wenn die Zelle ausgeführt wird, führen Sie den folgenden Befehl aus:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-
host primary node IP address -i cell process ID
```

- 6 Wenn Sie eine Zelle, die nicht ausgeführt wird, neu konfiguriert haben, führen Sie den Befehl zum Neustarten des `vmware-vcd`-Dienstes aus.

- a Führen Sie den Befehl aus, um den Dienst anzuhalten.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid
cell) -s
```

- b Führen Sie den Befehl aus, um den Dienst zu starten.

```
systemctl start vmware-vcd
```

Erfassen von VMware Cloud Director-Protokollen

6

VMware Cloud Director stellt Protokollierungsinformationen für jede Cloud-Zelle in Ihrer Servergruppe bereit. Sie können die Protokolle anzeigen, um Ihre Zellen zu überwachen und Probleme zu beheben, die gegebenenfalls während der täglichen Ausführung von VMware Cloud Director auftreten.

VMware Cloud Director-Protokolle

Protokollname, Datei oder -verzeichnis	Beschreibung
<code>/opt/vmware/vcloud-director/logs/cell.log</code>	Konsolenausgabe von der VMware Cloud Director-Zelle.
<code>/opt/vmware/vcloud-director/logs/cell-management-tool</code>	Zellenverwaltungstool-Protokollnachrichten der Zelle.
<code>/opt/vmware/vcloud-director/logs/cell-runtime</code>	Laufzeitprotokollnachrichten der Zelle.
<code>/opt/vmware/vcloud-director/logs/cloud-proxy</code>	Cloud-Proxy-Nachrichten der Zelle.
<code>/opt/vmware/vcloud-director/logs/console-proxy</code>	Remotekonsolen-Proxy-Nachrichten der Zelle.
<code>/opt/vmware/vcloud-director/logs/server-group-communications</code>	Servergruppenkommunikationen der Zelle.
<code>/opt/vmware/vcloud-director/logs/statsfeeder</code>	Abrufen von VM-Metriken von vCenter Server sowie Speicherinformationen und -fehlermeldungen.
<code>/opt/vmware/vcloud-director/logs/vcloud-container-debug.log</code>	Protokollnachrichten der Zelle (Debugging-Ebene).
<code>/opt/vmware/vcloud-director/logs/vcloud-container-info.log</code>	Protokollnachrichten der Zelle (Informationsebene). In diesem Protokoll sind auch Warnungen und Fehler in der Zelle verzeichnet.
<code>/opt/vmware/vcloud-director/logs/vmware-vcd-watchdog.log</code>	Protokollnachrichten des Watchdogs für die Zelle (Informationsebene). Hier wird protokolliert, wenn die Zelle nicht mehr reagiert, neu gestartet wird usw.
<code>/opt/vmware/vcloud-director/logs/diagnostics.log</code>	Diagnoseprotokoll für die Zelle. Diese Datei bleibt leer, wenn die Diagnoseprotokollierung in der lokalen Protokollierungskonfiguration deaktiviert ist.
<code>/opt/vmware/vcloud-director/logs/YYYY_MM_DD.request.log</code>	HTTP-Anforderungsprotokolle im Standard-Apache-Protokollformat

Protokolle der VMware Cloud Director-Appliance

Die VMware Cloud Director-Appliance bietet einige zusätzliche Protokolldateien.

Protokolldatei	Beschreibung
<code>/opt/vmware/var/log/firstboot</code>	Enthält Protokollierungsinformationen im Zusammenhang mit dem ersten Start der Appliance.
<code>/opt/vmware/var/log/vcd</code>	Enthält Protokolle im Zusammenhang mit dem Setup, der Neukonfiguration und der Appliance-Synchronisierung der Replication Manager-Tool-Suite (<code>repmgr</code>).
<code>/opt/vmware/var/log/vcd/pg</code>	Enthält Protokolle im Zusammenhang mit der Sicherung der eingebetteten Appliance-Datenbank.
<code>/opt/vmware/etc/vami/ovfEnv.xml</code>	Enthält die OVF-Bereitstellungsparameter.
<code>/var/vmware/vpostgres/current/pgdata/log</code>	Enthält Protokolle im Zusammenhang mit der eingebetteten PostgreSQL-Datenbank.
<code>/opt/vmware/var/log/vami/updatecli.log</code>	Enthält die Protokollierung im Zusammenhang mit Appliance-Upgrades.

Verwenden Sie einen Texteditor, Textviewer oder ein Drittanbietertool zum Anzeigen der Protokolle.

Deinstallieren der VMware Cloud Director-Software

7

Verwenden Sie den Linux-Befehl `rpm`, um die VMware Cloud Director-Software von einem einzelnen Server zu deinstallieren.

Verfahren

- 1 Melden Sie sich beim Zielsystem als **root** an.
- 2 Heben Sie die Einbindung des Übertragungsdienstspeichers auf, der normalerweise unter `/opt/vmware/vcloud-director/data/transfer` eingebunden ist.
- 3 Öffnen Sie eine Konsole, Shell oder ein Terminalfenster und führen Sie den Linux-Befehl `rpm` aus.

```
rpm -e vmware-pherehome vmware-vcloud-director vmware-vcloud-director-rhel
```

Wenn andere installierte Pakete vom `vmware-vcloud-director`-Paket abhängig sind, werden Sie vom System aufgefordert, diese Pakete zu deinstallieren, bevor Sie VMware Cloud Director deinstallieren.