

Installations-, Konfigurations- und Upgrade-Handbuch zu vCloud Director

28. MÄRZ 2019

VMware Cloud Director 9.7

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 © 2010-2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Installations-, Konfigurations- und Upgrade-Handbuch zu vCloud Director	7
Aktuelle Informationen	8
1 Übersicht über Installation, Konfiguration und Upgrade von vCloud Director	9
vCloud Director-Architektur	9
Konfigurationsplanung	11
2 vCloud Director-Hardware- und Softwareanforderungen	12
Netzwerkkonfigurationsanforderungen für vCloud Director	13
Empfehlungen für die Netzwerksicherheit	15
3 Vor der Installation von vCloud Director oder der Bereitstellung der vCloud Director-Appliance	17
Vorbereiten der vCloud Director-Datenbank	17
Konfigurieren einer externen PostgreSQL-Datenbank für vCloud Director unter Linux	18
Konfigurieren einer externen Microsoft SQL Server-Datenbank für vCloud Director unter Linux	19
Vorbereiten des Übertragungsserverspeichers	21
Herunterladen und Installieren des öffentlichen Schlüssels von VMware	24
Installieren und Konfigurieren von NSX Data Center for vSphere für vCloud Director	24
Installieren und Konfigurieren von NSX-T Data Center für vCloud Director	25
4 Erstellen und Verwalten von SSL-Zertifikaten für vCloud Director unter Linux	27
Vor dem Erstellen von SSL-Zertifikaten für vCloud Director unter Linux	27
Erstellen von selbstsignierten SSL-Zertifikaten für vCloud Director unter Linux	28
Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores für vCloud Director unter Linux	29
Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores mit importierten privaten Schlüsseln für vCloud Director unter Linux	33
5 Installieren von vCloud Director unter Linux	35
Installieren von vCloud Director auf dem ersten Mitglied einer Servergruppe	37
Konfigurieren der Netzwerk- und Datenbankverbindungen	38
Interaktive Konfigurationsreferenz	40
Referenz für unbeaufsichtigte Konfiguration	42
Schützen und Wiederverwenden der Antwortdatei	46
Installieren von vCloud Director auf einem weiteren Mitglied einer Servergruppe	47
Einrichten von vCloud Director	50

6 Bereitstellen der vCloud Director-Appliance 52

- Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration 54
- Voraussetzungen für die Bereitstellung der vCloud Director-Appliance 57
- Bereitstellen der vCloud Director-Appliance mithilfe des vSphere Web Client oder des vSphere Client 57
 - Starten der Bereitstellung der vCloud Director-Appliance 58
 - Anpassen der vCloud Director-Appliance und Fertigstellen der Bereitstellung 60
- Bereitstellen der vCloud Director-Appliance mit dem VMware OVF Tool 63

7 Erstellung und Verwaltung von SSL-Zertifikaten der vCloud Director-Appliance 70

- Bereitstellen der vCloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation 70
- Erstellen und Importieren der von einer Zertifizierungsstelle signierten SSL-Zertifikate in die vCloud Director-Appliance 72
- Importieren von privaten Schlüsseln und den von einer Zertifizierungsstelle signierten SSL-Zertifikaten in die vCloud Director-Appliance 76
- Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und vCloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats 78
- Verlängern der vCloud Director-Appliance-Zertifikate 79

8 Konfiguration der vCloud Director-Appliance 81

- Anzeigen des Status der Zellen in einem Datenbank-Hochverfügbarkeits-Cluster 81
- Wiederherstellen nach einem Ausfall der primären Datenbank in einem Hochverfügbarkeits-Cluster 82
- Sichern und Wiederherstellen der eingebetteten Datenbank der vCloud Director-Appliance 83
 - Sichern der eingebetteten Datenbank der vCloud Director-Appliance 83
 - Wiederherstellen einer vCloud Director-Appliance-Umgebung mit einer HA-Datenbankkonfiguration 84
 - Wiederherstellen einer vCloud Director-Appliance-Umgebung ohne HA-Datenbankkonfiguration 87
- Konfigurieren des externen Zugriffs auf die vCloud Director-Datenbank 90
- Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vCloud Director-Appliance 91
- Bearbeiten der DNS-Einstellungen für die vCloud Director-Appliance 92
- Bearbeiten der statischen Routen für die Netzwerkschnittstellen der vCloud Director-Appliance 92
- Konfigurationsskripts in der vCloud Director-Appliance 94
- Ändern der PostgreSQL-Konfigurationen in der vCloud Director-Appliance 94

9 Verwenden der Replication Manager-Tool-Suite in einer Hochverfügbarkeits-Cluster-Konfiguration 96

- Überprüfen des Verbindungsstatus eines Datenbank-Hochverfügbarkeits-Clusters 97
- Überprüfen des Replizierungsstatus eines Knotens in einem Datenbank-Hochverfügbarkeits-Cluster 98

- Überprüfen des Status eines Datenbank-Hochverfügbarkeits-Clusters 99
- Erkennen eines früheren primären Knotens, der in einem Hochverfügbarkeits-Cluster wieder online geschaltet wird 100
- Tauschen der Rollen der primären Zelle und einer Standby-Zelle in einem Datenbank-Hochverfügbarkeits-Cluster 103
- Aufheben der Registrierung eines fehlgeschlagenen oder nicht erreichbaren Standby-Knotens in einem Datenbank-Hochverfügbarkeits-Cluster 104
- Aufheben der Registrierung einer fehlgeschlagenen primären Zelle in einem Datenbank-Hochverfügbarkeits-Cluster 105
- Aufheben der Registrierung einer aktiven Standby-Zelle in einem Datenbank-Hochverfügbarkeits-Cluster 105
- 10 Nach der Installation von vCloud Director oder der Bereitstellung der vCloud Director-Appliance 107**
 - Installation von Microsoft Sysprep-Dateien auf den Servern 107
 - Anpassen öffentlicher Endpoints 108
 - Installieren und Konfigurieren einer RabbitMQ AMQP Broker-Instanz 112
 - Installieren und Konfigurieren einer Cassandra-Datenbank zum Speichern von historischen Metrikdaten 113
 - Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank 114
- 11 Upgrade von vCloud Director und Anwenden von Patches auf die vCloud Director-Appliance 117**
 - Durchführen eines koordinierten Upgrades einer vCloud Director-Installation 119
 - Manuelles Upgrade einer vCloud Director-Installation 122
 - Upgrade einer vCloud Director-Zelle 124
 - Aktualisieren der vCloud Director-Datenbank 126
 - Referenz zum Datenbank-Upgrade-Dienstprogramm 128
 - Patchen der vCloud Director-Appliance-Bereitstellung 130
- 12 Migrieren auf die vCloud Director-Appliance 133**
 - Migrieren von vCloud Director mit einer externen Microsoft SQL-Datenbank auf die vCloud Director-Appliance 133
 - Migrieren von vCloud Director mit einer externen PostgreSQL-Datenbank auf eine vCloud Director-Appliance 137
- 13 Nach dem Upgrade oder der Migration von vCloud Director 143**
 - Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist 143
 - Upgrade von vCenter Server-Systemen, ESXi-Hosts und NSX Edges 144
 - Neue Rechte in dieser Version 146
- 14 Fehlerbehebung für die vCloud Director-Appliance 148**
 - Prüfen der Protokolldateien in der vCloud Director-Appliance 148

Die vCloud Director-Zelle kann nach der Bereitstellung der Appliance nicht gestartet werden
149

Neukonfigurieren des vCloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf
der vCloud Director-Appliance fehl 150

Verwenden der Protokolldateien zur Fehlerbehebung bei vCloud Director-Updates und -Patches
150

Suchen nach vCloud Director-Updates schlägt fehl 151

Installieren des neuesten Updates von vCloud Director schlägt fehl 151

15 Deinstallieren der vCloud Director-Software 153

Installations-, Konfigurations- und Upgrade-Handbuch zu vCloud Director

Das *Installations-, Konfigurations- und Upgrade-Handbuch zu vCloud Director* enthält Informationen zur Installation und zum Upgrade der Software VMware vCloud Director[®] for Service Providers 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 vCloud Director* richtet sich an alle Benutzer, die vCloud 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.

Aktuelle Informationen

Dieses *Installations-, Konfigurations- und Upgrade-Handbuch zu vCloud Director* wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für *Installations-, Konfigurations- und Upgrade-Handbuch zu vCloud Director*.

Revision	Beschreibung
11. JUN. 2019	<ul style="list-style-type: none">■ Das Thema Verlängern der vCloud Director-Appliance-Zertifikate wurde hinzugefügt.■ Kapitel Kapitel 9 Verwenden der Replication Manager-Tool-Suite in einer Hochverfügbarkeits-Cluster-Konfiguration wurde hinzugefügt.
10. MAI 2019	<ul style="list-style-type: none">■ Kapitel #unique_5 wurde hinzugefügt.■ Das Thema Verwenden der Protokolldateien zur Fehlerbehebung bei vCloud Director-Updates und -Patches wurde hinzugefügt.■ Das Thema Suchen nach vCloud Director-Updates schlägt fehl wurde hinzugefügt.■ Das Thema Installieren des neuesten Updates von vCloud Director schlägt fehl wurde hinzugefügt.
5. April 2019	<ul style="list-style-type: none">■ Kapitel Kapitel 12 Migrieren auf die vCloud Director-Appliance wurde hinzugefügt.■ Das Thema Wiederherstellen einer vCloud Director-Appliance-Umgebung mit einer HA-Datenbankkonfiguration wurde hinzugefügt.■ Das Thema Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration wurde aktualisiert, um die Grafiken und Schritt 2 in den Workflows zu verbessern.■ Das Thema Prüfen der Protokolldateien in der vCloud Director-Appliance wurde aktualisiert, um Informationen über die Datei hinzuzufügen, die die OVF-Parameter für die Bereitstellung enthält.
28. März 2019	Erstversion.

Übersicht über Installation, Konfiguration und Upgrade von vCloud Director

1

Sie erstellen eine vCloud Director-Servergruppe, indem Sie die vCloud Director-Software auf einem oder mehreren Linux-Servern installieren oder eine oder mehrere Instanzen der vCloud Director-Appliance bereitstellen. Während des Installationsvorgangs führen Sie die Erstkonfiguration von vCloud Director durch. Dies umfasst auch die Einrichtung der Netzwerk- und Datenbankverbindungen.

Die vCloud Director-Software für Linux erfordert eine externe Datenbank, während die vCloud Director-Appliance eine eingebettete PostgreSQL-Datenbank verwendet.

Nachdem Sie die vCloud Director-Servergruppe erstellt haben, integrieren Sie die vCloud Director-Installation in Ihre vSphere-Ressourcen. Für Netzwerkressourcen kann vCloud Director NSX Data Center for vSphere oder NSX-T Data Center oder beides verwenden.

Wenn Sie ein Upgrade einer vorhandenen vCloud Director-Installation durchführen, aktualisieren Sie die vCloud Director-Software und das Datenbankschema und behalten die bestehenden Beziehungen zwischen Servern, der Datenbank und vSphere bei.

Wenn Sie eine vorhandene vCloud Director-Installation unter Linux auf die vCloud Director-Appliance migrieren, aktualisieren Sie die vCloud Director-Software und migrieren die Datenbank in die eingebettete Datenbank in der Appliance.

Dieses Kapitel enthält die folgenden Themen:

- [vCloud Director-Architektur](#)
- [Konfigurationsplanung](#)

vCloud Director-Architektur

Eine vCloud Director-Servergruppe besteht aus einem oder mehreren vCloud Director-Servern, die auf Linux oder Bereitstellungen der vCloud Director-Appliance installiert sind. Jeder Server in der Gruppe führt eine Sammlung von Diensten aus, die vCloud Director-Zelle genannt werden. Alle Zellen nutzen gemeinsam eine einzige vCloud Director-Datenbank und einen

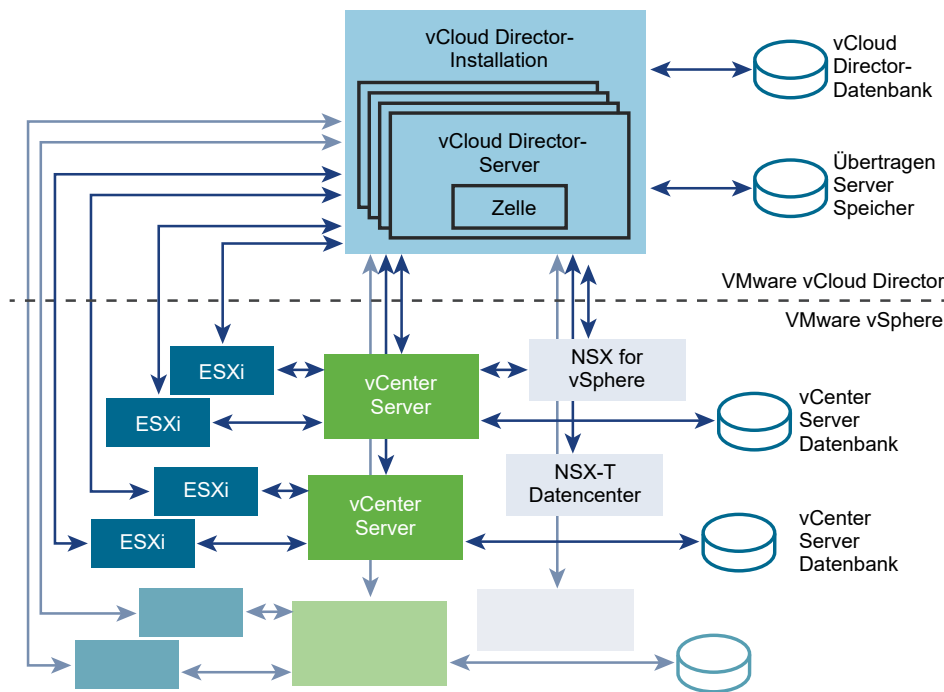
Übertragungsserverspeicher und stellen eine Verbindung zu den vSphere-Ressourcen und den Netzwerkressourcen her.

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

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

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

Abbildung 1-1. vCloud Director-Architekturdiagramm



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

Eine vCloud Director-Servergruppe, die aus Appliance-Bereitstellungen besteht, verwendet die eingebettete Datenbank im ersten Mitglied der Servergruppe. Sie können die Hochverfügbarkeit einer vCloud 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 1-2. vCloud Director-Appliances mit einem Hochverfügbarkeits-Cluster mit eingebetteter Datenbank

Beim vCloud 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 richtet der **Systemadministrator** Verbindungen mit dem vCenter Server-System, den ESXi-Hosts und den NSX Manager-Instanzen ein. Informationen zum Hinzufügen von vSphere-Ressourcen und Netzwerkressourcen finden Sie im *vCloud Director-Administratorhandbuch*.

Konfigurationsplanung

vSphere bietet vCloud Director Speicher-, Rechen- und Netzwerkkapazität. Überlegen Sie vor der Installation, wie viel vSphere- und vCloud 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 vCloud Director-Zelle zu.
- Stellen Sie sicher, dass alle Linux-Zielserver für vCloud Director mindestens die für Arbeitsspeicher und Speicher definierten Mindestanforderungen erfüllen. Eine Aufstellung dieser Anforderungen finden Sie unter *vCloud Director-Versionshinweise*.
- Wenn Sie vCloud Director unter Linux installieren möchten, konfigurieren Sie die vCloud Director-Datenbank wie in [Vorbereiten der vCloud Director-Datenbank](#) beschrieben.

vCloud Director-Hardware- und Softwareanforderungen

2

Jeder Server in einer vCloud 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 vCloud 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 vCloud Director verwendet werden sollen, müssen bestimmte Konfigurationsanforderungen erfüllen.

- vCenter Server-Netzwerke, die als externe vCloud Director-Netzwerke oder Netzwerkpools verwendet werden sollen, müssen für alle Hosts in jedem Cluster verfügbar sein, der für die Verwendung durch vCloud Director vorgesehen ist. Wenn diese Netzwerke für alle Hosts in einem Datacenter verfügbar gemacht werden, wird die Aufgabe, vCloud 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 vCloud 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 vCloud 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*.

vSphere-Lizenzierungsanforderungen

Das vCloud Director Service Provider Bundle enthält die notwendigen vSphere-Lizenzen.

Unterstützte Plattformen, Datenbanken und Browser

In den *Versionshinweisen zu vCloud Director 9.7* finden Sie Informationen zu Serverplattformen, Browsern, LDAP-Servern und Datenbanken, die von dieser Version von vCloud Director unterstützt werden.

Festplattenspeicher, Arbeitsspeicher und CPU-Anforderungen

Physische Anforderungen, wie z. B. Festplattenspeicher, Arbeitsspeicher und CPU für vCloud Director-Zellen, sind in den *Versionshinweisen zu vCloud Director 9.7* aufgelistet.

Freigegebener Speicher

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

Dieses Kapitel enthält die folgenden Themen:

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

Netzwerkkonfigurationsanforderungen für vCloud Director

Der sichere und zuverlässige Betrieb von vCloud 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 vCloud Director beginnen.

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

IP-Adressen

Jeder vCloud Director-Server muss zwei unterschiedliche SSL-Endpoints unterstützen. Ein Endpoint ist für den HTTP-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-Aliasen oder mehreren Netzwerkschnittstellen erstellen. Verwenden Sie nicht den Linux-Befehl `ip addr add` zum Erstellen der zweiten Adresse.

Die vCloud 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 die vCloud Director-Webkonsole anpassen. Für die vCloud 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 vCloud Director-Server, d. h. auch des Datenbankservers, synchronisieren. Die maximal zulässige Abweichung der Uhren von synchronisierten Servern beträgt zwei Sekunden.

Serverzeitzonen

Alle vCloud Director-Server einschließlich des Datenbankservers müssen mit der gleichen Zeitzone konfiguriert werden.

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 vCloud 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 vCloud Director ist eine sichere Netzwerkumgebung. Konfigurieren und testen Sie diese Netzwerkumgebung, bevor Sie mit der Installation von vCloud Director beginnen.

Verbinden Sie alle vCloud Director-Server mit einem gesicherten und überwachten Netzwerk. Für die Netzwerkverbindungen von vCloud Director sind mehrere zusätzliche Anforderungen zu beachten:

- Verbinden Sie vCloud Director nicht direkt mit dem öffentlichen Internet. Schützen Sie die Netzwerkverbindungen von vCloud 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.

Tabelle 2-1. Ports, die eingehende Pakete von vCloud Director-Hosts zulassen müssen

Port	Protokoll	Kommentare
111	TCP, UDP	NFS-Portmapper, vom Übertragungsdienst verwendet
920	TCP, UDP	NFS rpc.statd, vom Übertragungsdienst verwendet
61611	TCP	AMQP
61616	TCP	AMQP

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

Tabelle 2-2. Ports, die ausgehende Pakete von vCloud Director-Hosts zulassen müssen

Port	Protokoll	Kommentare
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	NFS-Portmapper, vom Übertragungsdienst verwendet
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	vCenter-, NSX Manager- und ESXi-Verbindungen, die den Standardport verwenden. Wenn Sie einen anderen Port für diese Dienste ausgewählt haben, deaktivieren Sie die Verbindung mit Port 443, und aktivieren Sie diese für den von Ihnen ausgewählten Port.

Tabelle 2-2. Ports, die ausgehende Pakete von vCloud Director-Hosts zulassen müssen (Fortsetzung)

Port	Protokoll	Kommentare
514	UDP	Optional. Aktiviert die syslog-Verwendung.
902	TCP	vCenter und ESXi-Verbindungen.
903	TCP	vCenter und ESXi-Verbindungen.
920	TCP, UDP	NFS rpc.statd, vom Übertragungsdienst verwendet.
1433	TCP	Microsoft SQL Server-Standarddatenbankport.
5672	TCP, UDP	Optional. AMQP-Meldungen für Aufgabenerweiterungen.
61611	TCP	AMQP
61616	TCP	AMQP

- Leiten Sie den Datenverkehr zwischen vCloud Director-Servern und den folgenden Servern über ein dediziertes privates Netzwerk weiter.
 - vCloud Director-Datenbankserver
 - RabbitMQ
 - Cassandra
- Leiten Sie den Datenverkehr soweit möglich zwischen vSphere-Servern, NSX und vCloud 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 vCloud Director-Übertragungsdiensts finden Sie im VMware-Knowledgebase-Artikel [2086127](#).

Vor der Installation von vCloud Director oder der Bereitstellung der vCloud Director-Appliance

3

Vor der Installation von vCloud Director auf einem Linux-Server oder der Bereitstellung der vCloud Director-Appliance müssen Sie Ihre Umgebung vorbereiten.

Dieses Kapitel enthält die folgenden Themen:

- [Vorbereiten der vCloud Director-Datenbank](#)
- [Vorbereiten des Übertragungsserverspeichers](#)
- [Herunterladen und Installieren des öffentlichen Schlüssels von VMware](#)
- [Installieren und Konfigurieren von NSX Data Center for vSphere für vCloud Director](#)
- [Installieren und Konfigurieren von NSX-T Data Center für vCloud Director](#)

Vorbereiten der vCloud Director-Datenbank

Die vCloud Director-Zellen speichern gemeinsam genutzte Informationen in einer Datenbank. Bevor Sie vCloud Director unter Linux installieren, müssen Sie eine externe vCloud Director-Datenbank installieren und konfigurieren. Die vCloud Director-Appliance verwendet eine eingebettete PostgreSQL-Datenbank.

Informationen zu den unterstützten vCloud Director-Datenbanken finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#).

Unabhängig von der ausgewählten Datenbanksoftware müssen Sie ein separates, dediziertes Datenbankschema zur Verwendung durch vCloud Director erstellen. vCloud Director kann ein Datenbankschema nicht mit einem anderen VMware-Produkt gemeinsam verwenden.

Wichtig vCloud Director unterstützt SSL-Verbindungen nur für eine PostgreSQL-Datenbank. Sie können SSL für die PostgreSQL-Datenbank während einer unbeaufsichtigten Konfiguration von Netzwerk- und Datenbankverbindungen oder nach dem Erstellen der vCloud Director-Servergruppe aktivieren. Weitere Informationen erhalten Sie unter [Referenz für unbeaufsichtigte Konfiguration](#) und [Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank](#).

Konfigurieren einer externen PostgreSQL-Datenbank für vCloud Director unter Linux

PostgreSQL-Datenbanken haben spezifische Konfigurationsanforderungen, wenn sie mit vCloud Director eingesetzt werden. Vor der Installation von vCloud Director unter Linux müssen Sie eine Datenbankinstanz installieren und konfigurieren und das vCloud Director-Datenbankbenutzerkonto erstellen.

Hinweis Nur vCloud Director unter Linux verwendet eine externe Datenbank. Die vCloud Director-Appliance verwendet die eingebettete PostgreSQL-Datenbank.

Voraussetzungen

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 vCloud 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 vCloud Director-Servergruppe können Sie die PostgreSQL-Datenbank so konfigurieren, dass SSL-Verbindungen aus den vCloud Director-Zellen benötigt und bestimmte Datenbankparameter für optimale Leistung angepasst werden. Weitere Informationen finden Sie unter [Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank](#).

Konfigurieren einer externen Microsoft SQL Server-Datenbank für vCloud Director unter Linux

SQL Server-Datenbanken haben spezifische Konfigurationsanforderungen, wenn sie mit vCloud Director eingesetzt werden. Vor der Installation von vCloud Director unter Linux müssen Sie eine Datenbankinstanz installieren und konfigurieren und das vCloud Director-Datenbankbenutzerkonto erstellen.

Die Leistung der vCloud Director-Datenbank ist ein wichtiger Faktor für die Gesamtleistung und Skalierbarkeit von vCloud Director. vCloud Director verwendet zur Speicherung großer Ergebnismengen und zur Sortierung und Verwaltung von gleichzeitig gelesenen und geänderten Daten die SQL Server-Datei tmpdb. Diese Datei kann sich erheblich vergrößern, wenn vCloud Director hohe, gleichzeitig auftretende Lasten zu bewältigen hat. Es empfiehlt sich, die Datei tmpdb auf einem dedizierten Volume mit schnellem Lese- und Schreibzugriff zu erstellen. Weitere Informationen zur Datei tmpdb und zur Leistung von SQL Server erhalten Sie unter <http://msdn.microsoft.com/en-us/library/ms175527.aspx>.

Hinweis Nur vCloud Director unter Linux verwendet eine externe Datenbank. Die vCloud Director-Appliance verwendet die eingebettete PostgreSQL-Datenbank.

Voraussetzungen

- Sie müssen mit den Befehlen, den Skripting-Möglichkeiten und der Bedienung von Microsoft SQL Server vertraut sein.
- Um Microsoft SQL Server zu konfigurieren, melden Sie sich mit Administrator-Anmeldeinformationen beim SQL Server-Hostcomputer an. SQL Server kann für die Ausführung mit der Identität LOCAL_SYSTEM oder irgendeiner zur Ausführung eines Windows-Dienstes berechtigten Identität konfiguriert werden.
- Weitere Informationen zur Verwendung von „AlwaysOn-Verfügbarkeitsgruppen“ von Microsoft SQL Server in Verbindung mit der vCloud Director-Datenbank finden Sie im VMware Knowledgebase-Artikel <https://kb.vmware.com/kb/2148767>.

Verfahren

1 Konfigurieren Sie den Datenbankserver.

Ein mit 16 GB Arbeitsspeicher, 100 GB Speicher und 4 CPUs konfigurierter Datenbankserver sollte für die meisten vCloud Director-Servergruppen geeignet sein.

2 Legen Sie während der Installation von SQL Server den "Gemischtem Modus" für die Authentifizierung fest.

Die Windows-Authentifizierung wird für den Einsatz von SQL Server in Verbindung mit vCloud Director nicht unterstützt.

3 Erstellen Sie die Datenbankinstanz.

Das folgende Skript erstellt die Datenbank und die Protokolldateien und legt die richtige Sortierreihenfolge fest.

```
USE [master]
GO
CREATE DATABASE [vcloud] ON PRIMARY
(NAME = N'vcloud', FILENAME = N'C:\vcloud.mdf', SIZE = 100MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcloud_log', FILENAME = N'C:\vcloud.ldf', SIZE = 1MB, FILEGROWTH = 10%)
COLLATE Latin1_General_CS_AS
GO
```

Die für SIZE gezeigten Werte sind nur Beispiele. Möglicherweise benötigen Sie größere Werte.

4 Legen Sie die Transaktionsisolationsstufe fest.

Das folgende Skript legt die Isolationsstufe für die Datenbank auf READ_COMMITTED_SNAPSHOT fest.

```
USE [vcloud]
GO
ALTER DATABASE [vcloud] SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
ALTER DATABASE [vcloud] SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE [vcloud] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [vcloud] SET MULTI_USER;
GO
```

Weitere Informationen zur Transaktionsisolierung erhalten Sie unter <http://msdn.microsoft.com/en-us/library/ms173763.aspx>.

5 Erstellen Sie das vCloud Director-Datenbankbenutzerkonto.

Das folgende Skript erstellt einen Datenbankbenutzer mit dem Namen vcloud und dem Kennwort vcloudpass.

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE =[vcloud],
```

```

DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vccloud] for LOGIN [vccloud]
GO

```

- 6** Weisen Sie dem vCloud Director-Datenbankbenutzerkonto die erforderlichen Berechtigungen zu.

Das folgende Skript weist dem in [Schritt 5](#) erstellten Datenbankbenutzer die Rolle db_owner zu.

```

USE [vccloud]
GO
sp_addrolemember [db_owner], [vccloud]
GO

```

Vorbereiten des Übertragungsserverspeichers

Um temporären Speicher für Uploads, Downloads und Katalogelemente, die extern veröffentlicht oder abonniert werden, bereitzustellen, müssen Sie veranlassen, dass alle Server in einer vCloud Director-Servergruppe auf ein NFS- oder ein anderes gemeinsam genutztes Speichervolume zugreifen können.

Wichtig Die vCloud Director-Appliance unterstützt nur den NFS-Typ des freigegebenen Speichers. Der Appliance-Bereitstellungsvorgang umfasst das Mounten des gemeinsam genutzten NFS-Übertragungsserverspeichers.

Wenn NFS für den Übertragungsserverspeicher verwendet wird, müssen Sie jede vCloud Director-Zelle in der vCloud Director-Servergruppe so konfigurieren, dass der NFS-basierte Übertragungsserverspeicher gemountet und verwendet wird. Sie benötigen bestimmte Benutzer- und Gruppenberechtigungen, um jede Zelle so zu konfigurieren, dass sie den NFS-basierten Speicherort mountet und als Übertragungsserverspeicher verwendet.

Jedes Mitglied der Servergruppe mountet dieses Volume am selben Mount-Punkt, in der Regel `/opt/vmware/vcloud-director/data/transfer`. Der Speicher auf diesem Volume wird auf zwei Arten genutzt:

- 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.

Verwendung der Dateisystemberechtigungen auf dem Übertragungsserverspeicher durch vCloud Director

Für alle vCloud Director-Zellen in der vCloud Director-Servergruppe:

- Bei Cloud-Standardvorgängen, wie z. B. dem Hochladen von Elementen in den Katalog, schreibt der Daemon der vCloud Director-Zelle mithilfe des **vCloud**-Benutzers in der **vCloud**-Gruppe Dateien in den Übertragungsserverspeicher und liest Dateien aus diesem Speicher. Der **vcloud**-Benutzer schreibt die Dateien mit `umask 0077`. Wenn das vCloud Director-Installationsprogramm ausgeführt und die vCloud Director-Software auf einem Servergruppenmitglied installiert wird, werden auch der **vCloud**-Benutzer und die **vCloud**-Gruppe erstellt.
- Im Datenerfassungsskript des vCloud Director-Protokoll mit dem Namen `vmware-vcd-support` können die Protokolle aller vCloud Director-Zellen in einem Vorgang erfasst und in einer einzelnen Datei vom Typ `tar.gz` gebündelt werden. Bei Ausführung des Skripts wird die resultierende Datei vom Typ `tar.gz` mithilfe der Benutzer-ID des Benutzers, der das Skript aufgerufen hat, in ein Verzeichnis am Speicherort des Übertragungsservers geschrieben. Standardmäßig verfügt nur der **root**-Benutzer über die Berechtigung zum Ausführen des Skripts.
- Der **root**-Benutzer der Zelle führt das Skript aus, das die Datei `tar.gz` in das Verzeichnis `vmware-vcd-support` am Speicherort des Übertragungsservers schreibt. Wenn Sie die Optionen für Mehrfachzellen verwenden möchten, um die Protokolle aus allen Zellen gleichzeitig zu erfassen, muss der **root**-Benutzer über eine Leseberechtigung zum Abrufen des Diagnoseprotokollpakets vom Typ `tar.gz` verfügen.

Anforderungen an die Konfiguration des NFS-Servers

Es gibt bestimmte Anforderungen an die Konfiguration des NFS-Servers, damit vCloud 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 vCloud 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 vCloud 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.

Wenn der NFS-Server beispielsweise die IP-Adresse 192.168.120.7 hat und ein Verzeichnis mit der Bezeichnung „vCDspace“ als Übertragungsspeicher für die vCloud 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 zwei Zellen mit der Bezeichnung `vcd-cell1-IP` und `vcd-cell2-IP` verwendet. Sie müssen der Datei `/etc/exports` eine Zeile hinzufügen.

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

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.

Jeder Server in der vCloud Director-Servergruppe muss die NFS-Freigabe durch Überprüfung der Exportliste für den NFS-Export mounten können. Sie exportieren den Mount, indem Sie `exportfs -a` für den erneuten Export aller NFS-Freigaben ausführen. Die NFS-Daemons `rpcinfo -p localhost` oder `service nfs status` müssen auf dem Server ausgeführt werden.

Überlegungen beim Planen des Upgrades Ihrer vCloud Director-Installation auf eine höhere Version

Während eines Upgrades einer vCloud Director-Servergruppe führen Sie die Installationsdatei für die aktualisierte Version aus, um alle Mitglieder der vCloud 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 vCloud 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 vCloud 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 vCloud Director

Wenn Sie Ihre vCloud 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 vCloud Director-Installation enthalten sein soll.

NSX Manager ist im Download für NSX Data Center for vSphere enthalten. Die neuesten Informationen zur Kompatibilität zwischen vCloud 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 vCloud Director](#).

Wichtig Dieses Verfahren ist nur anzuwenden, wenn Sie vCloud Director neu installieren. Wenn Sie eine vorhandene Installation von vCloud Director aktualisieren, lesen Sie die Informationen unter [Kapitel 11 Upgrade von vCloud Director und Anwenden von Patches auf die vCloud Director-Appliance](#).

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 vCloud Director hinzufügen möchten, Ihrer geplanten vCloud Director-Installation zu.
- 4 Konfigurieren Sie die VXLAN-Unterstützung in den zugehörigen NSX Manager-Instanzen.
vCloud 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 vCloud Director

Wenn in Ihrer vCloud Director-Installation Netzwerkressourcen von NSX-T Data Center verwendet werden sollen, müssen Sie NSX-T Data Center mit mindestens einer NSX-T Manager-Instanz installieren und konfigurieren.

NSX-T Manager ist im Download für NSX-T Data Center enthalten. Die neuesten Informationen zur Kompatibilität zwischen vCloud 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 Netzerkanforderungen finden Sie unter [Netzwerkkonfigurationsanforderungen für vCloud Director](#).

Wichtig Dieses Verfahren ist nur anzuwenden, wenn Sie vCloud Director neu installieren. Wenn Sie eine vorhandene Installation von vCloud Director aktualisieren, lesen Sie die Informationen unter [Kapitel 11 Upgrade von vCloud Director und Anwenden von Patches auf die vCloud Director-Appliance](#).

Voraussetzungen

Sie müssen mit NSX-T Data Center vertraut sein.

Verfahren

- 1** Installieren Sie die virtuelle Appliance NSX-T Manager.
Weitere Informationen dazu finden Sie im *Installationshandbuch für NSX-T*.
- 2** Bereiten Sie die ESXi-Hosts vor, die Sie mit NSX-T Data Center betreiben möchten.
Weitere Informationen dazu finden Sie im *Installationshandbuch für NSX-T*.
- 3** Erstellen Sie Transportknoten und Transportzonen für Ihre Cloud-Anforderungen.
Weitere Informationen dazu finden Sie im *Installationshandbuch für NSX-T*.
- 4** Konfigurieren Sie Edge-Knoten und Cluster.
Weitere Informationen dazu finden Sie im *Installationshandbuch für NSX-T*.
- 5** Konfigurieren Sie Ebene-0- und Ebene-1-Router.
Weitere Informationen dazu finden Sie im *Administratorhandbuch für NSX-T*.
- 6** Konfigurieren Sie mindestens einen VLAN- oder logischen Overlay-Switch, den Sie in Ihre vCloud Director-Installation importieren möchten.
Weitere Informationen dazu finden Sie im *Administratorhandbuch für NSX-T*.

Nächste Schritte

Nachdem Sie vCloud Director installiert haben, können Sie die NSX-T Manager-Instanz bei Ihrer Cloud registrieren. Informationen über die Registrierung einer NSX-T Manager-Instanz finden Sie im *vCloud API-Programmierhandbuch für Dienstleister*.

Erstellen und Verwalten von SSL-Zertifikaten für vCloud Director unter Linux

4

vCloud Director verwendet SSL, um die Kommunikation zwischen Clients und Servern zu sichern. Jeder vCloud 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.

Dieses Kapitel enthält die folgenden Themen:

- [Vor dem Erstellen von SSL-Zertifikaten für vCloud Director unter Linux](#)
- [Erstellen von selbstsignierten SSL-Zertifikaten für vCloud Director unter Linux](#)
- [Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores für vCloud Director unter Linux](#)
- [Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores mit importierten privaten Schlüsseln für vCloud Director unter Linux](#)

Vor dem Erstellen von SSL-Zertifikaten für vCloud Director unter Linux

Wenn Sie vCloud 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 vCloud Director unter Linux erstellen. Die vCloud Director-Appliance erstellt während des ersten Startvorgangs selbstsignierte SSL-Zertifikate.

Verfahren

- 1 Melden Sie sich beim vCloud 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 vCloud Director unter Linux](#).
- Informationen zum Erstellen von selbstsignierten SSL-Zertifikaten finden Sie unter [Erstellen von selbstsignierten SSL-Zertifikaten für vCloud 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 vCloud Director unter Linux](#).

Erstellen von selbstsignierten SSL-Zertifikaten für vCloud Director unter Linux

Selbstsignierte Zertifikate bieten die Möglichkeit, SSL bequem für vCloud Director in Umgebungen zu konfigurieren, in denen minimale Bedenken in Bezug auf Vertraulichkeit herrschen.

Jeder vCloud 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 vCloud 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 vCloud 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 vCloud 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 vCloud Director-Zelle ausführen. Weitere Informationen finden Sie unter [Konfigurieren der Netzwerk- und Datenbankverbindungen](#).

Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores für vCloud 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 vCloud Director-Server benötigt zwei SSL-Zertifikate, um die Kommunikation zwischen Clients und Servern zu sichern. Jeder vCloud 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 vCloud 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 vCloud 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 vCloud 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 vCloud 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 Details zu den verfügbaren Optionen für den Befehl `certificates` finden Sie unter [Ersetzen der Zertifikate für die HTTP- und Konsolen-Proxy-Endpoints](#).

Verfahren

- 1 Melden Sie sich direkt oder mithilfe eines SSH-Clients beim Betriebssystem der vCloud 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 vCloud 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 JCEKS -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 JCEKS -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 JCEKS-Keystore.

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

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

- c Importieren Sie das Zertifikat des HTTPS-Diensts.

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

- d Importieren Sie das Konsolen-Proxy-Dienstzertifikat.

```
keytool -import -storetype JCEKS -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 JCEKS-Keystore importiert wurden, führen Sie den Befehl zum Auflisten der Inhalte der Keystore-Datei aus.

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

- 7 Wiederholen Sie diesen Vorgang auf allen vCloud Director-Servern in der Servergruppe.

Nächste Schritte

- Wenn Sie Ihre vCloud Director-Instanz noch nicht konfiguriert haben, führen Sie das Skript `configure` aus, um den Zertifikat-Keystore in vCloud 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 Konfigurationsskript ausführen.

- Wenn Sie Ihre vCloud Director-Instanz bereits installiert und konfiguriert haben, verwenden Sie den Befehl `certificates` des Zellenverwaltungstools zum Importieren des Zertifikat-Kestores. Weitere Informationen finden Sie unter [Ersetzen der Zertifikate für die HTTP- und Konsolen-Proxy-Endpoints](#).

Erstellen eines von einer Zertifizierungsstelle signierten SSL-Zertifikat-Keystores mit importierten privaten Schlüsseln für vCloud Director unter Linux

Wenn Sie über einen eigenen privaten Schlüssel und von einer Zertifizierungsstelle signierte Zertifikatsdateien verfügen, müssen Sie vor dem Importieren der Keystores in die vCloud 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 vCloud 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 vCloud 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 vCloud 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 Details zu den verfügbaren Optionen für den Befehl `certificates` finden Sie unter [Ersetzen der Zertifikate für die HTTP- und Konsolen-Proxy-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.pfx -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.pfx -chain
```

- 3 Verwenden Sie keytool, um die PKCS12-Keystores in den JCEKS-Keystore 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 JCEKS -srckeystore http.pfx -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 JCEKS -srckeystore consoleproxy.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

- 4 Um zu überprüfen, ob die Zertifikate in den JCEKS-Keystore importiert wurden, führen Sie den Befehl zum Auflisten der Inhalte der Keystore-Datei aus.

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

- 5 Wiederholen Sie diese Schritte für alle vCloud Director-Zellen in Ihrer Umgebung.

Nächste Schritte

- Wenn Sie Ihre vCloud Director-Instanz noch nicht konfiguriert haben, führen Sie das Skript `configure` aus, um den Zertifikat-Keystore in vCloud 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 vCloud Director-Instanz bereits installiert und konfiguriert haben, verwenden Sie den Befehl `certificates` des Zellenverwaltungstools zum Importieren des Zertifikat-Keystores. Weitere Informationen finden Sie unter [Ersetzen der Zertifikate für die HTTP- und Konsolen-Proxy-Endpoints](#).

Installieren von vCloud Director unter Linux

5

Sie können eine vCloud Director-Servergruppe erstellen, indem Sie die vCloud 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 vCloud Director-Installation finden Sie unter [Kapitel 11 Upgrade von vCloud Director und Anwenden von Patches auf die vCloud Director-Appliance](#).

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

Voraussetzungen

- Vergewissern Sie sich, dass die Zielservers Ihrer Servergruppe den Anforderungen unter [Kapitel 2 vCloud Director-Hardware- und Softwareanforderungen](#) entsprechen.
- Vergewissern Sie sich, dass Sie für jeden Endpoint der Zielservers 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 vCloud Director unter Linux](#).
- Vergewissern Sie sich, dass Sie ein NFS- oder anderes freigegebenes Speichervolumen vorbereitet haben, auf das alle Zielservers für Ihre vCloud Director-Servergruppe zugreifen können. Weitere Informationen finden Sie unter [Vorbereiten des Übertragungsserverspeichers](#).
- Überprüfen Sie, ob eine vCloud Director-Datenbank erstellt wird und ob alle Server in der Gruppe auf diese zugreifen können. Weitere Informationen finden Sie unter [Vorbereiten der vCloud Director-Datenbank](#). Überprüfen Sie, ob der Datenbankdienst beim Neustart des Datenbankservers gestartet wird.

- Überprüfen Sie, ob alle vCloud Director-Server, der Datenbankserver, alle vCenter Server-Systeme und die zugeordneten NSX Manager-Instanzen jeden Hostnamen in der Umgebung wie in [Netzwerkkonfigurationsanforderungen für vCloud Director](#) beschrieben auflösen können.
- Überprüfen Sie, ob alle vCloud Director-Server und der Datenbankserver mit einem Netzwerkzeitserver mit den in [Netzwerkkonfigurationsanforderungen für vCloud Director](#) angegebenen Toleranzen synchronisiert sind.
- Wenn Sie Benutzer oder Gruppen von einem LDAP-Dienst importieren möchten, überprüfen Sie, ob alle vCloud Director-Server auf diesen Dienst zugreifen können.
- Öffnen Sie die Firewall-Ports gemäß der Beschreibung in [Empfehlungen für die Netzwerksicherheit](#). Port 443 muss zwischen vCloud Director und den vCenter Server-Systemen offen sein.

Verfahren

1 Installieren von vCloud Director auf dem ersten Mitglied einer Servergruppe

Nachdem Sie Ihre Umgebung vorbereitet und die Voraussetzungen überprüft haben, können Sie mit dem Erstellen der vCloud Director-Servergruppe beginnen, indem Sie das vCloud Director-Installationsprogramm auf dem ersten Linux-Zielsystem ausführen.

2 Konfigurieren der Netzwerk- und Datenbankverbindungen

Nach der Installation von vCloud 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.

3 Installieren von vCloud Director auf einem weiteren Mitglied einer Servergruppe

Sie können jederzeit Server zu einer vCloud 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.

4 Einrichten von vCloud Director

Nachdem Sie alle Server in der vCloud Director-Servergruppe installiert und konfiguriert haben, müssen Sie Ihre vCloud Director-Installation einrichten. Das vCloud Director-Setup initialisiert die vCloud Director-Datenbank mit einem Lizenzschlüssel, dem Systemadministratorkonto und zugehörigen Informationen.

Nächste Schritte

Sie können mit dem Hinzufügen von Ressourcen zu Ihrer vCloud Director-Installation beginnen. Informationen zu den ersten Schritten mit vCloud Director finden Sie unter *vCloud Director-Administratorhandbuch*.

Installieren von vCloud Director auf dem ersten Mitglied einer Servergruppe

Nachdem Sie Ihre Umgebung vorbereitet und die Voraussetzungen überprüft haben, können Sie mit dem Erstellen der vCloud Director-Servergruppe beginnen, indem Sie das vCloud Director-Installationsprogramm auf dem ersten Linux-Zielserver ausführen.

vCloud 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 vCloud Director installiert oder aktualisiert.

Das vCloud Director-Installationsprogramm überprüft, ob der Zielserver alle Voraussetzungen für die Plattform erfüllt, und installiert dann die vCloud Director-Software auf diesem Server.

Voraussetzungen

- Überprüfen Sie, ob Sie die für den Zielserver benötigten Superuser-Anmeldeinformationen besitzen.
- Laden Sie den öffentlichen Schlüssel von VMware auf den Zielserver 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 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@cell1 /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 setzt die Ausführungsberechtigung voraus. 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 vCloud Director-Installationsdatei ist.

```
[root@cell1 /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@cell1 /tmp]# ./Installationsdatei
```

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 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 vCloud Director-RPM-Paket.
- e Es installiert die Software.

Nach Abschluss der Installation werden Sie vom Installationsprogramm aufgefordert, das Konfigurationsskript auszuführen, das die Netzwerk- und Datenbankverbindungen konfiguriert.

6 Wählen Sie aus, ob das Konfigurationsskript ausgeführt werden soll.

- a Um das Konfigurationsskript im interaktiven Modus auszuführen, geben Sie **y** ein und drücken Sie die Eingabetaste.
- b Um das Konfigurationsskript zu einem späteren Zeitpunkt im interaktiven oder im unbeaufsichtigten Modus auszuführen, geben Sie **n** ein und drücken Sie die Eingabetaste.

Konfigurieren der Netzwerk- und Datenbankverbindungen

Nach der Installation von vCloud 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 vCloud Director-Servergruppe verwenden die Datenbankverbindung und andere Konfigurationsdetails gemeinsam. Wenn Sie das Konfigurationsskript auf dem ersten Mitglied der vCloud 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 HTTP-Dienst und den Konsolen-Proxy-Dienst verwenden möchten, müssen Sie das Konfigurationsskript in einem 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 im *vCloud Director-Administratorhandbuch*.

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 VCLLOUD_HOME auf den vollständigen Pfadnamen des Verzeichnisses festgelegt ist, in dem vCloud Director installiert ist. Dieser Wert lautet meistens `/opt/vmware/vcloud-director`.

Verfahren

- 1 Melden Sie sich beim vCloud 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/configureOptionen -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 vCloud Director einrichten** nach dem Start des vCloud Director-Diensts verbinden können.
 - c Es bietet das Starten der vCloud Director-Zelle an.
- 3** (Optional) Notieren Sie sich die URL des Assistenten **VMware vCloud Director einrichten** und geben Sie **y** ein, um den vCloud 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 5-1. Erforderliche Informationen während einer interaktiven Netzwerk- und Datenbankkonfiguration

Erforderliche Informationen	Beschreibung
IP-Adresse für den HTTP-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 HTTP-Dienst und den Konsolen-Proxy-Dienst verwenden möchten, müssen Sie das Konfigurationsskript in einem unbeaufsichtigten Modus ausführen.
Vollständiger Pfad der Java-Keystore-Datei	Beispiel: /opt/keystore/certificates.ks.
Kennwort für den Keystore	Weitere Informationen finden Sie unter Vor dem Erstellen von SSL-Zertifikaten für vCloud Director unter Linux .
Kennwort für den privaten Schlüssel für das HTTP-SSL-Zertifikat	Weitere Informationen finden Sie unter Vor dem Erstellen von SSL-Zertifikaten für vCloud 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 vCloud Director unter Linux .
Remote-Überwachungsprotokollierung für einen Syslog-Host aktivieren	Dienste in den einzelnen vCloud Director-Zellen protokollieren Überwachungsmeldungen an die vCloud Director-Datenbank, in der diese 90 Tage aufbewahrt werden. Um Überwachungsmeldungen für einen längeren Zeitraum zu speichern, können Sie die vCloud Director-Dienste so konfigurieren, dass diese die Überwachungsmeldungen nicht nur an die vCloud Director-Datenbank, sondern zusätzlich auch an das syslog-Dienstprogramm senden. <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.
Datenbanktyp	PostgreSQL oder Microsoft SQL Server Die Standardeinstellung ist PostgreSQL.
Hostname oder die IP-Adresse des Datenbankservers	Der Server, auf dem die Datenbank ausgeführt wird.
Datenbankport	Für PostgreSQL lautet der Standardport 5432. Für Microsoft SQL Server lautet der Standardport 1433.
Datenbankname	Standardmäßig „vcloud“.
Wenn der Datenbanktyp Microsoft SQL Server ist, die Datenbankinstanz	Standardmäßig die Standardinstanz.

Tabelle 5-1. Erforderliche Informationen während einer interaktiven Netzwerk- und Datenbankkonfiguration (Fortsetzung)

Erforderliche Informationen	Beschreibung
Name des Datenbankbenutzers	Weitere Informationen finden Sie unter Vorbereiten der vCloud Director-Datenbank .
Datenbankkennwort	Weitere Informationen finden Sie unter Vorbereiten der vCloud Director-Datenbank .
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. Informationen dazu finden Sie in der „Zellenverwaltungstool-Referenz“ im <i>vCloud Director-Administratorhandbuch</i>.</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 5-2. 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 vCloud 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 vCloud Director.

Tabelle 5-2. Optionen und Argumente des Konfigurationsdienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
--database-ssl	true oder false	Wenn Sie eine PostgreSQL-Datenbank verwenden, können Sie die Datenbank so konfigurieren, dass eine offiziell signierte SSL-Verbindung von vCloud Director benötigt wird. Wird ignoriert, wenn --database-type nicht postgres ist. 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 .
--database-host (-dbhost)	IP-Adresse oder vollqualifizierter Domänenname des vCloud Director-Datenbank-Hosts	Weitere Informationen finden Sie unter Vorbereiten der vCloud Director-Datenbank .
--database-domain (-dbdomain)	SQL Server-Datenbank-Benutzerdomäne	Optional, wenn es sich bei --database-type um sqlserver handelt.
--database-instance (-dbinstance)	SQL Server-Datenbankinstanz	Verwendet, wenn es sich bei --database-type um sqlserver handelt
--database-name (-dbname)	Der Datenbankdienstname	Weitere Informationen finden Sie unter Vorbereiten der vCloud Director-Datenbank .
--database-password (-dbpassword)	Kennwort für den Datenbankbenutzer. Der Wert kann null sein.	Weitere Informationen finden Sie unter Vorbereiten der vCloud Director-Datenbank .
--database-port (-dbport)	Portnummer, die vom Datenbankdienst auf dem Datenbank-Host verwendet wird	Weitere Informationen finden Sie unter Vorbereiten der vCloud Director-Datenbank .
--database-type (-dbtype)	Der Datenbanktyp. Möglichkeiten: ■ postgres ■ sqlserver	Weitere Informationen finden Sie unter Vorbereiten der vCloud Director-Datenbank .
--database-user (-dbuser)	Benutzername des Datenbankbenutzers.	Weitere Informationen finden Sie unter Vorbereiten der vCloud Director-Datenbank .

Tabelle 5-2. Optionen und Argumente des Konfigurationsdienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
--enable-ceip	true oder false	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. Informationen dazu finden Sie in der „Zellenverwaltungstool-Referenz“ im <i>vCloud Director-Administratorhandbuch</i> .
--uuid (-g)	Keine	Generiert einen neuen eindeutigen Bezeichner für die Zelle
--primary-ip (-ip)	IPv4-Adresse mit optionaler Portnummer	Das System verwendet diese Adresse für den Webschnittstellendienst von vCloud Director. Beispiel: <i>10.17.118.159</i> .
--primary-port-http	Ganzzahl im Bereich 0 bis 65535	Portnummer zur Verwendung für HTTP-Verbindungen (unsicher) zum Webschnittstellendienst von vCloud Director
--primary-port-https	Ganzzahl im Bereich 0 bis 65535	Portnummer zur Verwendung für HTTPS-Verbindungen (sicher) zum Webschnittstellendienst von vCloud Director
--keystore (-k)	Pfad zum Java-Keystore, der Ihre SSL-Zertifikate und privaten Schlüssel enthält	Muss ein vollständiger Pfadname sein. Beispiel: <i>/opt/keystore/certificates.ks</i> .

Tabelle 5-2. Optionen und Argumente des Konfigurationsdienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
--syslog-host (-loghost)	IP-Adresse oder vollqualifizierter Domänenname des Syslog-Server-Hosts	Dienste in den einzelnen vCloud Director-Zellen protokollieren Überwachungsmeldungen an die vCloud Director-Datenbank, in der diese 90 Tage aufbewahrt werden. Um Überwachungsmeldungen für einen längeren Zeitraum zu speichern, können Sie die vCloud Director-Dienste so konfigurieren, dass diese die Überwachungsmeldungen nicht nur an die vCloud Director-Datenbank, sondern zusätzlich auch an das syslog-Dienstprogramm senden.
--syslog-port (-logport)	Ganzzahl im Bereich 0 bis 65535	Der Port, an dem der syslog-Vorgang den angegebenen Server überwacht. Ist standardmäßig 514, wenn nicht angegeben.
--response-file (-r)	Pfad zur Antwortdatei	Muss ein vollständiger Pfadname sein. Ist standardmäßig /opt/vmware/vcloud-director/etc/responses.properties, 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.
--unattended-installation (-unattended)	Keine	Gibt eine unbeaufsichtigte Installation an
--keystore-password (-w)	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 vCloud Director-Servers mit zwei verschiedenen IP-Adressen für den HTTP-Dienst und den Konsolen-Proxy-Dienst aus.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 -cons 10.17.118.158 \
-dbtype sqlserver -dbhost 10.150.10.78 -dbname mssql-db -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 vCloud Director-Servers mit einer einzelnen IP-Adresse mit zwei verschiedenen Ports für den HTTP-Dienst und den Konsolen-Proxy-Dienst aus.

```
[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 sqlserver -dbhost 10.150.10.78 -dbname mssql-db \
-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 vCloud 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 vCloud 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@cell1 /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@cell1 /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 vCloud Director auf einem weiteren Mitglied einer Servergruppe

Sie können jederzeit Server zu einer vCloud 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 vCloud Director-Installationen unter Linux und vCloud 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 vCloud Director-Servergruppe unter `/opt/vmware/vcloud-director/data/transfer` gemountet haben.

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 Stellen Sie sicher, dass die Installationsdatei ausführbar ist.

Die Installationsdatei setzt die Ausführungsberechtigung voraus. 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 vCloud Director-Installationsdatei ist.

```
[root@cell1 /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@cell1 /tmp]# ./Installationsdatei
```

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 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 vCloud Director-RPM-Paket.
- e Es installiert die Software.

Nach Abschluss der Installation werden Sie vom Installationsprogramm aufgefordert, das Konfigurationsskript auszuführen, das die Netzwerk- und Datenbankverbindungen konfiguriert.

- 5 Geben Sie **n** ein und drücken Sie die Eingabetaste, um die Ausführung des Konfigurationsskripts abzulehnen.

Sie führen das Konfigurationsskript später aus, indem Sie die Antwortdatei als Eingabe bereitstellen.

- 6** Mounten Sie den gemeinsam genutzten Übertragungsspeicher unter `/opt/vmware/vcloud-director/data/transfer`.

Alle vCloud 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 vCloud Director-Zelle zu starten.

- 9** (Optional) Geben Sie `y` ein, um den vCloud 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 vCloud Director-Dienste auf allen Servern ausgeführt werden, müssen Sie die vCloud Director-Datenbank mit einem Lizenzschlüssel, einem Systemadministratorkonto und zugehörigen Informationen initialisieren. Sie können die Datenbank auf folgende Weisen initialisieren:

- Öffnen Sie in einem Webbrowser den Setup-Assistenten unter der URL, die angezeigt wird, wenn das Konfigurationsskript beendet wird. Weitere Informationen erhalten Sie unter [Einrichten von vCloud Director](#).
- Verwenden Sie das Zellenverwaltungstool mit dem Unterbefehl `system-setup`. Informationen zur Verwendung des Zellenverwaltungstools finden Sie unter *vCloud Director-Administratorhandbuch*.

Einrichten von vCloud Director

Nachdem Sie alle Server in der vCloud Director-Servergruppe installiert und konfiguriert haben, müssen Sie Ihre vCloud Director-Installation einrichten. Das vCloud Director-Setup initialisiert die vCloud Director-Datenbank mit einem Lizenzschlüssel, dem Systemadministratorkonto und zugehörigen Informationen.

Bevor Sie die Webkonsole von vCloud Director starten können, führen Sie den Assistenten **VMware vCloud Director einrichten** aus, der die Informationen sammelt, die für den Start der Webkonsole benötigt werden.

Als Alternative zur Verwendung des Assistenten **VMware vCloud Director einrichten** können Sie zum Konfigurieren der vCloud Director-Installation den Unterbefehl `system-setup` des Zellenverwaltungstools verwenden. Informationen zum Zellenverwaltungstool finden Sie im *vCloud Director-Administratorhandbuch*.

Voraussetzungen

- Vergewissern Sie sich, dass die vCloud Director-Dienste auf allen Servern gestartet wurden.
- Erhalten Sie eine vCloud Director-Produktseriennummer vom VMware-Lizenzportal.

Verfahren

Verfahren

- 1 Öffnen Sie einen Webbrowser und rufen Sie die URL auf, die im Konfigurationsskript angezeigt wurde.

Um die URL des Assistenten **VMware vCloud Director einrichten** zu ermitteln, können Sie auch nach dem vollqualifizierten Domännennamen suchen, der der IP-Adresse zugeordnet ist, die Sie bei der Installation des ersten Servers für den HTTP-Dienst angegeben haben. Um eine Verbindung mit dem Assistenten herzustellen, navigieren Sie zu `https://fully-qualified-domain-name`. Beispiel: `https://mycloud.example.com`.

Hinweis Das Starten des Assistenten kann einige Minuten dauern.

- 2 Überprüfen Sie die Begrüßungsseite und klicken Sie auf **Weiter**.
- 3 Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
Wenn Sie die Lizenzvereinbarung ablehnen, können Sie nicht mit der vCloud Director-Konfiguration fortfahren.
- 4 Geben Sie die Seriennummer Ihres vCloud Director-Produkts ein und klicken Sie auf **Weiter**.
- 5 Geben Sie einen Benutzernamen, ein Kennwort und die Kontaktinformationen für den vCloud Director-Systemadministrator ein und klicken Sie auf **Weiter**.

Der vCloud Director-Systemadministrator hat in der gesamten Cloud Superuser-Rechte. Dieser Systemadministrator kann zusätzliche Systemadministratorkonten einrichten.

- 6 Konfigurieren Sie die Systemeinstellungen, mit denen gesteuert wird, wie vCloud Director mit vSphere und NSX Manager interagiert, und klicken Sie auf **Weiter**.
 - a Geben Sie in das Textfeld **Systemname** einen Namen für den vCenter Server-Ordner ein, der für diese vCloud Director-Installation verwendet werden soll.
 - b Legen Sie im Textfeld **Installations-ID** die ID für diese vCloud Director-Installation fest, die verwendet werden soll, wenn Sie MAC-Adressen für virtuelle Netzwerkkarten erstellen.

Wenn Sie ausgeweitete Netzwerke für vCloud Director-Installationen in Multisite-Bereitstellungen erstellen möchten, richten Sie eine eindeutige Installations-ID für jede vCloud Director-Installation ein.
- 7 Überprüfen Sie auf der Seite „Bereit für Anmeldung“ die Einstellungen und klicken Sie auf **Beenden**.

Ergebnisse

Wenn der Konfigurationsvorgang abgeschlossen ist, werden Sie zur Anmeldeseite der vCloud Director-Webkonsole weitergeleitet.

Nächste Schritte

Melden Sie sich bei der vCloud Director-Webkonsole mit dem Benutzernamen und dem Kennwort des Systemadministrators an und beginnen Sie mit der Bereitstellung Ihrer Cloud. Informationen zum Hinzufügen von Ressourcen zu vCloud Director finden Sie im *vCloud Director-Administratorhandbuch*.

Bereitstellen der vCloud Director-Appliance

6

Sie können eine vCloud Director-Servergruppe erstellen, indem Sie eine oder mehrere Instanzen der vCloud Director-Appliance bereitstellen. Sie stellen die vCloud Director-Appliance mithilfe des vSphere Client (HTML5), des vSphere Web Client (Flex) oder des VMware OVF Tool bereit.

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

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

Die Appliance wird mit einem Namen im Format VMware vCloud Director-*v.v.v.v-nnnnnn_OVF10.ova*, wobei *v.v.v.v* die Produktversion und *nnnnnn* die Build-Nummer darstellt. Beispiel: VMware vCloud Director-9.7.0.0-9229800_OVA10.ova.

Das vCloud Director-Appliance-Paket enthält die folgende Software:

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

Die Größen „Primär-klein“ und „Standby-klein“ der vCloud 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 vCloud 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 vCloud 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 vCloud Director-Appliance als primäre Zelle und zwei Instanzen als Standby-Zellen bereitstellen. Sie können zusätzliche Instanzen der vCloud Director-Appliance in der Servergruppe als vCD-Anwendungszellen bereitstellen, die nur die vCloud 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 vCloud 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 vCloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats](#).

Hinweis Die vCloud Director-Appliance unterstützt keine externen Datenbanken.

Appliance-Netzwerkconfiguration

Ab Version 9.7 wird die vCloud 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.

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.

Die vCloud 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.

Dieses Kapitel enthält die folgenden Themen:

- [Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration](#)

- [Voraussetzungen für die Bereitstellung der vCloud Director-Appliance](#)
- [Bereitstellen der vCloud Director-Appliance mithilfe des vSphere Web Client oder des vSphere Client](#)
- [Bereitstellen der vCloud Director-Appliance mit dem VMware OVF Tool](#)

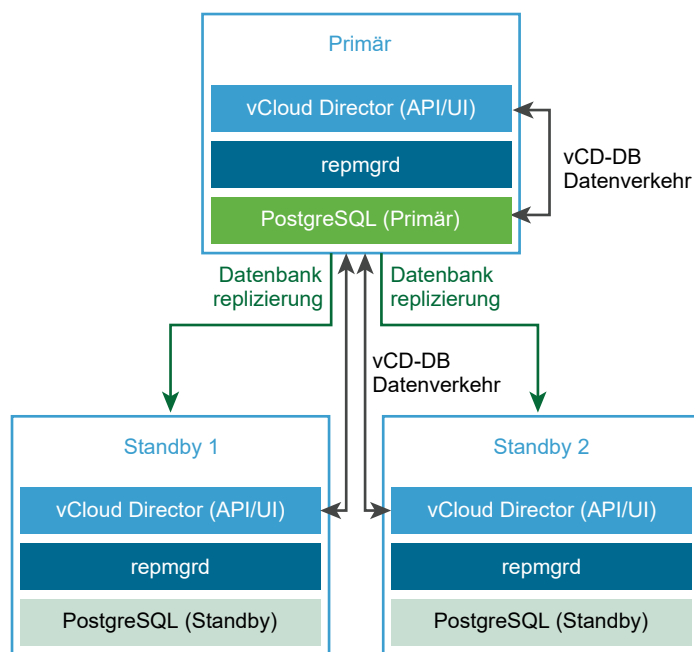
Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration

Die vCloud 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 vCloud Director-Datenbank bereitstellt.

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

Um HA für Ihre vCloud Director-Datenbank zu konfigurieren, können Sie beim Erstellen Ihrer Servergruppe einen Datenbank-HA-Cluster konfigurieren, indem Sie eine primäre und zwei Standby-Instanzen der vCloud Director-Appliance bereitstellen.

Abbildung 6-1. Ein HA-Cluster der vCloud Director-Appliance-Datenbank



Erstellen einer vCloud Director-Appliance-Bereitstellung mit Datenbank-HA

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

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

Die primäre Zelle ist das erste Mitglied in der vCloud Director-Servergruppe. Die eingebettete Datenbank ist als vCloud 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 vCloud Director-Diensts mit den Anmeldedaten des **Systemadministrators** bei der vCloud Director-Webkonsole unter `https://primary_eth0_ip_address/Cloud` 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 vCloud Director-Appliance als Standby-Zellen bereit.

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

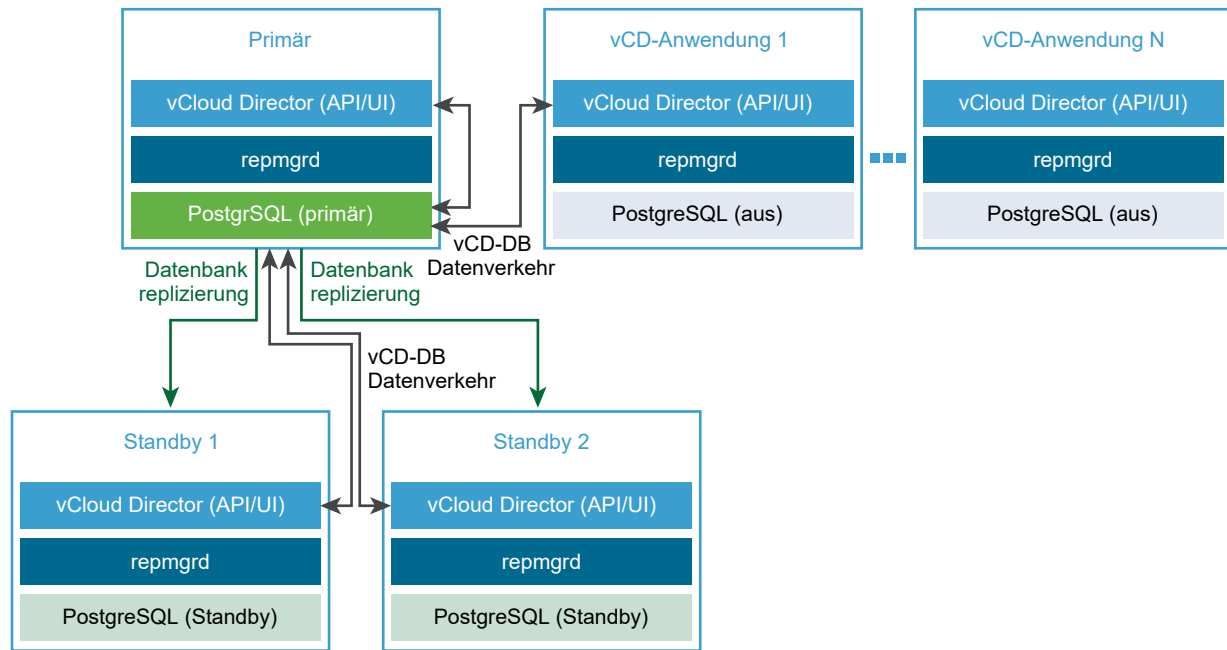
Hinweis Nach der anfänglichen Bereitstellung der Standby-Appliance beginnt der Replication Manager mit der Synchronisierung ihrer Datenbank mit der primären Appliance-Datenbank. Während dieser Zeit ist die vCloud Director-Datenbank und damit auch die vCloud Director-Benutzeroberfläche nicht verfügbar.

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

Weitere Informationen finden Sie unter [Anzeigen des Status der Zellen in einem Datenbank-Hochverfügbarkeits-Cluster](#).

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

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



Erstellen einer vCloud Director-Appliance-Bereitstellung ohne Datenbank-HA

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

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

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

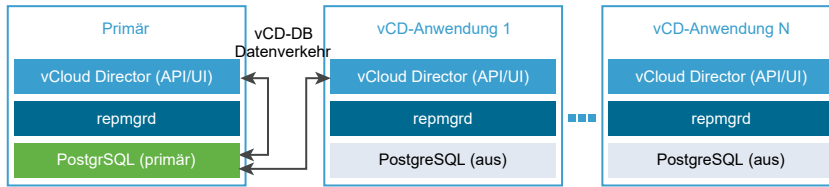
- 2 Stellen Sie sicher, dass die primäre Zelle aktiv ist und ausgeführt wird.

- a Melden Sie sich zum Überprüfen der Integrität des vCloud Director-Diensts mit den Anmeldedaten des **Systemadministrators** bei der vCloud Director-Webkonsole unter `https://primary_eth0_ip_address/Cloud` an.
- b Melden Sie sich zum Überprüfen der Integrität der PostgreSQL-Datenbank als **root** bei der Verwaltungsoberfläche 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 vCloud Director-Appliance als vCD-Anwendungszellen bereit.

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



Voraussetzungen für die Bereitstellung der vCloud Director-Appliance

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

- Überprüfen Sie, ob Sie Zugriff auf die vCloud 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](#).

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 vCloud Director-Appliance-Bereitstellung

- [Bereitstellen der vCloud Director-Appliance mithilfe des vSphere Web Client oder des vSphere Client](#)
- [Bereitstellen der vCloud Director-Appliance mit dem VMware OVF Tool](#)
- [Bereitstellen der vCloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation](#)

Bereitstellen der vCloud Director-Appliance mithilfe des vSphere Web Client oder des vSphere Client

Sie können die vCloud Director-Appliance mit dem vSphere Web Client (Flex) oder dem vSphere Client (HTML5) als OVF-Vorlage bereitstellen.

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

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

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 vCloud Director-Appliance mit dem VMware OVF Tool](#).

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

Voraussetzungen

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

Verfahren

1 Starten der Bereitstellung der vCloud Director-Appliance

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

2 Anpassen der vCloud Director-Appliance und Fertigstellen der Bereitstellung

Um die Details für vCloud Director zu konfigurieren, können Sie die Appliance-Vorlage anpassen.

Nächste Schritte

- Konfigurieren Sie die öffentliche Konsolen-Proxy-Adresse, da die vCloud Director-Appliance ihre eth0-NIC mit dem benutzerdefinierten Port 8443 für den Konsolen-Proxy-Dienst verwendet. Weitere Informationen finden Sie unter [Anpassen öffentlicher Endpoints](#).
- Um der vCloud Director-Servergruppe Mitglieder hinzuzufügen, wiederholen Sie den Vorgang.
- Um den Lizenzschlüssel einzugeben, melden Sie sich bei der vCloud Director-Webkonsole 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 vCloud Director unter Linux](#) ausführen.

Starten der Bereitstellung der vCloud Director-Appliance

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

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 vCloud 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 vCloud 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 vCloud Director-Servergruppe bereit.</p> <p>Die eingebettete Datenbank in der primären Zelle ist als vCloud Director-Datenbank konfiguriert. Der Datenbankname lautet vc1oud, und der Datenbankbenutzer ist vc1oud.</p>
Primär-groß	<p>Stellt die Appliance mit 24 GB RAM und 4 vCPUs als erstes Mitglied in einer vCloud Director-Servergruppe bereit.</p> <p>Die eingebettete Datenbank in der primären Zelle ist als vCloud Director-Datenbank konfiguriert. Der Datenbankname lautet vc1oud, und der Datenbankbenutzer ist vc1oud.</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 vCloud 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> <p>Stellt die Appliance mit 24 GB RAM und 4 vCPUs als zweites oder drittes Mitglied in einer vCloud Director-Servergruppe mit einer Datenbank-Hochverfügbarkeitskonfiguration bereit.</p> <p>Die eingebettete Datenbank in einer Standby-Appliance wird in einem Replizierungsmodus mit der primären Datenbank konfiguriert.</p>
vCD-Anwendungszelle	<p>Stellt die Appliance mit 8 GB RAM und 2 vCPUs als nachfolgendes Mitglied in einer vCloud Director-Servergruppe bereit.</p> <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 vCloud 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 zur Seite **Vorlage anpassen** geleitet, wo Sie die Details für vCloud Director konfigurieren.

Anpassen der vCloud Director-Appliance und Fertigstellen der Bereitstellung

Um die Details für vCloud Director zu konfigurieren, können Sie die Appliance-Vorlage anpassen.

Wenn Sie die vCloud Director-Appliance anpassen, konfigurieren Sie die Appliance-Einstellungen, die Datenbank und die Netzwerkeigenschaften. Sie konfigurieren die anfänglichen Systemeinstellungen nur, wenn Sie eine primäre Appliance bereitstellen, die das erste Mitglied einer Servergruppe ist.

Hinweis Nur [Schritt 3](#) dieses Verfahrens ist optional. Sie müssen alle anderen Schritte ausführen, um die vCloud Director-Appliance anzupassen.

Verfahren

- 1 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>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.
Aktivieren von SSH	Standardmäßig deaktiviert.
Mounten von NFS für Übertragungsdateispeicherort	Weitere Informationen finden Sie unter Vorbereiten des Übertragungsserverspeichers .

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

- 2 Wenn Sie das erste Mitglied einer Servergruppe bereitstellen, geben Sie im Abschnitt **VCD konfigurieren – nur für „primäre“ Appliances erforderlich** die Datenbankdetails ein, erstellen Sie das **Systemadministrator**-Konto und konfigurieren Sie die Systemeinstellungen.

Der Datenbankname lautet vcloud, und der Datenbankbenutzer ist vcloud.

Einstellung	Beschreibung
DB-Kennwort „vcloud“ für den Benutzer „vcloud“	Das Kennwort für den vcloud-Datenbankbenutzer.
Benutzername des Administrators	Der Benutzername für das Systemadministrator -Konto. Standardmäßig administrator.

Einstellung	Beschreibung
Vollständiger Name des Administrators	Der vollständige Name des Systemadministrators . Standardmäßig vCD Admin.
Benutzerkennwort des Administrators	Das Kennwort für das Systemadministrator -Konto.
E-Mail des Administrators	Die E-Mail-Adresse des Systemadministrators .
Systemname	Der Name des vCenter Server-Ordners, der für diese vCloud Director-Installation erstellt werden soll. Standardmäßig vcd1.
Installations-ID	Die ID für diese vCloud Director-Installation, die bei der Erstellung von MAC-Adressen für virtuelle Netzwerkkarten verwendet werden soll. Standardmäßig 1. Wenn Sie ausgeweitete Netzwerke für vCloud Director-Installationen in Multisite-Bereitstellungen erstellen möchten, richten Sie eine eindeutige Installations-ID für jede vCloud Director-Installation ein.

- 3** (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**.

Sie müssen möglicherweise statische Routen angeben, wenn Sie Hosts über eine nicht standardmäßige Gateway-Route erreichen möchten. 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 kommagetrennten 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, 172.16.100.253 192.168.100.0/24**.

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

Hinweis Alle Einstellungen sind erforderlich.

Einstellung	Beschreibung
Standard-Gateway	Die IP-Adresse des Standard-Gateways für die Appliance.
Domänenname	Der Domänenname, zum Beispiel <i>mydomain.com</i> .
Domänensuchpfad	Eine durch Kommas oder Leerzeichen getrennte Liste von Domännennamen für den Domänensuchpfad der Appliance.
Domännennamenserver	Die IP-Adresse des Domännennamenservers 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.

Einstellung	Beschreibung
eth1-Netzwerk-IP-Adresse	Die IP-Adresse für die eth1-Schnittstelle.
eth1-Netzwerkmaske	Die Netzmaske oder das Präfix für die eth1-Schnittstelle.

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

Nächste Schritte

Schalten Sie die neu erstellte virtuelle Maschine ein.

Bereitstellen der vCloud Director-Appliance mit dem VMware OVF Tool

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

Sie müssen das erste Mitglied einer vCloud Director-Servergruppe als primäre Zelle bereitstellen. Sie können ein nachfolgendes Mitglied einer vCloud Director-Servergruppe als Standby- oder vCD-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*.

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

ovftool-Befehlsoptionen und -Eigenschaften für die Bereitstellung der vCloud Director-Appliance

Option	Wert	Beschreibung
--noSSLVerify	n. v.	Überspringt die SSL-Überprüfung für vSphere-Verbindungen.
--acceptAllEulas	n. v.	Akzeptiert alle Endbenutzer-Lizenzvereinbarungen (EULAs).
--datastore	<i>target_vc_datastore</i>	Der Name des Zieldatenspeichers, auf dem die Konfigurationsdateien und virtuellen Festplatten der virtuellen Maschine gespeichert werden sollen.

Option	Wert	Beschreibung
<code>--allowAllExtraConfig</code>	n. v.	Konvertiert alle zusätzlichen Konfigurationsoptionen in das Format VMX.
<code>--net:"eth0 Network"</code>	<code>portgroup_on_vc_for_eth0</code>	Das Zielnetzwerk für das eth0-Netzwerk der Appliance. Wichtig Muss sich vom eth1-Zielnetzwerk unterscheiden.
<code>--net:"eth1 Network"</code>	<code>portgroup_on_vc_for_eth1</code>	Das Zielnetzwerk für das eth1-Netzwerk der Appliance. Wichtig Muss sich vom eth0-Zielnetzwerk unterscheiden.
<code>--name</code>	<code>vm_name_on_vc</code>	Der VM-Name für die Appliance.
<code>--diskMode</code>	thin oder thick	Das Festplattenformat für die Konfigurationsdateien und virtuellen Festplatten der virtuellen Maschine.
<code>--prop:"vami.ip0.VMware_vCloud_Director" eth0_ip_address</code>		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.
<code>--prop:"vami.ip1.VMware_vCloud_Director" eth1_ip_address</code>		IP-Adresse von eth1. Wird für den Zugriff auf interne Dienste verwendet, einschließlich des eingebetteten PostgreSQL-Datenbankdiensts.
<code>--prop:"vami.DNS.VMware_vCloud_Director" dns_ip_address</code>		Die IP-Adresse des Domänennamenservers für die Appliance.
<code>--prop:"vami.domain.VMware_vCloud_Director" domain_name</code>		Die DNS-Suchdomäne. Wird als erstes Element im Suchpfad angezeigt.
<code>--prop:"vami.gateway.VMware_vCloud_Director" gateway_ip_address</code>		Die IP-Adresse des Standard-Gateways für die Appliance.
<code>--prop:"vami.netmask0.VMware_vCloud_Director" netmask</code>		Die Netzmaske oder das Präfix für die eth0-Schnittstelle.
<code>--prop:"vami.netmask1.VMware_vCloud_Director" netmask</code>		Die Netzmaske oder das Präfix für die eth1-Schnittstelle.
<code>--prop:"vami.searchpath.VMware_vCloud_Director" searchpath</code>		Der Domänensuchpfad der Appliance. Eine komma- oder leerzeichengetrennte Liste von Domänennamen.
<code>--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director" enable_ssh</code>		Aktiviert oder deaktiviert den SSH- root -Zugriff auf die Appliance.

Option	Wert	Beschreibung
<code>--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"</code>	<code>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"</code>	<code>ip_address: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"</code>	<code>ip_address</code>	Die IP-Adresse des Zeitservers.
<code>--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"</code>	<code>password</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>password</code>	Das Datenbankkennwort des cloud -Benutzers. Wird nur für eine primäre Zelle verwendet.
<code>--prop:"vcloudwiz.admin_email.VMware_vCloud_Director"</code>	<code>email_address</code>	Die E-Mail-Adresse für das Systemadministrator -Konto. Wird nur für eine primäre Zelle verwendet.
<code>--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director"</code>	<code>first_name</code>	Der Name für das Systemadministrator -Konto. Wird nur für eine primäre Zelle verwendet.
<code>--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director"</code>	<code>password</code>	Das Kennwort für das Systemadministrator -Konto. Wird nur für eine primäre Zelle verwendet.
<code>--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director"</code>	<code>username</code>	Der Benutzername für das Systemadministrator -Konto. Wird nur für eine primäre Zelle verwendet.
<code>--prop:"vcloudwiz.inst_id.VMware_vCloud_Director"</code>	<code>install_ID</code>	Die Installations-ID für vCloud Director Wird nur für eine primäre Zelle verwendet.

Option	Wert	Beschreibung
<code>--prop:"vcloudconf.sys_name.VMware_vCloud_Director_sys_name"</code>	<code>sys_name</code>	Der Name des vCenter Server-Ordners, der für diese vCloud Director-Installation erstellt werden soll.
<code>--prop:"vcloudnet.routes0.VMware_vCloud_Director_ip_address1 cidr, ip_address2, ..."</code>	<code>ip_address1 cidr, ip_address2, ...</code>	Optional. Statische Routen für die eth0-Schnittstelle. Es muss sich um eine kommagetrennte 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.
<code>--prop:"vcloudnet.routes1.VMware_vCloud_Director_ip_address1 cidr, ip_address2, ..."</code>	<code>ip_address1 cidr, ip_address2, ...</code>	Optional. Statische Routen für die eth1-Schnittstelle. Es muss sich um eine kommagetrennte 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.

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 Appliance-Größen „Primär-klein“ und „Standby-klein“ 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 vCloud Director-Servergruppe bereit. Die eingebettete Datenbank in der primären Zelle ist als vCloud Director-Datenbank konfiguriert. Der Datenbankname lautet vcloud und der Datenbankbenutzer ist vcloud. ■ primary-large stellt die Appliance mit 24 GB RAM und 4 vCPUs als erstes Mitglied in einer vCloud Director-Servergruppe bereit. Die eingebettete Datenbank in der primären Zelle ist als vCloud Director-Datenbank konfiguriert. Der Datenbankname lautet vcloud, und der Datenbankbenutzer ist vcloud. ■ standby-small stellt die Appliance mit 12 GB RAM und 2 vCPUs als zweites oder drittes Mitglied in einer vCloud Director-Servergruppe mit einer Datenbank-Hochverfügbarkeitskonfiguration bereit. Die eingebettete Datenbank in einer Standby-Zelle wird in einem Replizierungsmodus mit der primären Datenbank konfiguriert. ■ standby-large stellt die Appliance mit 24 GB RAM und 4 vCPUs als zweites oder drittes Mitglied in einer vCloud 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"> ■ cell stellt die Appliance mit 8 GB RAM und 2 vCPUs als nachfolgendes Mitglied in einer vCloud Director-Servergruppe bereit. 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 vCloud 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.</p> <p>Nach der Bereitstellung können Sie die Größe der Appliance neu konfigurieren.</p>
--powerOn	<i>path_to_ova</i>	Schaltet die virtuelle Maschine nach der Bereitstellung manuell ein.

Ein Beispielbefehl für die Bereitstellung der primären vCloud Director-Appliance

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp_server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot_password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="Xj052mXAP7n#" \
```

```
--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"="o@e@vJW26Pnb" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

Ein Beispielbefehl zum Bereitstellen einer vCloud Director-Standby-Appliance

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp_server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varroot_password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \
--deploymentOption="standby-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

Erstellung und Verwaltung von SSL-Zertifikaten der vCloud Director-Appliance

7

Die vCloud Director-Appliance verwendet SSL, um die Kommunikation zwischen Clients und Servern zu sichern. Jede vCloud Director-Appliance muss zwei unterschiedliche SSL-Endpoints unterstützen – für die HTTPS- und die Konsolen-Proxy-Kommunikation.

Diese Endpoints können separate IP-Adressen oder eine einzelne IP-Adresse mit zwei verschiedenen Ports sein. Es wird für jeden Endpunkt ein eigenes SSL-Zertifikat benötigt. Sie können dasselbe Zertifikat (z. B. ein Platzhalterzertifikat) für beide Endpoints verwenden.

Dieses Kapitel enthält die folgenden Themen:

- [Bereitstellen der vCloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation](#)
- [Erstellen und Importieren der von einer Zertifizierungsstelle signierten SSL-Zertifikate in die vCloud Director-Appliance](#)
- [Importieren von privaten Schlüsseln und den von einer Zertifizierungsstelle signierten SSL-Zertifikaten in die vCloud Director-Appliance](#)
- [Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und vCloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats](#)
- [Verlängern der vCloud Director-Appliance-Zertifikate](#)

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

Sie können die vCloud 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 vCloud Director-Appliances generiert vCloud Director standardmäßig selbstsignierte Zertifikate und verwendet sie zum Konfigurieren der vCloud 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 vCloud 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 vCloud Director-Appliance](#).

Wenn es sich bei den signierten Zertifikaten, die Sie für die primäre vCloud Director-Appliance verwenden, um signierte Platzhalterzertifikate handelt, können diese Zertifikate auf alle anderen Appliances in der vCloud Director-Servergruppe, d. h. Standby-Zellen und vCloud 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 vCloud 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 vCloud Director-Appliance](#).
- Vergewissern Sie sich, dass das private Kennwort für die Schlüssel im Keystore mit dem Keystore-Kennwort übereinstimmt. Das Keystore-Kennwort muss mit dem anfänglichen Root-Kennwort übereinstimmen, das bei der Bereitstellung aller Appliances verwendet wird, beispielsweise

```
/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 vCloud 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 Dienst `vmware-vcd` auf der primären-Appliance neu.

```
service vmware-vcd restart
```

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

In der vCloud 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 vCloud Director-Appliance](#) beschriebenen Schritte.

Wichtig Bei der Bereitstellung generiert die vCloud 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_passwd* dargestellt.

Voraussetzungen

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

Verfahren

- 1 Melden Sie sich direkt oder mithilfe von SSH bei der Konsole der vCloud Director-Appliance als **root** an.

- 2 Je nach den Anforderungen Ihrer Umgebung wählen Sie eine der folgenden Optionen aus.

Wenn Sie die vCloud Director-Appliance bereitstellen, generiert vCloud 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 Schritt 5](#) fort.
- Wenn Sie neue Zertifikate mit benutzerdefinierten Optionen generieren möchten, z. B. eine größere Schlüsselgröße, fahren Sie mit [Schritt 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 vCloud 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 vCloud 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 JCEKS -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 JCEKS -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 vCloud Director-Appliance.

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

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

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

- 10** Führen Sie den Befehl aus, um die Zertifikate in die vCloud 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 vCloud Director-Appliance neu.

```
service vmware-vcd restart
```

Nächste Schritte

- Wenn Sie Platzhalterzertifikate verwenden, finden Sie weitere Informationen unter [Bereitstellen der vCloud Director-Appliance mit signierten Platzhalterzertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation](#).

- Wenn Sie keine Platzhalterzertifikate verwenden, wiederholen Sie diesen Vorgang auf allen vCloud Director-Servern in der Servergruppe.
- Weitere Informationen zum Ersetzen der Zertifikate für die eingebettete PostgreSQL-Datenbank und die Verwaltungsschnittstelle der vCloud Director-Appliance finden Sie unter [Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und vCloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats](#).

Importieren von privaten Schlüsseln und den von einer Zertifizierungsstelle signierten SSL-Zertifikaten in die vCloud 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 vCloud 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 vCloud Director-Appliance zu importieren. vCloud 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 von SSH bei der Konsole der vCloud 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 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.pfx -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.pfx -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 JCEKS-Keystore 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 JCEKS -srckeystore http.pfx -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 JCEKS -srckeystore consoleproxy.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

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

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

- 7** Führen Sie den Befehl aus, um die signierten Zertifikate in die vCloud 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 vCloud Director-Appliance neu.

```
service vmware-vcd restart
```

Nächste Schritte

- Wenn Sie Platzhalterzertifikate verwenden, finden Sie weitere Informationen unter [Bereitstellen der vCloud 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 vCloud Director-Appliance in der Servergruppe.
- Weitere Informationen zum Ersetzen der Zertifikate für die eingebettete PostgreSQL-Datenbank und die Verwaltungsschnittstelle der vCloud Director-Appliance finden Sie unter [Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und vCloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats](#).

Ersetzen eines selbstsignierten eingebetteten PostgreSQL- und vCloud Director-Appliance-Verwaltungsbenutzeroberflächen-Zertifikats

Standardmäßig nutzen die eingebettete PostgreSQL-Datenbank und die Verwaltungsbenutzeroberfläche der vCloud 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 vCloud Director-Appliance bereitstellen, werden selbstsignierte Zertifikate mit einem Gültigkeitszeitraum von 365 Tagen generiert. Die vCloud Director-Appliance verwendet zwei Sätze von SSL-Zertifikaten. Der vCloud Director-Dienst verwendet einen Satz von Zertifikaten für die HTTPS- und die Konsolen-Proxy-Kommunikation. Die eingebettete PostgreSQL-Datenbank und die Verwaltungsbenutzeroberfläche der vCloud 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 vCloud Director-Truststore auf anderen vCloud Director-Zellen importiert. Der Vorgang kann bis zu 60 Sekunden dauern.

Verlängern der vCloud Director-Appliance-Zertifikate

Wenn Sie die vCloud 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 vCloud Director-Zelle einzeln erneuern.

Die vCloud Director-Appliance verwendet zwei Sätze von SSL-Zertifikaten. Der vCloud Director-Dienst verwendet einen Satz von Zertifikaten für die HTTPS- und Konsolen-Proxy-Kommunikation. Die eingebettete PostgreSQL-Datenbank und die Verwaltungsbenutzeroberfläche der vCloud 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 vCloud 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](#).

Verfahren

- 1 Melden Sie sich direkt oder mithilfe von SSH beim Betriebssystem der vCloud Director-Appliance als **root** an.

- 2** Führen Sie zum Beenden der vCloud Director-Dienste den folgenden Befehl aus.

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

- 3** Führen Sie zum Generieren von neuen selbstsignierten Zertifikaten den folgenden Befehl aus.

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

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 vCloud Director, die in [Schritt 4](#) verwendet werden.

- 4** Wenn Sie keine von einer Zertifizierungsstelle signierten Zertifikate verwenden, führen Sie den Befehl zum Importieren der neu generierten selbstsignierten Zertifikate in vCloud Director aus.

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

- 5** Starten Sie den vCloud Director-Dienst neu.

```
service vmware-vcd start
```

Ergebnisse

Die verlängerten selbstsignierten Zertifikate werden in der vCloud Director-Benutzeroberfläche angezeigt.

Das neue PostgreSQL-Zertifikat wird bei der nächsten Ausführung der Funktion `appliance-sync` in den vCloud Director-Truststore auf anderen vCloud 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.

Konfiguration der vCloud Director-Appliance

8

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 vCloud 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 vCloud 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.

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen des Status der Zellen in einem Datenbank-Hochverfügbarkeits-Cluster](#)
- [Wiederherstellen nach einem Ausfall der primären Datenbank in einem Hochverfügbarkeits-Cluster](#)
- [Sichern und Wiederherstellen der eingebetteten Datenbank der vCloud Director-Appliance](#)
- [Konfigurieren des externen Zugriffs auf die vCloud Director-Datenbank](#)
- [Aktivieren oder Deaktivieren des SSH-Zugriffs auf die vCloud Director-Appliance](#)
- [Bearbeiten der DNS-Einstellungen für die vCloud Director-Appliance](#)
- [Bearbeiten der statischen Routen für die Netzwerkschnittstellen der vCloud Director-Appliance](#)
- [Konfigurationsskripts in der vCloud Director-Appliance](#)
- [Ändern der PostgreSQL-Konfigurationen in der vCloud Director-Appliance](#)

Anzeigen des Status der Zellen in einem Datenbank-Hochverfügbarkeits-Cluster

Um den Status der primären und Standby-Zellen in einem Hochverfügbarkeits-Cluster (HA) einer Appliance-Datenbank anzuzeigen, können Sie sich bei der Appliance-Verwaltungsbenutzeroberfläche einer beliebigen Zelle des Datenbank-HA-Clusters anmelden.

Der HA-Cluster der vCloud Director-Appliance-Datenbank besteht aus einer primären und zwei Standby-Zellen. Weitere Informationen finden Sie unter [Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration](#).

Verfahren

- 1 Navigieren Sie in einem Webbrowser zur Appliance-Verwaltungsbenutzeroberfläche unter `https://vcd_ip_address:5480`.
- 2 Melden Sie sich als **root** an.
- 3 Um die Details zu den Zellen im HA-Datenbank-Cluster anzuzeigen, klicken Sie auf **vCD-Datenbankverfügbarkeit**.

Eigenschaft	Beschreibung
Name	Der DNS-Name der Zelle.
Rolle	Es kann sich um primär oder Standby handeln. Ein HA-Cluster einer Appliance-Datenbank besteht aus einer primären und zwei Standby-Zellen.
Status	Kann ausgeführt, nicht erreichbar oder fehlgeschlagen sein. Ein Sternchen (*) gibt den Status der primären Zelle an.
Folgend	Der Name der primären Zelle, mit der die Standby-Zelle repliziert wird.

Nächste Schritte

Wenn sich eine Standby-Zelle nicht im ausgeführten Status befindet, stellen Sie eine neue Standby-Zelle bereit.

Wenn sich die primäre Zelle nicht im ausgeführten Status befindet, finden Sie weitere Informationen unter [Wiederherstellen nach einem Ausfall der primären Datenbank in einem Hochverfügbarkeits-Cluster](#).

Wiederherstellen nach einem Ausfall der primären Datenbank in einem Hochverfügbarkeits-Cluster

Wenn die primäre Zelle nicht ordnungsgemäß ausgeführt wird, können Sie zum Wiederherstellen der vCloud Director-Datenbank eine der Standby-Zellen heraufstufen, damit diese zur neuen primären Zelle wird. Danach müssen Sie eine neue Standby-Zelle bereitstellen.

Voraussetzungen

- Die primäre Zelle befindet sich im Status „nicht erreichbar“ oder „fehlgeschlagen“.
- Die beiden Standby-Zellen befinden sich im ausgeführten Status.

Weitere Informationen finden Sie unter [Anzeigen des Status der Zellen in einem Datenbank-Hochverfügbarkeits-Cluster](#).

Verfahren

- 1 Melden Sie sich als **root** bei der Appliance-Verwaltungsbenutzeroberfläche einer aktiven Standby-Zelle an: `https://standby_ip_address:5480`.
- 2 Klicken Sie in der Spalte **Rolle** für die Standby-Zelle, die zur neuen primären Zelle werden soll, auf **Heraufstufen**.

Die Zelle wird zur neuen primären Zelle im ausgeführten Status. Die andere Standby-Zelle folgt der neu heraufgestuften primären Zelle.
- 3 Stellen Sie eine neue Standby-Appliance bereit.

Nächste Schritte

- 1 Entfernen Sie die fehlgeschlagene primäre Appliance aus der vCloud Director-Servergruppe und dem repmgr-Hochverfügbarkeits-Cluster. Weitere Informationen finden Sie unter [Löschen einer Cloud-Zelle](#) und [Aufheben der Registrierung einer fehlgeschlagenen primären Zelle in einem Datenbank-Hochverfügbarkeits-Cluster](#).
- 2 Löschen Sie bei Bedarf die fehlgeschlagene primäre Appliance.

Sichern und Wiederherstellen der eingebetteten Datenbank der vCloud Director-Appliance

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

Sichern der eingebetteten Datenbank der vCloud Director-Appliance

Wenn Ihre Umgebung aus Bereitstellungen der vCloud Director-Appliance mit eingebetteten PostgreSQL-Datenbanken besteht, können Sie die vCloud 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 von SSH bei der primären Zelle als **root** an.
- 2 Navigieren Sie zu `/opt/vmware/appliance/bin`.
- 3 Führen Sie den Befehl `create-db-backup` aus.

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 Datei `.tgz` enthält die Speicherabbilddatei der Datenbank sowie die Dateien `global.properties`, `responses.properties`, `certificates` und `proxycertificates` der primären Zelle.

Wiederherstellen einer vCloud Director-Appliance-Umgebung mit einer HA-Datenbankkonfiguration

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

Informationen zum Wiederherstellen einer Appliance-Bereitstellung mit einer Datenbankkonfiguration ohne HA finden Sie unter [Wiederherstellen einer vCloud Director-Appliance-Umgebung ohne HA-Datenbankkonfiguration](#).

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 vCloud Director-Appliance](#).
- Stellen Sie eine primäre und zwei Standby-Datenbankzellen bereit. Weitere Informationen finden Sie im [Kapitel 6 Bereitstellen der vCloud 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 vCloud 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 vCloud Director 9.7.0.1 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 vCloud 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 vCloud Director 9.7.0.1 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` steht nur für vCloud Director 9.7.0.1 und höher zur Verfügung.

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

- 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 den Befehl aus, um den vCloud 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 --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
```

Dabei gilt:

- Die Option `--keystore-password` stimmt mit dem Keystore-Kennwort für die Zertifikate in der Appliance überein.
- Die Option `--database-password` stimmt mit dem Datenbankkennwort überein, das Sie während der Bereitstellung der Appliance 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 vCloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der vCloud Director-Appliance fehl](#).

- e Führen Sie den Befehl aus, um den vCloud 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 [Kapitel 6 Bereitstellen der vCloud Director-Appliance](#).

- 7 Nachdem alle Zellen der Servergruppe gestartet wurden, stellen Sie sicher, dass die Wiederherstellung Ihrer vCloud Director-Umgebung erfolgreich verlaufen ist.
 - a Öffnen Sie die vCloud Director Web Console mithilfe der eth0-Netzwerk-IP-Adresse einer beliebigen Zelle aus der neuen Servergruppe, https://et0_IP_new_cell/cloud.
 - b Melden Sie sich bei der vCloud Director Web Console mit den vorhandenen Anmeldedaten für **Systemadministratoren** an.
 - c Stellen Sie sicher, dass Ihre vSphere- und Cloud-Ressourcen in der neuen Umgebung zur Verfügung stehen.
- 8 Verwenden Sie nach erfolgreicher Überprüfung der Datenbankwiederherstellung die vCloud Director Web Console, um die getrennten Zellen zu löschen, die zur alten vCloud Director-Umgebung gehören.
 - a Klicken Sie auf der Registerkarte **Verwalten und Überwachen** auf **Cloud-Zellen**.
 - b Klicken Sie mit der rechten Maustaste auf den Namen einer Zelle und wählen Sie **Löschen** aus.

Wiederherstellen einer vCloud Director-Appliance-Umgebung ohne HA-Datenbankkonfiguration

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

Informationen zum Wiederherstellen einer Appliance-Bereitstellung mit einer HA-Datenbankkonfiguration finden Sie unter [Wiederherstellen einer vCloud Director-Appliance-Umgebung mit einer HA-Datenbankkonfiguration](#).

Der Wiederherstellungs-Workflow umfasst drei Hauptphasen.

- Kopieren der eingebetteten Datenbanksicherungsdatei .tar aus dem freigegebenen NFS-Speicher des Übertragungsdiensts
- Wiederherstellen der Datenbank in der primären Zelle 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 vCloud Director-Appliance](#).
- Stellen Sie eine primäre Datenbankzelle bereit. Weitere Informationen finden Sie im [Kapitel 6 Bereitstellen der vCloud 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 in der primären Zelle als **root** bei der Konsole an und führen Sie den Befehl aus, um den vCloud Director-Dienst zu beenden.

```
service vmware-vcd stop
```

- 2 Kopieren Sie 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 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 vCloud Director 9.7.0.1 und höher zur Verfügung.

- 4 Führen Sie die Befehle aus, um die Datenbank zu löschen und in der neuen Appliance wiederherzustellen.

- 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 der primären Zelle eine Kopie der Konfigurationsdatendateien und ersetzen Sie sie. Konfigurieren Sie den vCloud 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 vCloud Director 9.7.0.1 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` steht nur für vCloud Director 9.7.0.1 und höher zur Verfügung.

```
cp certificates /optvmware/vcloud-director/.
```

- 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 den Befehl aus, um den vCloud 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 --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
```

Dabei gilt:

- Die Option `--keystore-password` stimmt mit dem Keystore-Kennwort für die Zertifikate in der Appliance überein.
- Die Option `--database-password` stimmt mit dem Datenbankkennwort überein, das Sie während der Bereitstellung der Appliance 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 vCloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der vCloud Director-Appliance fehl](#).

- e Führen Sie den Befehl aus, um den vCloud 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 [Kapitel 6 Bereitstellen der vCloud Director-Appliance](#).
- 7 Nachdem alle Zellen der Servergruppe gestartet wurden, stellen Sie sicher, dass die Wiederherstellung Ihrer vCloud Director-Umgebung erfolgreich verlaufen ist.
 - a Öffnen Sie die vCloud Director Web Console mithilfe der `eth0`-Netzwerk-IP-Adresse einer beliebigen Zelle aus der neuen Servergruppe, `https://eth0_IP_new_cell/cloud`.
 - b Melden Sie sich beim vCloud Director Web Console mit den vorhandenen Anmeldedaten für **Systemadministratoren** an.
 - c Stellen Sie sicher, dass Ihre vSphere- und Cloud-Ressourcen in der neuen Umgebung zur Verfügung stehen.
- 8 Verwenden Sie nach erfolgreicher Überprüfung der Datenbankwiederherstellung die vCloud Director Web Console, um die getrennten Zellen zu löschen, die zur alten vCloud Director-Umgebung gehören.
 - a Klicken Sie auf der Registerkarte **Verwalten und Überwachen** auf **Cloud-Zellen**.
 - b Klicken Sie mit der rechten Maustaste auf den Namen einer Zelle und wählen Sie **Löschen** aus.

Konfigurieren des externen Zugriffs auf die vCloud Director-Datenbank

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

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

Verfahren

- 1 Melden Sie sich direkt oder mithilfe von SSH 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	<i>CIDR_notation</i>	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 vCloud Director-Appliance

Während der Bereitstellung der Appliance können Sie den SSH-Zugriff auf die Appliance deaktivieren 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.

Verfahren

- 1 Wenn Sie zu Testzwecken vorübergehende Änderungen an der OVF-Eigenschaft vornehmen möchten, ändern Sie die Eigenschaft in vCloud Director.
 - a Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der vCloud 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**.

Bearbeiten der DNS-Einstellungen für die vCloud Director-Appliance

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

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

Verfahren

- 1 Wenn Sie die DNS-Einstellungen zu Testzwecken vorübergehend ändern möchten, bearbeiten Sie die DNS-Einstellungen in vCloud Director.

- a Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der vCloud 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 vCloud Director-Appliance

Sie können die statischen Routen für die Netzwerkschnittstellen *eth0* und *eth1* nach der ersten vCloud Director-Bereitstellung ändern.

Verfahren

- 1 Wenn Sie den Wert der statischen Route zu Testzwecken vorübergehend ändern möchten, bearbeiten Sie die statischen Routen in vCloud Director.
 - a Melden Sie sich direkt oder mithilfe eines SSH-Clients bei der Konsole der vCloud 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 kommasetrennten 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 vCloud 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 kommasetrennten 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.

Konfigurationsskripts in der vCloud Director-Appliance

Die vCloud Director-Appliance enthält bestimmte Konfigurationsskripts.

Verzeichnis	Beschreibung
<code>/opt/vmware/appliance/bin/</code>	Die Konfigurationsskripts 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 vCloud Director-Datenbank .

Ändern der PostgreSQL-Konfigurationen in der vCloud Director-Appliance

Sie können die PostgreSQL-Konfigurationen der vCloud 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` nicht, da diese Änderungen nach einem Neustart nicht beibehalten werden.

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.

Verwenden der Replication Manager-Tool-Suite in einer Hochverfügbarkeits-Cluster-Konfiguration

9

Die repmgr-Open-Source-Tool-Suite ist Teil der eingebetteten PostgreSQL-Datenbank der vCloud Director-Appliance. Mit repmgr können Sie PostgreSQL-Replizierung und -Datenbankfailover in Ihrem vCloud Director-Datenbank-Hochverfügbarkeits-Cluster konfigurieren, überwachen und steuern.

Sie können die repmgr-Befehlszeilenschnittstelle verwenden, um den Status und die Ereignisse eines Knotens oder Clusters zu überprüfen, um einen Knoten zu registrieren oder seine Registrierung aufzuheben, um einen Standby-Knoten heraufzustufen, um die Rollen eines primären und eines Standby-Knotens zu tauschen oder um einem neuen primären Knoten zu folgen.

Weitere Informationen zur vCloud Director-Datenbank-Hochverfügbarkeitskonfiguration finden Sie unter [Appliance-Bereitstellungen und Datenbank-Hochverfügbarkeitskonfiguration](#).

Um mehr über repmgr zu erfahren, besuchen Sie repmgr.org.

Dieses Kapitel enthält die folgenden Themen:

- [Überprüfen des Verbindungsstatus eines Datenbank-Hochverfügbarkeits-Clusters](#)
- [Überprüfen des Replizierungsstatus eines Knotens in einem Datenbank-Hochverfügbarkeits-Cluster](#)
- [Überprüfen des Status eines Datenbank-Hochverfügbarkeits-Clusters](#)
- [Erkennen eines früheren primären Knotens, der in einem Hochverfügbarkeits-Cluster wieder online geschaltet wird](#)
- [Tauschen der Rollen der primären Zelle und einer Standby-Zelle in einem Datenbank-Hochverfügbarkeits-Cluster](#)
- [Aufheben der Registrierung eines fehlgeschlagenen oder nicht erreichbaren Standby-Knotens in einem Datenbank-Hochverfügbarkeits-Cluster](#)
- [Aufheben der Registrierung einer fehlgeschlagenen primären Zelle in einem Datenbank-Hochverfügbarkeits-Cluster](#)
- [Aufheben der Registrierung einer aktiven Standby-Zelle in einem Datenbank-Hochverfügbarkeits-Cluster](#)

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 liefert Informationen zum Knoten, zur PostgreSQL-Version und zu den Replizierungsdetails.

- 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>/opt/vmware/vpostgres/current/bin/psql</code>
Führen Sie eine Abfrage auf einem Standby-Knoten aus.	<code>select * from pg_stat_wal_receiver;</code>

Überprüfen des Status eines Datenbank-Hochverfügbarkeits-Clusters

Zur Behebung von Problemen in Ihrem Datenbank-Hochverfügbarkeits-Cluster müssen Sie den Status der Knoten und die Ereignisse im Cluster überwachen.

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 den Status des Clusters.

In der **Upstream** wird der aktuelle primäre Knoten angezeigt.

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

Die Konsolenausgabe zeigt die Clusterinformationen an. Im folgenden Beispiel ist der primäre Knoten im Cluster, Knoten 3, nicht erreichbar.

```

ID | Name      | Role   | Status      | Upstream | Location | Connection string
---+-----+-----+-----+-----+-----+-----
Node 1 | Node name | standby | running     | Node 3 name | default | host=host IP address

```

```

user=repmgr dbname=repmgr
Node 2 | Node name | standby |      running      | Node 3 name | default | host=host IP address
user=repmgr dbname=repmgr
Node 3 | Node name | primary | ? unreachable |      | default | host=host IP address
user=repmgr dbname=repmgr

```

Im folgenden Systemausgabenbeispiel ist Knoten 3 der primäre Knoten in einem fehlerfreien Cluster.

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	Node name	standby	running	Node3 name	default	host=host IP address user=repmgr dbname=repmgr
Node 2	Node name	standby	running	Node3 name	default	host=host IP address user=repmgr dbname=repmgr
Node 3	Node name	primary	*running		default	host=host IP address user=repmgr dbname=repmgr

4 Überprüfen Sie das Cluster-Ereignisprotokoll.

```

/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf cluster
event

```

Die Systemausgabe zeigt Erstellungs-, Klon- und Registrierungsereignisse im Cluster.

Nächste Schritte

Wenn der Status des primären Knotens `unreachable` oder `failed` lautet, müssen Sie einen Standby-Knoten heraufstufen.

Wenn der Status eines Standby-Knotens `unreachable` oder `failed` lautet, reparieren Sie den Knoten und starten Sie den PostgreSQL-Dienst, wenn er nicht ausgeführt wird.

Erkennen eines früheren primären Knotens, der in einem Hochverfügbarkeits-Cluster wieder online geschaltet wird

Wenn ein primärer Knoten in Ihrem Cluster ausfällt und dann wieder online geschaltet wird, wenn Sie einen Standby-Knoten zum neuen primären Knoten heraufstufen, führt dies zu Ungenauigkeiten in den `repmgr`-Daten. Sie können diese Unregelmäßigkeiten mit dem Befehl `repmgr cluster show` erkennen.

Beispiel: Ausführen von `repmgr cluster show` auf dem früheren primären Knoten

Im folgenden Beispiel führt das Ausführen des Befehls `repmgr cluster show` auf einem früheren primären Knoten, der wieder online geschaltet wird, zu der folgenden Systemausgabe.

```

      ID | Name      | Role   | Status          | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Name Knoten 1 | standby | !running as primary | Name Knoten 3 | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
Node 2 | Name Knoten 2 | standby | running         | Name Knoten 3 | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
Node 3 | Name Knoten 3 | primary | * running       |           | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is registered as standby but running as primary

```

Im Beispiel ist Knoten 1 der aktuelle primäre Knoten im Cluster.

Wenn Sie beim Ausführen des Befehls `repmgr cluster show` den Status `!running as primary` für einen Standby-Knoten erhalten, weist dies darauf hin, dass ein früherer primärer Knoten im Cluster ausgeführt wird. In diesem Fall müssen Sie den früheren primären Knoten herunterfahren und seine Registrierung aufheben.

Beispiel: Ausführen von `repmgr cluster show` auf dem neuen primären Knoten

Im folgenden Beispiel führt das Ausführen des Befehls `repmgr cluster show` auf dem neuen primären Knoten zu der folgenden Systemausgabe.

```

      ID | Name      | Role   | Status          | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Name Knoten 1 | primary | * running       |           | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
Node 2 | Name Knoten 2 | standby | running         | Name Knoten 1 | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
Node 3 | Name Knoten 3 | primary | ! running       |           | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 3(ID: Node 3) is running but the repmgr node record is inactive

```

In diesem Fall sind die `repmgr`-Daten korrekt. Sie geben genau an, dass Knoten 1 ausgeführt wird und dass es sich um den aktuellen primären Knoten handelt. Die Warnmeldung zu Knoten 3, dem früheren primären Knoten, gibt an, dass die `repmgr`-Daten auf diesem Knoten nicht korrekt sind.

Beispiel: Ausführen von `repmgr cluster show` nach dem Heraufstufen eines Standby-Knotens ohne Ausführen von `standby follow` auf den verbleibenden Standby-Knoten

Im folgenden Beispiel werden die `repmgr`-Daten auf jedem Knoten in einem Cluster angezeigt, in dem der primäre Knoten fehlgeschlagen ist. Ein Standby-Knoten wurde mit dem Befehl `repmgr standby promote` manuell heraufgestuft, ohne auf den verbleibenden Standby-Knoten `repmgr standby follow` auszuführen.

Wenn Sie `repmgr cluster show` auf dem neuen primären Knoten ausführen, zeigt die Systemausgabe korrekte `repmgr`-Daten an, aber auf den neuen primären Knoten, Knoten 2, folgen keine Standby-Knoten.

```

ID | Name      | Role   | Status   | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Name Knoten 1 | primary | * running |          | default | host=Host-IP-Adresse user=repmgr
dbname=repmgr
Node 2 | Name Knoten 2 | primary | ! running |          | default | host=Host-IP-Adresse user=repmgr
dbname=repmgr
Node 3 | Name Knoten 3 | standby | running  | Name Knoten 1 | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is running but the repmgr node record is inactive

```

Sowohl Knoten 1, der frühere primäre Knoten, als auch Knoten 3, der Standby-Knoten, der auf den früheren primären Knoten folgt, liefern ungenaue `repmgr`-Daten.

```

ID | Name      | Role   | Status           | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Name Knoten 1 | primary | * running        |          | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
Node 2 | Name Knoten 2 | standby | ! running as primary | Name Knoten 1 | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
Node 3 | Name Knoten 3 | standby | running          | Name Knoten 1 | default | host=Host-IP-Adresse
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 2(ID: Node 2) is registered as standby but running as primary

```

Beispiel: Ausführen von `repmgr cluster show` auf einem Standby-Knoten

Wenn Sie den Befehl auf einem Standby-Knoten ausführen, der auf den aktuellen primären Knoten folgt, führt dies zu einer Systemausgabe mit genauen `repmgr`-Daten, die mit den Daten auf dem aktuellen primären Knoten identisch sind.

Wenn Sie den Befehl auf einem Standby-Knoten ausführen, der auf den früheren primären Knoten folgt, führt dies zu einer Systemausgabe mit ungenauen `repmgr`-Daten, die mit den Daten auf dem früheren primären Knoten identisch sind.

Protokolleinträge

Wenn ein früherer primärer Knoten, der fehlgeschlagen ist, wieder online geschaltet wird, nachdem Sie einen Standby-Knoten zum neuen primären Knoten heraufgestuft haben, werden die folgenden Einträge in der Datei `update-repmgr-data.log` auf allen Knoten mit ungenauen `repmgr`-Daten angezeigt.

```
ERROR: An old primary is running in the repmgr cluster.
ERROR: Manual intervention is required to repair the repmgr cluster.
ERROR: The first step should be to shutdown and unregister the old primary.
```

Tauschen der Rollen der primären Zelle und einer Standby-Zelle in einem Datenbank-Hochverfügbarkeits-Cluster

Sie können einen `repmgr`-Befehl verwenden, um die Rollen des primären Knotens und eines der Standby-Knoten in Ihrem Datenbank-Hochverfügbarkeits-Cluster während einer geplanten Wartung zu tauschen.

Voraussetzungen

- Versetzen Sie alle vCloud Director-Zellen, die Teil des Hochverfügbarkeits-Clusters sind, in den Wartungsmodus.
- Stellen Sie sicher, dass alle Knoten im Cluster fehlerfrei und online sind.

Verfahren

- 1 Melden Sie sich, bei Bedarf mithilfe von SSH, als **root** beim Betriebssystem des Standby-Knotens an, den Sie heraufstufen möchten.
- 2 Ändern Sie den Benutzer in **postgres**.

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

- 3 (Optional) Stellen Sie sicher, dass die Voraussetzungen für die Umstellung erfüllt sind, indem Sie den Befehl mit der Option `--dry-run` ausführen.

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow --dry-run
```

- 4 Tauschen Sie die Rollen der primären und der Standby-Zelle.

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow
```

Ergebnisse

Die letzte Zeile der Konsolenausgabe gibt an, dass die Standby-Umstellung erfolgreich abgeschlossen wurde.

Nächste Schritte

- 1 Führen Sie den Befehl **reconfigure-database** aus, um die Datenbank-IP-Adresse auf allen vCloud Director-Zellen zu aktualisieren. Weitere Informationen finden Sie unter [Aktualisieren der Datenbank-IP-Adressen auf vCloud Director-Zellen](#).
- 2 Wenn Sie die vCloud Director-Zellen in der Servergruppe neu konfigurieren, damit sie auf die neue primäre Datenbank verweisen, deaktivieren Sie den Wartungsmodus aller vCloud Director-Zellen, die Teil des Hochverfügbarkeits-Clusters sind.

Aufheben der Registrierung eines fehlgeschlagenen oder nicht erreichbaren Standby-Knotens in einem Datenbank-Hochverfügbarkeits-Cluster

Sie können repmgr auf einem aktiven Knoten in Ihrem Cluster verwenden, um die Registrierung eines fehlgeschlagenen oder nicht erreichbaren Standby-Knotens aufzuheben.

Hinweis Damit der primäre Knoten normal funktioniert, muss immer mindestens ein Standby-Knoten ausgeführt werden.

Voraussetzungen

Um die Registrierung eines inaktiven Standby-Knotens aufzuheben, müssen Sie die Knoten-ID angeben. Um die IP-Adresse zu finden, überprüfen Sie den Status des Clusters und suchen Sie nach dem Knoten. Verwenden Sie in dieser Zeile den Hostwert aus der Spalte „Connection string“, um die IP-Adresse des Knotens zu identifizieren. Weitere Informationen finden Sie im [Überprüfen des Status eines Datenbank-Hochverfügbarkeits-Clusters](#).

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 Heben Sie die Registrierung des fehlgeschlagenen oder nicht erreichbaren Knotens auf.

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

Ergebnisse

Durch das Aufheben der Registrierung des Knotens werden die Knoteninformationen aus den repmgr-Metadaten entfernt.

Aufheben der Registrierung einer fehlgeschlagenen primären Zelle in einem Datenbank-Hochverfügbarkeits-Cluster

Wenn der primäre Knoten in Ihrem Datenbank-Hochverfügbarkeits-Cluster fehlschlägt und Sie einen neuen primären Knoten heraufstufen, müssen Sie die Registrierung des fehlgeschlagenen primären Knotens aufheben, um ihn aus dem Cluster zu entfernen und inkonsistente Clusterstatusdaten zu vermeiden.

Voraussetzungen

- Um die Registrierung eines inaktiven primären Standby-Knotens aufzuheben, müssen Sie die Knoten-ID angeben. Um die IP-Adresse zu finden, überprüfen Sie den Status des Clusters und suchen Sie nach dem Knoten. Verwenden Sie in dieser Zeile den Hostwert aus der Spalte „Connection string“, um die IP-Adresse des Knotens zu identifizieren. Weitere Informationen finden Sie unter [Überprüfen des Status eines Datenbank-Hochverfügbarkeits-Clusters](#).
- Stellen Sie sicher, dass der fehlgeschlagene primäre Knoten inaktiv ist und keine der folgenden Standby-Knoten enthält, und stufen Sie einen neuen Knoten zum primären Knoten herauf.

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 (Optional) Um sicherzustellen, dass die Voraussetzungen für die Aufhebung der Registrierung des Knotens erfüllt sind, führen Sie den Befehl mit der Option `--dry-run` aus.

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=Knoten-ID --dry-run
```

- 4 Heben Sie die Registrierung des Knotens auf.

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=Knoten-ID
```

Ergebnisse

Durch den Vorgang wird der Knoten aus den repmgr-Metadaten entfernt.

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.

Sie können diesen Befehl während des normalen Systembetriebs ausführen.

Hinweis Damit der primäre Knoten normal funktioniert, muss immer mindestens ein Standby-Knoten ausgeführt werden.

Voraussetzungen

Um die Registrierung eines Standby-Knotens aufzuheben, müssen Sie die Knoten-ID angeben. Um die IP-Adresse zu finden, überprüfen Sie den Status des Clusters und suchen Sie nach dem Knoten. Verwenden Sie in dieser Zeile den Hostwert aus der Spalte „Connection string“, um die IP-Adresse des Knotens zu identifizieren. Weitere Informationen finden Sie unter [Überprüfen des Status eines Datenbank-Hochverfügbarkeits-Clusters](#).

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 Heben Sie die Registrierung des Knotens auf.

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

Ergebnisse

Durch das Aufheben der Registrierung des Knotens wird der Datensatz des Standby-Knotens aus der internen Metadatentabelle der repmgr-Tool-Suite entfernt.

Nach der Installation von vCloud Director oder der Bereitstellung der vCloud Director-Appliance

10

Nach dem Erstellen der vCloud 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.

Dieses Kapitel enthält die folgenden Themen:

- [Installation von Microsoft Sysprep-Dateien auf den Servern](#)
- [Anpassen öffentlicher Endpoints](#)
- [Installieren und Konfigurieren einer RabbitMQ AMQP Broker-Instanz](#)
- [Installieren und Konfigurieren einer Cassandra-Datenbank zum Speichern von historischen Metrikdaten](#)
- [Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank](#)

Installation von Microsoft Sysprep-Dateien auf den Servern

Wenn Ihre Cloud für bestimmte ältere Microsoft-Betriebssysteme Unterstützung für die Anpassung von Gastsystemen benötigt, müssen Sie die entsprechenden Microsoft Sysprep-Dateien auf jedem Mitglied der Servergruppe installieren.

Sysprep-Dateien sind nur für einige ältere Microsoft-Betriebssysteme erforderlich. Wenn Ihre Cloud die Gastanpassung für diese Betriebssysteme nicht unterstützen muss, müssen Sie keine Sysprep-Dateien installieren.

Um die Sysprep-Programmdateien zu installieren, müssen Sie sie an einen bestimmten Speicherort auf dem Server kopieren. Sie müssen die Dateien auf jedes Mitglied der Servergruppe kopieren.

Voraussetzungen

Stellen Sie sicher, dass Sie Zugriff auf die 32- und 64-Bit-Sysprep-Binärdateien für Windows 2003 und Windows XP haben.

Verfahren

- 1 Melden Sie sich beim Zielsystem als **root** an.

- 2 Wechseln Sie in das Verzeichnis `$VCLLOUD_HOME/guestcustomization/default/windows`.

```
[root@cell1 /]# cd /opt/vmware/vcloud-director/guestcustomization/default/windows
```

- 3 Erstellen Sie ein Verzeichnis mit dem Namen `sysprep`.

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep
```

- 4 Erstellen Sie für jedes Gastbetriebssystem, das Sysprep-Programmdateien benötigt, ein Unterverzeichnis von `$VCLLOUD_HOME/guestcustomization/default/windows/sysprep`.

Unterverzeichnisnamen unterscheiden sich je nach Gastbetriebssystem.

Tabelle 10-1. Unterverzeichniszuweisungen für Sysprep-Dateien

Gastbetriebssystem	Unterverzeichnis, das unter <code>\$VCLLOUD_HOME/guestcustomization/default/windows/sysprep</code> zu erstellen ist
Windows 2003 (32-Bit)	svr2003
Windows 2003 (64-Bit)	svr2003-64
Windows XP (32-Bit)	xp
Windows XP (64-Bit)	xp-64

Beispiel: Um ein Unterverzeichnis zum Speichern der Sysprep-Programmdateien für Windows XP zu erstellen, verwenden Sie den folgenden Linux-Befehl:

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep/xp
```

- 5 Kopieren Sie die Sysprep-Programmdateien auf jedem vCloud Director-Server in der Servergruppe an den entsprechenden Speicherort.
- 6 Stellen Sie sicher, dass die Sysprep-Dateien vom Benutzer `vcloud.vcloud` gelesen werden können.

Führen Sie dazu den Linux-Befehl `chown` aus.

```
[root@cell1 /]# chown -R vcloud:vcloud $VCLLOUD_HOME/guestcustomization
```

Ergebnisse

Nachdem die Sysprep-Dateien auf alle Mitglieder der Servergruppe kopiert wurden, können Sie eine Gastanpassung für die virtuellen Maschinen in Ihrer Cloud durchführen. Nach dem Kopieren der Sysprep-Dateien müssen Sie vCloud Director nicht neu starten.

Anpassen öffentlicher Endpoints

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

Wenn Sie die vCloud Director-Appliance bereitgestellt haben, müssen Sie die Adresse des öffentlichen vCloud Director-Konsolen-Proxys konfigurieren, da die Appliance eine einzelne IP-Adresse mit dem benutzerdefinierten Port 8443 für den Konsolen-Proxy-Dienst verwendet. Siehe [Schritt 5](#).

Voraussetzungen

Nur der **Systemadministrator** kann öffentliche Endpoints anpassen.

Verfahren

- 1 Klicken Sie auf die Registerkarte **Administration** und im linken Bereich auf **Öffentliche Adressen**.

- 2 Wählen Sie **Öffentliche Endpunkte anpassen** aus.

Wenn Sie dieses Kontrollkästchen deaktivieren, werden alle Endpoints auf ihre Standardwerte zurückgesetzt, die auf der Seite nicht angezeigt werden.

- 3 Bearbeiten Sie die **API**-Endpoints zum Anpassen der vCloud-REST-API und der OpenAPI-URLs.

- 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 vCloud-API unter **http://vcloud.example.com/api** und auf die vCloud-OpenAPI unter **http://vcloud.example.com/cloudapi** zugreifen.

- b Geben Sie eine benutzerdefinierte Basis-URL und klicken Sie auf **Durchsuchen**, 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 vCloud-API unter **https://vcloud.example.com/api** und auf die vCloud-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 vCloud 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.

- 4 Bearbeiten Sie zum Anpassen der URLs des vCloud Director-Mandantenportals die Endpoints des **Mandantenportals**.
 - Um das vCloud Director-Mandantenportal zur Verwendung derselben Endpoints und derselben Zertifikatskette zu konfigurieren, die Sie in [Schritt 3](#) angegeben haben, wählen Sie **API-URL-Einstellungen kopieren** aus.

- Führen Sie die folgenden Schritte aus, um das vCloud Director-Mandantenportal für die Verwendung unterschiedlicher Endpoints und der Zertifikatskette zu konfigurieren.

a Deaktivieren Sie **API-URL-Einstellungen kopieren**.

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

Wenn Sie die HTTP-Basis-URL beispielsweise auf **http://vcloud.example.com** festlegen, können Sie unter `http://vcloud.example.com/tenant/org_name` auf das Mandantenportal zugreifen.

c Geben Sie eine benutzerdefinierte Basis-URL und klicken Sie auf **Durchsuchen**, um die Zertifikate hochzuladen, die die Vertrauenskette für diesen Endpoint bilden.

Wenn Sie die Basis-URL für die HTTPS-REST-API beispielsweise auf **https://vcloud.example.com** setzen, können Sie unter `https://vcloud.example.com/tenant/org_name` auf das Mandantenportal zugreifen.

Die Zertifikatskette muss mit dem vom Dienst-Endpoint verwendeten Zertifikat übereinstimmen. Hierbei handelt es sich entweder um das Zertifikat, das auf alle vCloud 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.

5 Bearbeiten Sie zum Anpassen der vCloud Director Web Console-URLs und der Adresse des Konsolen-Proxys die Endpoints der **Webkonsole**.

- a Geben Sie eine benutzerdefinierte öffentliche vCloud Director-URL für HTTP-Verbindungen ein.

Die URL muss `/cloud` enthalten.

Wenn Sie die öffentliche vCloud Director-URL beispielsweise auf **`http://vcloud.example.com/cloud`** setzen, können Sie auf die vCloud Director Web Console unter `http://vcloud.example.com/cloud` zugreifen.

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

Die URL muss `/cloud` enthalten.

Wenn Sie die Basis-URL beispielsweise auf **`https://vcloud.example.com`** setzen, können Sie auf die vCloud Director Web Console unter `https://vcloud.example.com/cloud` zugreifen.

Die Zertifikatskette muss mit dem vom Dienst-Endpoint verwendeten Zertifikat übereinstimmen. Hierbei handelt es sich entweder um das Zertifikat, das auf jeden vCloud Director-Zellen-Keystore mit dem Alias **HTTP** hochgeladen wurde, oder, bei Verwendung der SSL-Terminierung, um das VIP-Zertifikat des Lastausgleichsdiensts. Die Zertifikatskette muss ein Endpoint-Zertifikat, Zwischenzertifikate und ein Stammzertifikat im PEM-Format ohne einen privaten Schlüssel enthalten.

- c Geben Sie die Adresse eines benutzerdefinierten öffentlichen vCloud Director-Konsolen-Proxys ein.

Bei dieser Adresse handelt es sich um den vollqualifizierten Domännennamen (FQDN) des vCloud Director-Servers oder Lastausgleichsdiensts mit der Portnummer. Der Standardport ist 443.

Wichtig Die vCloud Director-Appliance verwendet ihre `eth0`-NIC an dem benutzerdefinierten Port 8443 für den Konsolen-Proxy-Dienst.

SSL-Terminierung der Konsolen-Proxy-Verbindungen auf einem Lastausgleichsdienst wird nicht unterstützt. Das Konsolen-Proxy-Zertifikat wird auf jeden vCloud Director Zellen-Keystore mit dem Alias **consoleproxy** hochgeladen.

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

Die vCloud Director-Webkonsole verwendet die Konsolen-Proxy-Adresse beim Öffnen eines Remote-Konsolenfensters auf einer VM.

6 Klicken Sie zum Speichern der Änderungen auf **Anwenden**.

Installieren und Konfigurieren einer RabbitMQ AMQP Broker-Instanz

AMQP, das Advanced Message Queuing Protocol, ist ein offener Standard für Nachrichten-Warteschlangen, der flexible Messaging-Funktionen unterstützt. vCloud Director verwendet RabbitMQ AMQP Broker zum Bereitstellen des Nachrichtenbuses, der von Erweiterungsdiensten, Objekterweiterungen und Benachrichtigungen verwendet wird.

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 *vCloud Director-Versionshinweise*.

- 2 Befolgen Sie die Installationsanweisungen für RabbitMQ und installieren Sie die Software auf einem geeigneten Host.

Der RabbitMQ-Serverhost muss für jede vCloud Director-Zelle im Netzwerk erreichbar sein.

- 3 Notieren Sie sich während der RabbitMQ-Installation folgende Werte, die Sie später beim Konfigurieren von vCloud Director für die Zusammenarbeit mit dieser RabbitMQ-Installation bereitstellen müssen:

- Den vollqualifizierten Domännennamen des RabbitMQ-Serverhosts, zum Beispiel *amqp.example.com*
- Eine zur Authentifizierung mit RabbitMQ gültige Kombination aus Benutzername und Kennwort.
- Den Port, über den der Broker Nachrichten empfängt. Der Standardwert ist 5672.
- Den virtuellen RabbitMQ-Host. Der Standardwert ist `"/`.

Nächste Schritte

Der AMQP-Dienst von vCloud 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 vCloud Director-Zelle verwenden, normalerweise unter `$VCLLOUD_HOME/jre/lib/security/cacerts`.

So aktivieren Sie SSL mit dem AMQP-Dienst von vCloud Director:

- 1 Klicken Sie in der vCloud Director-Webkonsole auf die Registerkarte **Administration** und dann auf **Erweiterbarkeit**.
- 2 Klicken Sie auf **Erweiterbarkeit** und dann auf die Registerkarte **Einstellungen**.
- 3 Wählen Sie im Abschnitt **AMQP Broker-Einstellungen** die Option **SSL verwenden** aus.

4 Aktivieren Sie entweder das Kontrollkästchen **Alle Zertifikate akzeptieren** oder geben Sie Folgendes an:

- den Pfadnamen eines SSL-Zertifikats
- den Pfadnamen und das Kennwort für den JCEKS-Truststore

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

vCloud 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 vCloud 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 vCloud Director verwenden. Für das Abrufen aktueller Metriken ist keine optionale Datenbanksoftware erforderlich.

Voraussetzungen

- Bevor Sie die optionale Datenbanksoftware konfigurieren, stellen Sie sicher, dass vCloud 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 *vCloud 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 vCloud 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 im *vCloud Director-Administratorhandbuch*.

- 2 (Optional) Wenn Sie ein Upgrade von vCloud 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 vCloud Director-Zelle neu.

Durchführen zusätzlicher Konfigurationen in der externen PostgreSQL-Datenbank

Nach dem Erstellen der vCloud Director-Servergruppe können Sie die externe PostgreSQL-Datenbank so konfigurieren, dass SSL-Verbindungen aus den vCloud 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 vCloud 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 vCloud Director und der PostgreSQL-Datenbank.
 - a Wenn Sie ein selbstsigniertes oder privates Zertifikat für die externe PostgreSQL-Datenbank verwendet haben, führen Sie in jeder vCloud Director-Zelle den Befehl zum Importieren des Datenbankzertifikats in den vCloud Director-Truststore aus.

```
[root@cell1 /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 vCloud Director und PostgreSQL aus.

```
[root@cell1 /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@cell1 /opt/vmware/vcloud-director/bin]#  
cell-management-tool reconfigure-database --database-ssl true --private-key-path  
path_to_private_key
```

Informationen zur Verwendung des Zellenverwaltungstools finden Sie im *vCloud Director-Administratorhandbuch*.

- 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 vCloud 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.

Upgrade von vCloud Director und Anwenden von Patches auf die vCloud Director-Appliance

11

Sie können ein orchestriertes Upgrade durchführen, für vCloud Director manuell ein Upgrade auf eine neue Version durchführen oder Patches auf die vCloud Director-Appliance-Bereitstellungen anwenden.

Wenn Ihre vorhandene vCloud Director-Servergruppe aus vCloud Director-Installationen unter Linux besteht, können Sie das vCloud Director-Installationsprogramm für Linux zum Aktualisieren Ihrer Umgebung verwenden. Alternativ können Sie Ihre Umgebung auf die vCloud Director 9.7-Appliance migrieren. Weitere Informationen finden Sie unter [Kapitel 12 Migrieren auf die vCloud Director-Appliance](#).

Wenn Ihre vorhandene vCloud Director-Servergruppe aus Bereitstellungen der vCloud Director 9.5-Appliance besteht, können Sie Ihre Umgebung nur auf die vCloud Director 9.7-Appliance migrieren. Sie verwenden das vCloud Director-Installationsprogramm für Linux, um die vorhandene Umgebung ausschließlich als Teil des Migrations-Workflows zu aktualisieren. Weitere Informationen finden Sie unter [Kapitel 12 Migrieren auf die vCloud Director-Appliance](#).

Sie können entweder [Durchführen eines koordinierten Upgrades einer vCloud Director-Installation](#) oder [Manuelles Upgrade einer vCloud 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 vCloud Director 9.5:

- Oracle-Datenbanken werden nicht unterstützt. Wenn Ihre vorhandene vCloud Director-Installation eine Oracle-Datenbank verwendet, erhalten Sie weitere Informationen unter [Workflow zum Aktualisieren einer vCloud Director-Installation mit einer Oracle-Datenbank](#).
- Das Aktivieren und Deaktivieren von ESXi-Hosts wird nicht unterstützt. Bevor Sie das Upgrade starten, müssen Sie alle ESXi-Hosts aktivieren. Zum Versetzen von ESXi-Hosts in den Wartungsmodus können Sie den vSphere Web Client verwenden.
- vCloud 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>.

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

- Mit der Datenbanksoftware, die Sie derzeit für die vCloud Director-Datenbank verwenden.

Wenn Ihre vorhandene vCloud Director-Installation eine Oracle-Datenbank verwendet, erhalten Sie weitere Informationen unter [Workflow zum Aktualisieren einer vCloud Director-Installation mit einer Oracle-Datenbank](#).

- Mit der derzeit verwendeten VMware vSphere® -Version.
- Mit der derzeit verwendeten VMware NSX®-Version.

Informationen zu den Upgrade-Pfaden und der Kompatibilität von vCloud 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 vCloud Director-Upgrades aktualisieren möchten, erhalten Sie weitere Informationen unter [Kapitel 13 Nach dem Upgrade oder der Migration von vCloud Director](#).

Nach dem Upgrade mindestens eines vCloud Director-Servers können Sie die vCloud Director-Datenbank aktualisieren. In der Datenbank werden Informationen über den Laufzeitstatus des Servers gespeichert. Dazu gehören auch die Status aller vCloud 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 vCloud 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 vCloud 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.

Workflow zum Aktualisieren einer vCloud Director-Installation mit einer Oracle-Datenbank

Vor dem Aktualisieren einer vCloud Director-Installation, die eine Oracle-Datenbank verwendet, müssen Sie die Datenbank von vCloud Director Version 9.1 zu PostgreSQL migrieren.

- 1 Ist die aktuelle vCloud Director-Version älter als 9.1, führen Sie ein Upgrade auf Version 9.1 durch.

Informationen zum Aktualisieren von vCloud Director auf Version 9.1 finden Sie im *Installations-, Konfigurations- und Upgrade-Handbuch zu vCloud Director 9.1*.

- 2 Wenn Sie vCloud Director 9.1 bereits installiert haben, migrieren Sie die Oracle-Datenbank zu einer PostgreSQL-Datenbank.

Informationen über die Migration zu einer PostgreSQL-Datenbank finden Sie in der Referenz zum Zellenverwaltungstool im *vCloud Director-Administratorhandbuch*.

- 3 Führen Sie ein Upgrade Ihrer vCloud Director-Installation von Version 9.1 durch. Sie können entweder die Aufgabe [Durchführen eines koordinierten Upgrades einer vCloud Director-Installation](#) oder die Aufgabe [Manuelles Upgrade einer vCloud Director-Installation](#) durchführen.

Anwenden von Patches auf die vCloud Director-Appliance-Bereitstellung

Sie können Patches auf die vCloud Director-Appliance anwenden, um ihre Funktionalität zu verbessern oder ihre Sicherheit zu verbessern. Weitere Informationen finden Sie im [Patchen der vCloud Director-Appliance-Bereitstellung](#). Nachdem Sie den Patch auf jede vCloud Director-Appliance angewendet haben und das Datenbank-Upgrade abgeschlossen ist, müssen Sie die vCloud Director-Dienste in der Servergruppe neu starten, um sie wieder online zu schalten.

Dieses Kapitel enthält die folgenden Themen:

- [Durchführen eines koordinierten Upgrades einer vCloud Director-Installation](#)
- [Manuelles Upgrade einer vCloud Director-Installation](#)
- [Referenz zum Datenbank-Upgrade-Dienstprogramm](#)
- [Patchen der vCloud Director-Appliance-Bereitstellung](#)

Durchführen eines koordinierten Upgrades einer vCloud Director-Installation

Sie können alle Zellen in der Servergruppe mit der gemeinsam genutzten Datenbank aktualisieren, indem Sie das vCloud Director-Installationsprogramm mit der Option `--private-key-path` ausführen.

Sie können das vCloud Director-Installationsprogramm für Linux zur Aktualisierung einer vCloud Director-Servergruppe verwenden, die aus vCloud Director-Installationen auf einem unterstützten Linux-Betriebssystem besteht. Wenn die vCloud Director-Servergruppe aus Bereitstellungen von vCloud Director 9.5-Appliances besteht, verwenden Sie das vCloud Director-Installationsprogramm für Linux, um die vorhandene Umgebung nur als Teil des Migrations-Workflows zu aktualisieren. Weitere Informationen finden Sie unter [Kapitel 12 Migrieren auf die vCloud Director-Appliance](#).

vCloud Director für Linux wird als digital signierte ausführbare Datei mit einem Namen im Format `vmware-vcloud-director-distribution-v.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 vCloud Director installiert oder aktualisiert.

Wenn Sie das vCloud 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 vCloud Director-Datenbank, die vSphere-Komponenten und die NSX-Komponenten mit der neuen Version von vCloud Director kompatibel sind.

Wichtig Wenn Ihre vorhandene vCloud Director-Installation eine Oracle-Datenbank verwendet, stellen Sie sicher, dass Sie von vCloud Director Version 9.1 zu einer PostgreSQL-Datenbank migriert sind. Weitere Informationen finden Sie unter [Workflow zum Aktualisieren einer vCloud Director-Installation mit einer Oracle-Datenbank](#).

- Überprüfen Sie, ob Sie die für den Zielservers benötigten Superuser-Anmeldeinformationen besitzen.
- Laden Sie den öffentlichen Schlüssel von VMware auf den Zielservers 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 vCloud 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 *vccloud.vccloud* 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 *vccloud*, die Gruppe *vccloud* und das Konto *vccloud.vccloud* werden vom vCloud Director-Installationsprogramm zur Verwendung als Identität erstellt, mit der vCloud Director-Prozesse ausgeführt werden. Der Benutzer *vccloud* hat kein Kennwort.

- Überprüfen Sie, ob alle ESXi-Hosts aktiviert sind. Beginnend mit vCloud Director 9.5 werden deaktivierte ESXi-Hosts 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](#).
- Wenn Ihre vCloud 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@cell1 /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 setzt die Ausführungsberechtigung voraus. 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 vCloud 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 Befehlsoptionen 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 vCloud Director und fordert Sie auf, das Upgrade zu bestätigen.

Wenn das Installationsprogramm eine Version von vCloud 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 vCloud Director-RPM-Paket.
- 3 Es führt ein Upgrade der vCloud Director-Software auf der aktuellen Zelle aus.
- 4 Es aktualisiert die vCloud Director-Datenbank.
- 5 Es aktualisiert vCloud Director-Software in allen verbleibenden Zellen und startet dann vCloud Director-Dienste in der Zelle neu.
- 6 Es startet die vCloud Director-Dienste auf der aktuellen Zelle neu.

Nächste Schritte

Starten Sie die vCloud 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 vCloud Director-Installation

Sie können eine einzelne Zelle durch Ausführen des Installationsprogramms von vCloud 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 vCloud Director-Installationsprogramm für Linux zur Aktualisierung einer vCloud Director-Servergruppe verwenden, die aus vCloud Director-Installationen auf einem unterstützten Linux-Betriebssystem besteht. Wenn die vCloud Director-Servergruppe aus Bereitstellungen von vCloud Director 9.5-Appliances besteht, verwenden Sie das vCloud Director-Installationsprogramm für Linux, um die vorhandene Umgebung nur als Teil des Migrations-Workflows zu aktualisieren. Weitere Informationen finden Sie unter [Kapitel 12 Migrieren auf die vCloud Director-Appliance](#).

Statt die einzelnen Zellen und die Datenbank der Reihe nach manuell zu aktualisieren, können Sie bei einer vCloud Director-Installation mit mehreren Zellen folgendes Verfahren anwenden: [Durchführen eines koordinierten Upgrades einer vCloud Director-Installation](#).

Voraussetzungen

- Vergewissern Sie sich, dass Ihre vCloud Director-Datenbank, die vSphere-Komponenten und die NSX-Komponenten mit der neuen Version von vCloud Director kompatibel sind.

Wichtig Wenn Ihre vorhandene vCloud Director-Installation eine Oracle-Datenbank verwendet, stellen Sie sicher, dass Sie von vCloud Director Version 9.1 zu einer PostgreSQL-Datenbank migriert sind. Weitere Informationen finden Sie unter [Workflow zum Aktualisieren einer vCloud Director-Installation mit einer Oracle-Datenbank](#).

- Vergewissern Sie sich, dass Sie über Superuser-Anmeldeinformationen für die Server in Ihrer vCloud 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 vCloud Director-Software zu verwenden, auf die Sie ein Upgrade durchführen.
- Überprüfen Sie, ob alle ESXi-Hosts aktiviert sind. Beginnend mit vCloud Director 9.5 werden deaktivierte ESXi-Hosts nicht unterstützt.

Verfahren

1 [Upgrade einer vCloud Director-Zelle](#)

Das vCloud Director-Installationsprogramm überprüft, ob der Zielsystem alle Upgrade-Voraussetzungen erfüllt, und aktualisiert die vCloud Director-Software auf dem Server.

2 [Aktualisieren der vCloud Director-Datenbank](#)

Auf einem aktualisierten vCloud Director-Server können Sie ein Tool ausführen, mit dem die vCloud Director-Datenbank aktualisiert wird. Aktualisierte vCloud Director-Server dürfen nicht neu gestartet werden, bevor die gemeinsam genutzte Datenbank aktualisiert wurde.

Nächste Schritte

Nachdem Sie alle vCloud Director-Server in der Servergruppe und die Datenbank aktualisiert haben, können Sie die vCloud Director-Dienste für alle Zellen starten.

Sie können [Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist](#) und anschließend [Upgrade von vCenter Server-Systemen, ESXi-Hosts und NSX Edges](#) .

Upgrade einer vCloud Director-Zelle

Das vCloud Director-Installationsprogramm überprüft, ob der Zielsystem alle Upgrade-Voraussetzungen erfüllt, und aktualisiert die vCloud Director-Software auf dem Server.

vCloud Director für Linux wird als digital signierte ausführbare Datei mit einem Namen im Format `vmware-vcloud-director-distribution-v.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 vCloud Director installiert oder aktualisiert.

Bei einer vCloud Director-Installation mit mehreren Zellen müssen Sie das vCloud Director-Installationsprogramm für jedes Mitglied der vCloud Director-Servergruppe ausführen.

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@cell1 /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 setzt die Ausführungsberechtigung voraus. 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 vCloud Director-Installationsdatei ist.

```
[root@cell1 /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@cell1 /tmp]# ./Installationsdatei
```

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 vCloud 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 vCloud 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 vCloud Director-RPM-Paket.
- c Nachdem alle aktiven vCloud Director-Aufgaben auf der Zelle abgeschlossen sind, beendet es die vCloud Director-Dienste auf dem Server und aktualisiert die installierte vCloud 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 vCloud 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 vCloud Director-Datenbank aktualisieren. Wiederholen Sie diesen Vorgang für jede vCloud Director-Zelle in der Servergruppe.

Wichtig Starten Sie die vCloud Director-Dienste erst, wenn alle Zellen in der Servergruppe und der Datenbank aktualisiert wurden.

Aktualisieren der vCloud Director-Datenbank

Auf einem aktualisierten vCloud Director-Server können Sie ein Tool ausführen, mit dem die vCloud Director-Datenbank aktualisiert wird. Aktualisierte vCloud 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 vCloud 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 vCloud Director-Servergruppe nutzen dieselbe Datenbank. Unabhängig davon, wie viele Zellen Sie aktualisieren, die Datenbank wird nur einmal aktualisiert. Nachdem die Datenbank aktualisiert wurde, können nicht aktualisierte vCloud Director-Zellen keine Verbindung zur Datenbank herstellen. Sie müssen alle Zellen aktualisieren, damit sie eine Verbindung zur aktualisierten Datenbank herstellen können.

Voraussetzungen

- Sichern Sie Ihre vorhandene Datenbank. Gehen Sie dabei nach den Empfehlungen des Datenbanksoftwareherstellers vor.

- Überprüfen Sie, ob alle vCloud Director-Zellen in der Servergruppe beendet wurden. Während des Aktualisierungsvorgangs werden die aktualisierten Zellen beendet. Wenn noch nicht aktualisierte vCloud 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 *vCloud Director-Administratorhandbuch*.
- Wenn in Ihrer vCloud Director-Installation eine Oracle-Datenbank verwendet wird, migrieren Sie zu einer PostgreSQL-Datenbank. Informationen zur Migration zu einer PostgreSQL-Datenbank finden Sie in der Referenz zum Zellenverwaltungstool im *vCloud Director-Administratorhandbuch*.
- Lesen Sie die [Referenz zum Datenbank-Upgrade-Dienstprogramm](#). Die Optionen und Argumente sind nicht obligatorisch.

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 Schritt 1](#).

Ergebnisse

Das Datenbank-Upgrade-Tool wird ausgeführt und zeigt Statusmeldungen an. Wenn das Upgrade abgeschlossen ist, werden Sie aufgefordert, den vCloud 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 vCloud Director-Server starten.

Sie können die restlichen vCloud Director-Mitglieder der Servergruppe aktualisieren und ihre Dienste starten. Weitere Informationen finden Sie unter [Upgrade einer vCloud 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.

Tabelle 11-1. Optionen und Argumente des Datenbank-Upgrade-Dienstprogramms

Option	Argument	Beschreibung
<code>--backup-completed</code>	Keines	Gibt an, dass Sie eine Sicherungskopie von vCloud 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.	Das Upgrade schlägt fehl, wenn ein Benutzer mit diesem Benutzernamen bereits in der Systemorganisation vorhanden ist. Standard: <code>phone-home-system-account</code> .
<code>--enable-ceip</code>	Wählen Sie einen Typ aus: <ul style="list-style-type: none"> ■ <code>true</code> ■ <code>false</code> 	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. Siehe „Zellenverwaltungstool-Referenz“ in <i>vCloud Director Administratorhandbuch</i> .

Tabelle 11-1. Optionen und Argumente des Datenbank-Upgrade-Dienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
--installer-path	Vollständiger Pfadname der vCloud Director-Installationsdatei. Die Installationsdatei und das Verzeichnis, in dem sie gespeichert ist, müssen für den Benutzer „vcloud.vcloud“ lesbar sein.	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. Informationen dazu finden Sie in der „Zellenverwaltungstool-Referenz“ im <i>vCloud Director-Administratorhandbuch</i> . Erfordert die Option --private-key-path .
--maintenance-cell	IP-Adresse	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 --private-key-path .
--multisite-user	Der Benutzername für das Multi-Site-Systemkonto.	Dieses Konto wird von der vCloud Director Multi-Site-Funktion verwendet. Das Upgrade schlägt fehl, wenn ein Benutzer mit diesem Benutzernamen bereits in der Systemorganisation vorhanden ist. Standard: multisite-system-account.

Tabelle 11-1. Optionen und Argumente des Datenbank-Upgrade-Dienstprogramms (Fortsetzung)

Option	Argument	Beschreibung
<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 vCloud 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 vCloud Director-Installationsprogramm zur Verwendung als Identität erstellt, mit der vCloud Director-Prozesse ausgeführt werden. Der Benutzer `vcloud` hat kein Kennwort.

Patchen der vCloud Director-Appliance-Bereitstellung

Sie können die vCloud Director-Appliance mit Patches aktualisieren, die möglicherweise mit Produktfunktionen und Sicherheitsverbesserungen in Zusammenhang stehen.

Während des Patchens der vCloud Director-Appliance-Bereitstellung funktioniert der vCloud Director-Dienst nicht mehr, und es können Ausfälle erwartet werden. Der Ausfall hängt von der Zeit ab, die Sie zum Patchen der einzelnen vCloud Director-Appliances und zum Ausführen des vCloud Director-Datenbank-Upgradeskripts benötigen. Die Anzahl der funktionierenden Zellen in der vCloud Director-Servergruppe wird reduziert, bis Sie den vCloud Director-Dienst auf der letzten vCloud Director-Appliance beenden. Ein ordnungsgemäß konfigurierter Lastausgleichsdienst vor den vCloud Director-HTTP-Endpoints sollte das Routing des Datenverkehrs zu den beendeten Zellen stoppen.

Nachdem Sie den Patch auf jede vCloud Director-Appliance angewendet haben und das Datenbank-Upgrade abgeschlossen ist, müssen Sie die vCloud Director-Dienste in der Servergruppe neu starten, um sie wieder online zu schalten.

Verfahren

- 1 Melden Sie sich in einem Webbrowser bei der Appliance-Verwaltungsbenutzeroberfläche einer vCloud 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 den Namen der primären Appliance beim Upgrade der Datenbank verwenden.

- 2 Laden Sie das Updatepaket in eine Appliance herunter.

vCloud Director wird als ausführbare Datei mit einem Namen im Format `VMware_vCloud_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_vCloud_Director_9.7.0.4248-13560441_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 -zxf VMware_vCloud_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.

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

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

```
vamcli update --check
```

Die Patch-Version wird als verfügbares Update angezeigt.

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

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

- 8 Sichern Sie von der primären Appliance aus die eingebettete Datenbank der vCloud Director-Appliance.

Hinweis Wenn Sie ein Upgrade von vCloud Director 9.7.0.1 auf eine höhere Version durchführen, sichern Sie die Truststore-Datei im Verzeichnis `/opt/vmware/vcloud-director/etc/truststore` manuell.

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

- 9 Wenden Sie den verfügbaren Patch an.

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

- 10 Wiederholen Sie [Schritt 2](#) bis [Schritt 7](#) und [Schritt 9](#) auf jeder Appliance.
- 11 Führen Sie von jeder Appliance aus das vCloud Director-Datenbank-Upgradeskript aus.

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

- 12 Starten Sie die vCloud Director-Dienste auf jeder Appliance.

```
service vmware-vcd start
```

Migrieren auf die vCloud Director-Appliance

12

Ab Version 9.7 enthält die vCloud Director-Appliance eine eingebettete PostgreSQL-Datenbank mit einer Hochverfügbarkeitsfunktion. Sie können Ihre vorhandene vCloud Director-Umgebung einer früheren Version auf eine vCloud Director-Umgebung migrieren, die aus Bereitstellungen der vCloud Director 9.7-Appliance besteht.

Sie können eine vCloud Director-Umgebung migrieren, die aus vCloud Director-Installationen auf Linux oder Bereitstellungen der vCloud Director-Appliance besteht. Sie können eine vCloud Director-Umgebung migrieren, die eine externe Microsoft SQL-Datenbank oder eine externe PostgreSQL-Datenbank verwendet.

Wenn Ihre vCloud Director-Umgebung eine externe Oracle-Datenbank verwendet, müssen Sie vor der Migration auf die vCloud Director-Appliance die Datenbank von vCloud Director Version 9.1 auf PostgreSQL migrieren. Informationen zum Workflow für das Upgrade einer vCloud Director-Installation mit einer Oracle-Datenbank finden Sie unter [Kapitel 11 Upgrade von vCloud Director und Anwenden von Patches auf die vCloud Director-Appliance](#).

Dieses Kapitel enthält die folgenden Themen:

- [Migrieren von vCloud Director mit einer externen Microsoft SQL-Datenbank auf die vCloud Director-Appliance](#)
- [Migrieren von vCloud Director mit einer externen PostgreSQL-Datenbank auf eine vCloud Director-Appliance](#)

Migrieren von vCloud Director mit einer externen Microsoft SQL-Datenbank auf die vCloud Director-Appliance

Wenn Ihre aktuelle vCloud Director-Umgebung einer früheren Version eine externe Microsoft SQL-Datenbank verwendet, können Sie auf eine neue vCloud Director-Umgebung migrieren, die aus Bereitstellungen der vCloud Director 9.7-Appliance besteht. Ihre aktuelle vCloud Director-Umgebung kann aus vCloud Director-Installationen auf Linux oder aus Bereitstellungen der vCloud Director-Appliance bestehen. Die neue vCloud Director-Umgebung kann die eingebetteten PostgreSQL-Datenbanken der Appliance in einem Hochverfügbarkeitsmodus verwenden.

Der Migrations-Workflow umfasst vier Hauptphasen.

- Erstellen der neuen vCloud Director-Servergruppe durch Bereitstellen einer oder mehrerer Instanzen der vCloud Director 9.7-Appliance
- Aktualisieren der vorhandenen vCloud Director-Umgebung
- Migrieren der externen Datenbank auf die eingebettete Datenbank
- Kopieren der gemeinsam genutzten Übertragungsdienst- und Zertifikatsdaten.

Vorgehensweise

- 1 Führen Sie ein Upgrade der aktuellen vCloud Director-Umgebung auf Version 9.7 und ein Upgrade des Quelldatenbankschemas durch.

Weitere Informationen finden Sie unter [Kapitel 11 Upgrade von vCloud Director und Anwenden von Patches auf die vCloud Director-Appliance](#).

- 2 Vergewissern Sie sich, dass der Neustart von vCloud Director der Migrationsquelle erfolgreich ist.
- 3 Wenn die neue vCloud Director-Umgebung die IP-Adressen der vorhandenen Umgebung verwenden soll, ändern Sie die IP-Adressen der vorhandenen Zellen in temporäre IP-Adressen.
- 4 Wenn die neue vCloud 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.

- 5 Erstellen Sie die neue Servergruppe, indem Sie eine oder mehrere Instanzen der vCloud Director 9.7-Appliance bereitstellen.
 - 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 IP-Adressen der vorhandenen Zellen in temporäre IP-Adressen geändert 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 [Kapitel 6 Bereitstellen der vCloud Director-Appliance](#).

- 6 Führen Sie in jeder vorhandenen Zelle und in jeder neu bereitgestellten Zelle den Befehl zum Beenden des vCloud Director-Diensts aus.

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

- 7 Wählen Sie eine der vorhandenen Zellen aus, die als Migrationsquelle dienen soll.

Die Migrationsquelle muss Zugriff auf die eth1-Netzwerk-IP-Adresse der neu bereitgestellten primären Zelle haben.

- 8 Aktivieren Sie in der neuen primären Zelle den Zugriff auf die eingebettete Datenbank über die Migrationsquelle.

Weitere Informationen finden Sie unter [Konfigurieren des externen Zugriffs auf die vCloud Director-Datenbank](#).

- 9 Führen Sie in der Migrationsquelle das Zellenverwaltungstool aus, um die externe Datenbank auf die Datenbank zu migrieren, die in die neue primäre Zelle eingebettet ist.

Die eingebettete Datenbank verwendet die eth1-Netzwerk-IP-Adresse der Appliance.

```
/opt/vmware/vcloud-director/bin/cell-management-tool dbmigrate -dbhost eth1_IP_new_primary \
-dbport 5432 -dbuser vcloud -dbname vcloud -dbpassword database_password_new_primary
```

Informationen zur Verwendung des Zellenverwaltungstools finden Sie im *vCloud Director-Administratorhandbuch*.

- 10 Sichern und ersetzen Sie die Konfigurationsdaten in jeder neu bereitgestellten Zelle, konfigurieren Sie den vCloud Director-Dienst neu und starten Sie ihn.

- a Sichern Sie die Eigenschaften und Zertifikatsdateien und kopieren und ersetzen Sie diese Dateien aus der Migrationsquelle.

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

Wichtig Wenn Sie auf vCloud Director Version 9.7.0.1 oder höher migrieren, müssen Sie zusammen mit den anderen Dateien auch die Truststore-Datei aus der Migrationsquelle sichern, kopieren und ersetzen.

- 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 vCloud 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 --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

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 `--keystore` ist der Pfad zur Datei `certificates.ks`, die Sie in Schritt 10.b gesichert haben.
- 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.

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

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

```
service vmware-vcd start
```

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

- 11 Nachdem alle Zellen der neuen Servergruppe gestartet wurden, stellen Sie sicher, dass die Migration Ihrer vCloud Director-Umgebung erfolgreich verlaufen ist.
 - a Öffnen Sie die vCloud Director Web Console mithilfe der eth0-Netzwerk-IP-Adresse einer beliebigen Zelle aus der neuen Servergruppe, `https://eth0_IP_new_cell/cloud`.
 - b Melden Sie sich bei der vCloud Director Web Console mit den vorhandenen Anmeldedaten für **Systemadministratoren** an.
 - c Stellen Sie sicher, dass Ihre vSphere- und Cloud-Ressourcen in der neuen Umgebung zur Verfügung stehen.
- 12 Verwenden Sie nach erfolgreicher Überprüfung der vCloud Director-Migration die vCloud Director Web Console, um die getrennten Zellen zu löschen, die zur alten vCloud Director-Umgebung gehören.
 - a Klicken Sie auf der Registerkarte **Verwalten und Überwachen** auf **Cloud-Zellen**.
 - b Klicken Sie mit der rechten Maustaste auf den Namen einer Zelle und wählen Sie **Löschen** aus.

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

Weitere Schritte

In der neuen Umgebung der migrierten vCloud 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 vCloud 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.

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

Wenn Ihre aktuelle vCloud Director-Umgebung einer früheren Version eine externe PostgreSQL-Datenbank verwendet, können Sie auf eine neue vCloud Director-Umgebung migrieren, die aus Bereitstellungen der vCloud Director 9.7-Appliance besteht. Ihre aktuelle vCloud Director-Umgebung kann aus vCloud Director-Installationen auf Linux oder aus Bereitstellungen der vCloud Director-Appliance bestehen. Die neue vCloud Director-Umgebung kann die eingebetteten PostgreSQL-Datenbanken der Appliance in einem Hochverfügbarkeitsmodus verwenden.

Der Migrations-Workflow umfasst vier Hauptphasen.

- Aktualisieren der vorhandenen vCloud Director-Umgebung
- Erstellen der neuen vCloud Director-Servergruppe durch Bereitstellen einer oder mehrerer Instanzen der vCloud Director 9.7-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 durch.
- 2 Aktualisieren Sie die aktuelle vCloud Director-Umgebung auf Version 9.7.

Weitere Informationen finden Sie unter [Kapitel 11 Upgrade von vCloud Director und Anwenden von Patches auf die vCloud Director-Appliance](#).

- 3 Vergewissern Sie sich, dass der Neustart von vCloud Director der Migrationsquelle erfolgreich ist.
- 4 Führen Sie in jeder Zelle der aktualisierten vCloud Director-Umgebung den Befehl zum Beenden des vCloud 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 vCloud 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` und `proxycertificates`, die sich unter `/opt/vmware/vcloud-director/etc/` befinden, nach `/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 vCloud 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, indem Sie eine oder mehrere Instanzen der vCloud Director 9.7-Appliance bereitstellen.

- 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 [Kapitel 6 Bereitstellen der vCloud Director-Appliance](#).

- 10 Führen Sie in jeder neu bereitgestellten Zelle den Befehl zum Beenden des vCloud 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 vCloud 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 den Datenbanknamen 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 vCloud 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 vCloud Director-Dienst neu und starten Sie ihn.

- a Sichern Sie die Eigenschaften 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 7a kopiert haben.

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

Wichtig Wenn Sie auf vCloud Director Version 9.7.0.1 oder höher migrieren, müssen Sie zusammen mit den anderen Dateien auch die Truststore-Datei aus der Migrationsquelle sichern, kopieren und ersetzen.

- 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 vCloud 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 --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

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 vCloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der vCloud Director-Appliance fehl](#).

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

```
service vmware-vcd start
```

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

- 15 Nachdem alle Zellen der neuen Servergruppe gestartet wurden, stellen Sie sicher, dass die Migration Ihrer vCloud Director-Umgebung erfolgreich verlaufen ist.
 - a Öffnen Sie die vCloud Director Web Console mithilfe der `eth0`-Netzwerk-IP-Adresse einer beliebigen Zelle aus der neuen Servergruppe, `https://eth0_IP_new_cell/ccloud`.
 - b Melden Sie sich beim vCloud Director Web Console mit den vorhandenen Anmeldedaten für **Systemadministratoren** an.
 - c Stellen Sie sicher, dass Ihre vSphere- und Cloud-Ressourcen in der neuen Umgebung zur Verfügung stehen.
- 16 Verwenden Sie nach erfolgreicher Überprüfung der vCloud Director-Migration die vCloud Director Web Console, um die getrennten Zellen zu löschen, die zur alten vCloud Director-Umgebung gehören.
 - a Klicken Sie auf der Registerkarte **Verwalten und Überwachen** auf **Cloud-Zellen**.
 - b Klicken Sie mit der rechten Maustaste auf den Namen einer Zelle und wählen Sie **Löschen** aus.

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

Weitere Schritte

In der neuen Umgebung der migrierten vCloud 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 vCloud 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 oder der Migration von vCloud Director

13

Nach dem Upgrade oder der Migration aller vCloud 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 vCloud Director-Installation registriert sind.

Wichtig Ab Version 9.7 unterstützt vCloud Director 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>.

Dieses Kapitel enthält die folgenden Themen:

- [Aktualisieren jeder NSX Manager-Instanz, die einem verbundenen vCenter Server-System zugeordnet ist](#)
- [Upgrade von vCenter Server-Systemen, ESXi-Hosts und NSX Edges](#)
- [Neue Rechte in dieser Version](#)

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 vCloud 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 vCloud Director durchgeführt haben. Dies ist unabhängig davon, ob vCloud 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 vCloud 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 vCloud Director und NSX Manager müssen Sie das Upgrade der vCenter Server-Systeme und ESXi-Hosts durchführen, die bei vCloud 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 Klicken Sie in der vCloud Director-Webkonsole auf die Registerkarte **Verwalten und Überwachen** und anschließend im linken Fensterbereich auf **vCenter**.
 - b Klicken Sie mit der rechten Maustaste auf den Namen des zieleseitigen vCenter Server und klicken Sie dann auf **Deaktivieren**.
 - c Klicken Sie auf **Ja**.
- 2 Führen Sie ein Upgrade des vCenter Server-Systems durch.

Informationen dazu finden Sie unter *Upgrade von vCenter Server*.
- 3 Verifizieren Sie alle öffentlichen vCloud Director-URLs und Zertifikatsketten.
 - a Klicken Sie in der vCloud Director-Webkonsole auf die Registerkarte **Administration** und dann im linken Fensterbereich auf **Öffentliche Adressen**.
 - b Überprüfen Sie alle öffentlichen Adressen.
- 4 Aktualisieren Sie die Registrierung von vCenter Server bei vCloud Director.
 - a Klicken Sie in der vCloud Director-Webkonsole auf die Registerkarte **Verwalten und Überwachen** und dann im linken Fensterbereich auf **vCenter**.
 - b Klicken Sie mit der rechten Maustaste auf den Namen des zieleseitigen vCenter Servers und klicken Sie dann auf **Aktualisieren**.
 - c Klicken Sie auf **Ja**.

- 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 vCloud 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>.
- Um vCloud Director für das Upgrade von NSX Edges zu verwenden, müssen Sie das durch das Edge unterstützte vCloud Director-Netzwerkobjekt verwenden:
 - Ein entsprechendes Upgrade eines Edge-Gateways findet automatisch statt, wenn Sie entweder die vCloud Director-Webkonsole oder vCloud-API zum Zurücksetzen eines vom Edge-Gateway bedienten Netzwerks verwenden.
 - Durch das erneute Bereitstellen eines Edge-Gateways wird ein Upgrade der zugeordneten NSX Edge-Appliance durchgeführt.
 - Durch das Zurücksetzen eines vApp-Netzwerks von innerhalb des Kontexts der vApp wird ein Upgrade der diesem Netzwerk zugeordneten NSX Edge-Appliance durchgeführt. Um die vCloud Director-Webkonsole zum Zurücksetzen eines vApp-Netzwerks innerhalb des Kontexts einer vApp zu verwenden, navigieren Sie zur Registerkarte **Netzwerk** der vApp, zeigen Sie deren Netzwerkdetails an, klicken Sie mit der rechten Maustaste auf das vApp-Netzwerk und wählen Sie **Netzwerk zurücksetzen**.

Weitere Informationen zum erneuten Bereitstellen von Edge-Gateways und zum Zurücksetzen von vApp-Netzwerken finden Sie in der Onlinehilfe der vCloud Director-Webkonsole oder im *vCloud API-Programmierhandbuch*.

Nächste Schritte

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

Neue Rechte in dieser Version

vCloud Director 9.7 führt neue Rechte ein, die Sie möglicherweise zu allen vorhandenen globalen Rollen hinzufügen möchten, die Sie für Ihre Mandanten veröffentlicht haben.

Recht	Beschreibung	Standardrolle
SDDC: SDDC anzeigen	Ermöglicht Ihnen, alle SDDCs anzuzeigen, die in Ihrer Organisation veröffentlicht wurden. Der Systemadministrator kann alle SDDCs anzeigen.	Systemadministrator und Organisationsadministrator
SDDC: SDDC verwalten	Ermöglicht Ihnen, SDDCs hinzuzufügen, zu entfernen und zu bearbeiten.	Systemadministrator
SDDC: SDDC-Proxy verwalten	Ermöglicht Ihnen, SDDC-Proxys hinzuzufügen, zu entfernen, zu aktivieren und zu deaktivieren.	Systemadministrator
Dienstanwendungen: Dienstanwendungen anzeigen	Ermöglicht Ihnen, die Liste der registrierten Dienstanwendungen anzuzeigen. Wird für VMC-Konten verwendet.	Systemadministrator
Dienstanwendungen: VMC-SDDC registrieren	Ermöglicht Ihnen, Dienstanwendungen zu erstellen, anzuzeigen, zu bearbeiten und zu entfernen. Wird für VMC-Konten verwendet.	Systemadministrator
Dienstanwendungen: Dienstanwendungen verwalten	Ermöglicht Ihnen, Dienstanwendungen zu registrieren. Wird für VMC-Konten verwendet.	Systemadministrator
Edge-Cluster: Edge-Cluster anzeigen	Ermöglicht Ihnen, eine Liste von Edge-Clustern anzuzeigen und einen einzelnen Edge-Cluster abzurufen.	Systemadministrator und Organisationsadministrator

Recht	Beschreibung	Standardrolle
Edge-Cluster: Edge-Cluster verwalten	Ermöglicht Ihnen, Edge-Cluster zu erstellen, zu bearbeiten und zu entfernen.	Systemadministrator und Organisationsadministrator
vApp: VM-Computing-Richtlinie bearbeiten	Ermöglicht Benutzern die Änderung der Computing-Richtlinie einer virtuellen Maschine.	Systemadministrator , Organisationsadministrator , Katalogautor und vApp-Autor
Gateway: Edge-Gateway importieren	Ermöglicht Ihnen, einen Tier-1-Router als Edge-Gateway zu importieren.	Systemadministrator und Organisationsadministrator

Informationen zum Verwalten von Mandantenrechten und -rollen finden Sie im *vCloud Director Service Provider Admin Portal-Handbuch*.

Fehlerbehebung für die vCloud Director-Appliance

14

Wenn die Bereitstellung der vCloud 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 vCloud Director-Protokollen verwenden. Weitere Informationen zum Erfassen von Diagnoseinformationen für vCloud 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>.

Dieses Kapitel enthält die folgenden Themen:

- [Prüfen der Protokolldateien in der vCloud Director-Appliance](#)
- [Die vCloud Director-Zelle kann nach der Bereitstellung der Appliance nicht gestartet werden](#)
- [Neukonfigurieren des vCloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der vCloud Director-Appliance fehl](#)
- [Verwenden der Protokolldateien zur Fehlerbehebung bei vCloud Director-Updates und -Patches](#)
- [Suchen nach vCloud Director-Updates schlägt fehl](#)
- [Installieren des neuesten Updates von vCloud Director schlägt fehl](#)

Prüfen der Protokolldateien in der vCloud Director-Appliance

Nach der Bereitstellung der vCloud Director-Appliance können Sie die „firstboot“- und Datenbankprotokolle auf Fehler und Warnungen prüfen.

Verfahren

- 1 Melden Sie sich direkt oder mithilfe von SSH bei der Konsole der vCloud 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 vCloud Director-Zelle kann nach der Bereitstellung der Appliance nicht gestartet werden

Sie haben die vCloud Director-Appliance erfolgreich bereitgestellt, aber die vCloud 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 vCloud 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 vCloud 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 Übertragungsdienstspeicher die `responses.properties`-Datei enthalten.

Lösung

- 1** Melden Sie sich direkt oder mithilfe von SSH bei der Konsole der vCloud 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.

Neukonfigurieren des vCloud Director-Diensts schlägt beim Migrieren oder Wiederherstellen auf der vCloud Director-Appliance fehl

Wenn Sie die vCloud Director-Appliance migrieren oder wiederherstellen, schlägt die Ausführung des Befehls `configure` unter Umständen fehl.

Problem

Während der Migration oder Wiederherstellung von vCloud Director in einer neuen Umgebung der vCloud Director-Appliance führen Sie den Befehl `configure` aus, um den vCloud 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.

Verwenden der Protokolldateien zur Fehlerbehebung bei vCloud Director-Updates und -Patches

Sie können die Protokolldateien auf Fehler und Warnungen prüfen, wenn Sie Patches auf die vCloud 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 vCloud 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 vCloud Director-Updates schlägt fehl

Wenn Sie nach Updates der vCloud Director-Appliance suchen, schlägt die Ausführung des Befehls `vamicli update --check` möglicherweise fehl.

Problem

Während der Anwendung eines Patches auf die vCloud 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 vCloud Director schlägt fehl

Wenn Sie die neuesten Updates auf der vCloud Director-Appliance installieren, schlägt die Ausführung des Befehls `vamicli update --install latest` möglicherweise fehl.

Problem

Während der Anwendung eines Patches auf die vCloud 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
```


Deinstallieren der vCloud Director-Software

15

Verwenden Sie den Linux-Befehl `rpm`, um die vCloud 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-phonehome 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 vCloud Director deinstallieren.