

Installations- und Upgradehandbuch zu vCloud Director

vCloud Director 5.5

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter <http://www.vmware.com/de/support/pubs>.

DE-0001030-00

vmware[®]

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

<http://www.vmware.com/de/support/>

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2010–2013 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter <http://www.vmware.com/go/patents-de> aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

VMware, Inc.

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

VMware Global, Inc.

Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

VMware vCloud Director Installations- und Upgrade-Handbuch	5
1 Übersicht über Installation, Konfiguration und Upgrade von vCloud Director	7
vCloud Director -Architektur	7
Konfigurationsplanung	8
vCloud Director-Hardware- und Softwareanforderungen	9
2 Erstellen einer vCloud Director-Servergruppe	25
Installieren und Konfigurieren der vCloud Director -Software auf dem ersten Mitglied einer Servergruppe	26
Konfigurieren der Netzwerk- und Datenbankverbindungen	28
Installieren der vCloud Director-Software auf einem weiteren Mitglied einer Servergruppe	33
Installation von Microsoft Sysprep-Dateien auf den Servern	34
Starten oder Beenden der vCloud Director -Dienste	35
Deinstallieren der vCloud Director -Software	36
3 Aktualisieren von vCloud Director	37
Stilllegen und Herunterfahren eines Servers mithilfe des Zellenverwaltungstools	39
Aktualisieren der vCloud Director -Software auf einem beliebigen Mitglied einer Servergruppe	41
Aktualisieren der vCloud Director -Datenbank	44
Aktualisieren von vShield Manager	46
Aktualisieren von vCenter, Hosts und vShield Edge-Appliances	46
4 vCloud Director -Einrichtung	49
Lesen der Lizenzvereinbarung	50
Eingeben des Lizenzschlüssels	50
Erstellen eines Systemadministratorkontos	50
Angabe der Systemeinstellungen	51
Bereit zur Anmeldung bei vCloud Director	51
5 Überblick über das Zellenverwaltungstool	53
Befehle zum Verwalten von Zellen	54
Befehle zum Exportieren von Datenbanktabellen	55
Befehle zum Ersetzen von SSL-Zertifikaten	58
Befehle zum Generieren selbstsignierter SSL-Zertifikate	58
Wiederherstellen des Kennworts für den Systemadministrator	60
Index	61

VMware vCloud Director Installations- und Upgrade-Handbuch

Das *VMware vCloud Director Installations- und Upgrade-Handbuch* enthält Informationen darüber, wie die VMware vCloud Director-Software installiert oder aktualisiert und so konfiguriert wird, dass sie mit VMware vCenter™ zusammenarbeitet und für VMware vorbereitete VMware vCloud®-Dienste bereitstellt.

Zielgruppe

Das *VMware vCloud Director Installations- und Upgrade-Handbuch* wendet sich an alle Benutzer, die die VMware vCloud Director-Software installieren oder aktualisieren möchten. Die in ihm enthaltenen Informationen wurden für erfahrene Systemadministratoren erstellt, die mit Linux, Windows, IP-Netzwerken und VMware vSphere® vertraut sind.

Übersicht über Installation, Konfiguration und Upgrade von vCloud Director

1

Eine VMware vCloud[®] kombiniert eine vCloud Director-Servergruppe mit der vSphere-Plattform. Sie erstellen eine vCloud Director-Servergruppe, indem Sie die vCloud Director-Software auf einem oder mehreren Servern installieren, die Server mit einer gemeinsam genutzten Datenbank verbinden und die vCloud Director-Servergruppe in vSphere integrieren.

Im Verlauf der Installation wird die Erstkonfiguration von vCloud Director einschließlich Datenbank- und Netzwerkverbindungsdetails eingerichtet. Bei einem Upgrade einer vorhandenen Installation auf eine neue vCloud Director-Version werden die Software und das Datenbankschema von vCloud Director aktualisiert, die bestehenden Beziehungen zwischen Servern, der Datenbank und vSphere werden hingegen beibehalten.

Dieses Kapitel behandelt die folgenden Themen:

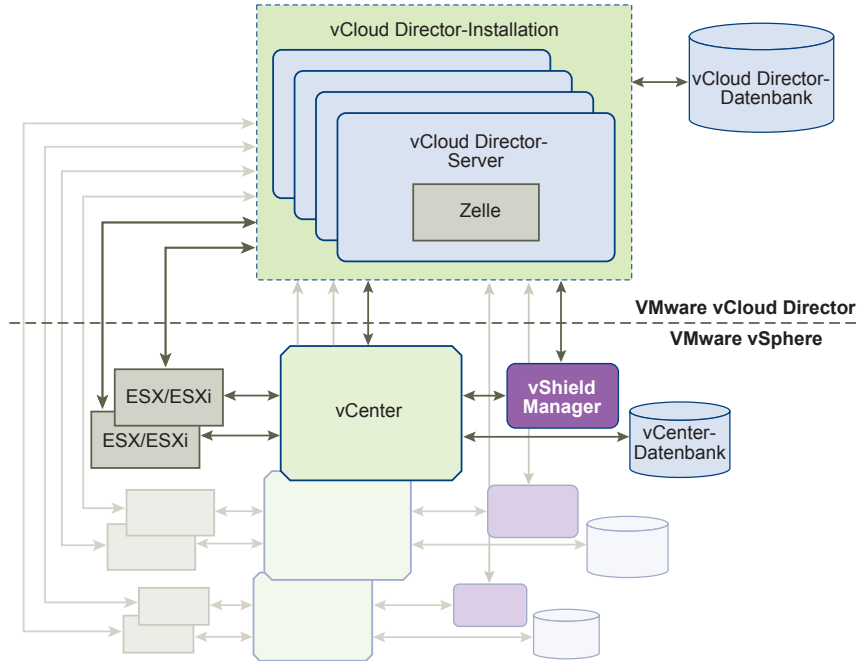
- [„vCloud Director-Architektur“](#), auf Seite 7
- [„Konfigurationsplanung“](#), auf Seite 8
- [„vCloud Director-Hardware- und Softwareanforderungen“](#), auf Seite 9

vCloud Director -Architektur

Eine vCloud Director-Servergruppe besteht aus einem oder mehreren vCloud Director-Servern. Diese Server nutzen eine gemeinsame Datenbank und sind mit einer beliebigen Anzahl von vCenter Servern und ESXi-Hosts verknüpft. vShield Manager-Server bieten vCenter und vCloud Director Netzwerkdienste an.

Bei einer typischen Installation wird eine vCloud Director-Servergruppe erstellt, die aus mehreren Servern besteht. Jeder Server in der Gruppe führt eine Sammlung von Diensten aus, die vCloud Director-Zelle genannt werden. Alle Mitglieder der Gruppe nutzen eine einzelne Datenbank gemeinsam. Jede Zelle in der Gruppe ist mit mehreren vCenter Servern, den von ihnen verwalteten Hosts und den vShield Manager-Servern verbunden, die für die Unterstützung der vCenter Server konfiguriert sind.

Abbildung 1-1. vCloud Director-Architekturdiagramm



Der vCloud Director-Installations- und Konfigurationsvorgang erstellt die Zellen, verbindet sie mit der gemeinsam genutzten Datenbank und stellt die ersten Verbindungen zu einem vCenter Server, vShield Manager und Hosts her. Ein Systemadministrator kann dann mithilfe der vCloud Director-Webkonsole jederzeit weitere vCenter Server, vShield Manager und Hosts zur vCloud Director-Servergruppe hinzufügen.

Konfigurationsplanung

vSphere bietet vCloud Director Speicher-, Rechen- und Netzwerkkapazität. Überlegen Sie vor der Installation, wie viel vSphere- und vCloud Director-Kapazität Sie 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:

- Weisen Sie einen vCloud Director-Server (Zelle) pro vCenter Server zu, auf den der Zugriff in der Cloud ermöglicht werden soll.
- Stellen Sie sicher, dass alle vCloud Director-Server mindestens die für Arbeitsspeicher, CPU und Speicher definierten Mindestanforderungen erfüllen. Eine Aufstellung dieser Anforderungen finden Sie unter „vCloud Director-Hardware- und Softwareanforderungen“, auf Seite 9.
- Konfigurieren Sie die vCloud Director-Datenbank gemäß Beschreibung unter „Installieren und Konfigurieren einer vCloud Director-Datenbank“, auf Seite 15.

vCloud Director-Hardware- und Softwareanforderungen

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 einen vCenter Server, vShield Manager und einen oder mehrere ESX/ESXi-Hosts.

Unterstützte Plattformen

Aktuelle Informationen über die VMware-Plattformen, die von dieser Version von vCloud Director unterstützt werden, finden Sie in den *VMware-Produktinteroperabilitätstabellen* unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Konfigurationsanforderungen für vSphere

Server und Hosts, die mit vCloud Director verwendet werden sollen, müssen bestimmte Konfigurationsanforderungen erfüllen.

- vCenter-Netzwerke, die als externe vCloud Director-Netzwerke oder Netzwerkpools verwendet werden sollen, müssen für alle Hosts in einem Cluster verfügbar sein, der von vCloud Director verwendet werden soll. Wenn diese Netzwerke für alle Hosts in einem Datacenter verfügbar gemacht werden, wird die Aufgabe, neue vCenter Server zu vCloud Director hinzuzufügen, vereinfacht.
- vSphere Distributed Switches müssen zum hostübergreifenden Fencing und zur Netzwerkpoolzuweisung verwendet werden.
- vCenter-Cluster, die mit vCloud Director verwendet werden, müssen Speicher-DRS mit der Automatisierungsebene [**Voll automatisiert**] konfigurieren. Diese Konfiguration setzt voraus, dass gemeinsam genutzter Speicher an alle ESXi-Hosts in einem DRS-Cluster angefügt wurde. vCloud Director kann Speicher-DRS vollständig nutzen, einschließlich der Unterstützung von Fast Provisioning mit vCenter 5.1 oder höher.
- vCenter Server 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*.

Lizenzierungsanforderungen für vSphere

vCloud Director erfordert folgende vSphere-Lizenzen:

- VMware DRS, von vSphere Enterprise und Enterprise Plus lizenziert
- VMware Distributed Switch und dvFilter, lizenziert von vSphere Enterprise Plus Diese Lizenz ermöglicht die Erstellung und Nutzung von vCloud Director-isolierten Netzwerken.

Unterstützte vCloud Director -Server-Betriebssysteme

Tabelle 1-1. Unterstützte vCloud Director -Server-Betriebssysteme

Betriebssystem (nur 64-Bit)	Aktualisierungen
CentOS 6	4
Red Hat Enterprise Linux 5	4-9
Red Hat Enterprise Linux 6	1-4

Speicherplatzanforderungen

Jeder vCloud Director -Server setzt ungefähr 1350 MB freien Speicherplatz für die Installations- und Protokolldateien voraus.

Arbeitsspeicheranforderungen

Jeder vCloud Director-Server muss mit mindestens 4GB Arbeitsspeicher bereitgestellt werden.

Linux-Softwarepakete

Jeder vCloud Director-Server muss Installationen mehrerer häufig verwendeter Linux-Softwarepakete enthalten. Diese Pakete werden meist standardmäßig mit der Betriebssystemsoftware installiert. Wenn Pakete fehlen, schlägt das Installationsprogramm mit einer Diagnosemeldung fehl.

Tabelle 1-2. Erforderliche Softwarepakete

Paketname	Paketname	Paketname
alsa-lib	libICE	module-init-tools
bash	libSM	net-tools
chkconfig	libstdc	pciutils
coreutils	libX11	procps
findutils	libXau	redhat-lsb
glibc	libXdmcp	sed
grep	libXext	tar
initscripts	libXi	which
krb5-libs	libXt	
libgcc	libXtst	

Unterstützte vCloud Director -Datenbanken

vCloud Director unterstützt Oracle- und Microsoft SQL Server-Datenbanken. Aktuelle Informationen zu unterstützten Datenbanken finden Sie in den *Matrizen zur VMware-Produktinteroperabilität* unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Informationen über empfohlene Datenbankserverkonfigurationen erhalten Sie unter „[Installieren und Konfigurieren einer vCloud Director-Datenbank](#)“, auf Seite 15.

Unterstützte LDAP-Server

Tabelle 1-3. Unterstützte LDAP-Server

Plattform	LDAP-Server	Authentifizierungsmethoden
Windows Server 2003	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Windows Server 2008	Active Directory	Simple

Tabelle 1-3. Unterstützte LDAP-Server (Fortsetzung)

Plattform	LDAP-Server	Authentifizierungsmethoden
Windows 7 (2008 R2)	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Linux	OpenLDAP	Simple, Simple SSL

Gastbetriebssystem-Unterstützung

Im *vCloud Director-Benutzerhandbuch* finden Sie eine Liste der unterstützten Gastbetriebssysteme.

Von vCloud Director unterstützte Webbrowser

Die vCloud Director-Webkonsole ist mit neuen Versionen von Mozilla Firefox und Microsoft Internet Explorer kompatibel.

HINWEIS Die vCloud Director-Webkonsole ist nur mit 32-Bit-Webbrowsern kompatibel. Ist bei einem Webbrowser die Unterstützung auf einer 64-Bit-Plattform angegeben, bezieht sich dies implizit auf die Verwendung eines 32-Bit-Browsers auf der 64-Bit-Plattform.

Browser-Unterstützung auf Linux-Plattformen

Auf diesen Linux-Plattformen ist die vCloud Director-Webkonsole mit der neuesten Version von Mozilla Firefox und Google Chrome und deren unmittelbaren Vorgängerversionen kompatibel.

Tabelle 1-4. Webbrowserunterstützung und Betriebssystemkompatibilität auf Linux-Plattformen

Plattform	Google Chrome	Mozilla Firefox
CentOS 6.x	JA	JA
Red Hat Enterprise Linux 6.x	JA	JA
Ubuntu 12.x	JA	JA

Browser-Unterstützung auf Windows-Plattformen

Auf Windows-Plattformen ist die vCloud Director-Webkonsole mit mindestens einer Version von Microsoft Internet Explorer kompatibel. Einige Windows-Plattformen sind auch mit der aktuellsten Version von Mozilla Firefox und Google Chrome und deren unmittelbaren Vorgängerversionen kompatibel.

Tabelle 1-5. Webbrowserunterstützung und Betriebssystemkompatibilität auf Microsoft Windows-Plattformen

Plattform	Google Chrome	Mozilla Firefox	Internet Explorer 8.x	Internet Explorer 9.x	Internet Explorer 10.x
Windows XP Pro	JA	JA	JA	Nein	Nein
Windows Server 2003, Enterprise Edition	JA	JA	JA	Nein	Nein
Windows Server 2008	JA	JA	JA	JA	JA
Windows Server 2008 R2	JA	JA	JA	JA	JA
Windows Vista	JA	Nein	JA	JA	JA
Windows 7	JA	JA	JA	JA	JA
Windows 8	JA	JA	Nein	Nein	JA

Browser-Unterstützung auf Macintosh-Plattformen

Auf Macintosh-Plattformen ist die vCloud Director-Webkonsole mit der neuesten Version von Mozilla Firefox und Google Chrome und deren unmittelbaren Vorgängerversionen kompatibel.

Unterstützte Versionen von Adobe Flash Player

Für die vCloud Director-Webkonsole ist Adobe Flash Player Version 11.2 oder höher erforderlich. Es wird nur die 32-Bit-Version unterstützt.

Unterstützte Java-Versionen

Auf vCloud Director-Clients muss JRE 1.6.0 Update 10 oder höher installiert und aktiviert sein. Es wird nur die 32-Bit-Version unterstützt.

Unterstützte TLS- und SSL-Protokollversionen und Verschlüsselungssammlungen

vCloud Director setzt voraus, dass Clients SSL verwenden. Die folgenden SSL-Serverprotokolle werden unterstützt:

- TLS-Versionen 1.0, 1.1 und 1.2
- SSL-Version 3

Verschlüsselungssammlungen, die unterstützt werden, sind solche mit RSA-, DSS- oder 'Elliptische Kurve'-Signaturen sowie DES3-, AES-128- oder AES-256-Verschlüsselung.

Zusammenfassung der 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, das vCloud Director-Server, den Datenbankserver, vCenter Server und vCloud Networking and Security verbindet, muss mehrere Anforderungen erfüllen:

IP-Adressen

Jeder vCloud Director-Server benötigt zwei IP-Adressen, damit er zwei verschiedene SSL-Verbindungen unterstützen kann. Eine Verbindung ist für den HTTP-Dienst bestimmt. Die andere ist für den Konsolen-Proxy-Dienst erforderlich. Sie können diese Adressen mithilfe von IP-Aliasen oder mehreren Netzwerkschnittstellen erstellen. Sie können die zweite Adresse jedoch nicht mithilfe des Linux-Befehls `ip addr add` erstellen.

Proxy-Adresse der Konsole

Die als Proxy-Adresse der Konsole konfigurierte IP-Adresse darf nicht auf eine Position hinter einem SSL-terminierenden Lastenausgleichsmodul oder einem Reverse-Proxy verweisen. Alle Anforderungen an den Konsolen-Proxy müssen direkt an die IP-Adresse des Konsolen-Proxys weitergeleitet werden.

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.

Serverzeitzone

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

Auflösung der Hostnamen

Alle von Ihnen während der Installation und Konfiguration angegebenen Hostnamen müssen von DNS mithilfe eines Forward- und Reverse-Lookups des vollqualifizierten Domänennamens 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
```

Übertragungsserverspeicher

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. Dieses gemeinsam genutzte Volume benötigt die Schreibberechtigung für „Root“. Jedes Mitglied der Servergruppe muss dieses Volume unter dem gleichen Einrichtungspunkt mounten, in der Regel `/opt/vmware/vcloud-director/data/transfer`. Der Speicher auf diesem Volume wird auf zwei Arten genutzt:

- Übertragungen (Uploads und Downloads) belegen diesen Speicher während der Übertragung und werden nach Abschluss der Übertragung 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 das Zwischenspeichern von veröffentlichten Inhalten ermöglichen, belegen diesen Speicher, so lange sie bestehen. (Objekte von Katalogen, die extern veröffentlicht werden, aber keine Zwischenspeicherung ermöglichen, belegen diesen Speicher nicht.) Wenn Sie Organisationen in Ihrer Cloud die Erstellung von extern veröffentlichten Katalogen ermöglichen, ist zu erwarten, dass hunderte oder sogar tausende Katalogobjekte Speicherplatz auf diesem Volume benötigen und jeder Katalog die Größe einer virtuellen Maschine in komprimiertem OVF-Format haben wird.

HINWEIS Wenn möglich, sollte die Kapazität des Volumens, das Sie für die Übertragung von Serverspeicher verwenden, leicht zu erweitern sein.

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. Der gesamte übrige eingehende Datenverkehr aus einem öffentlichen Netzwerk muss von der Firewall zurückgewiesen werden.

Tabelle 1-6. 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	ActiveMQ
61616	TCP	ActiveMQ

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

Tabelle 1-7. 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-, vShield Manager- und ESX-Verbindungen
514	UDP	Optional. Aktiviert die syslog-Verwendung.
902	TCP	vCenter- und ESX-Verbindungen.
903	TCP	vCenter- und ESX-Verbindungen.
920	TCP, UDP	NFS rpc.statd, vom Übertragungsdienst verwendet.
1433	TCP	Microsoft SQL Server-Standarddatenbankport.
1521	TCP	Oracle-Standarddatenbankport.
5672	TCP, UDP	Optional. AMQP-Meldungen für Aufgabenerweiterungen.
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

- Leiten Sie Datenverkehr zwischen vCloud Director-Servern und dem vCloud Director-Datenbankserver nach Möglichkeit über ein dediziertes privates Netzwerk.
- Virtuelle Switches und Distributed Virtual Switches, die Provider-Netzwerke unterstützen, müssen voneinander isoliert sein. Sie können das physische Netzwerksegment auf Ebene 2 nicht gemeinsam nutzen.

Installieren und Konfigurieren einer vCloud Director -Datenbank

vCloud Director-Zellen speichern gemeinsam genutzte Informationen in einer Datenbank. Diese Datenbank muss vorhanden sein, bevor Sie die Installation und Konfiguration der vCloud Director-Software durchführen können.

HINWEIS Unabhängig davon, welche Datenbanksoftware Sie wählen, müssen Sie ein separates, dediziertes Datenbankschema erstellen, das von vCloud Director verwendet wird. vCloud Director kann ein Datenbankschema nicht mit einem anderen VMware-Produkt gemeinsam nutzen.

Konfigurieren einer Oracle-Datenbank

Oracle-Datenbanken haben spezifische Konfigurationsanforderungen, wenn sie mit vCloud Director eingesetzt werden. Installieren und konfigurieren Sie eine Datenbankinstanz und erstellen Sie das vCloud Director-Datenbankbenutzerkonto, bevor Sie vCloud Director installieren.

Vorgehensweise

- 1 Konfigurieren Sie den Datenbankserver.

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

- 2 Erstellen Sie die Datenbankinstanz.

Erstellen Sie mithilfe von Befehlen im folgenden Format separate Daten- (CLOUD_DATA) und Index-Tablespaces (CLOUD_INDX):

```
Create Tablespace CLOUD_DATA datafile '$ORACLE_HOME/oradata/cloud_data01.dbf' size 1000M autoextend on;
```

```
Create Tablespace CLOUD_INDX datafile '$ORACLE_HOME/oradata/cloud_indx01.dbf' size 500M autoextend on;
```

- 3 Erstellen Sie das vCloud Director-Datenbankbenutzerkonto.

Der folgende Befehl erstellt einen Datenbankbenutzer mit dem Namen vcloud und dem Kennwort vcloudpass.

```
Create user $vcloud identified by $vcloudpass default tablespace CLOUD_DATA;
```

HINWEIS Wenn Sie das vCloud Director-Datenbankbenutzerkonto erstellen, müssen Sie CLOUD_DATA als Standard-Tablespace angeben.

- 4 Konfigurieren Sie die Datenbankverbindungs-, Prozess- und Transaktionsparameter.

Die Datenbank muss so konfiguriert werden, dass mindestens 75 Verbindungen pro vCloud Director-Zelle sowie ca. 50 weitere, die von Oracle selbst genutzt werden, verfügbar sind. Sie können auf der Grundlage der Anzahl der Verbindungen Werte für andere Konfigurationsparameter abrufen, wobei C die Anzahl der Zellen im vCloud Director-Cluster darstellt.

Oracle-Konfigurationsparameter	Wert für C Zellen
CONNECTIONS	75*C+50
PROCESSES	= CONNECTIONS

Oracle-Konfigurationsparameter	Wert für C Zellen
SESSIONS	= PROCESSES*1.1+5
TRANSACTIONS	= SESSIONS*1.1
OPEN_CURSORS	= SESSIONS

- 5 Erstellen Sie das vCloud Director-Datenbankbenutzerkonto.

Verwenden Sie das Oracle-Systemkonto nicht als vCloud Director-Datenbankbenutzerkonto. Sie müssen ein eigenes Benutzerkonto speziell für diesen Zweck erstellen. Gewähren Sie dem Konto die folgenden Systemberechtigungen:

- CONNECT
- RESOURCE
- CREATE TRIGGER
- CREATE TYPE
- CREATE VIEW
- CREATE MATERIALIZED VIEW
- CREATE PROCEDURE
- CREATE SEQUENCE

- 6 Notieren Sie sich den Datenbankdienstnamen, damit Sie ihn beim Konfigurieren der Netzwerk- und Datenbankverbindungen verwenden können.

Sie erhalten den Datenbankdienstnamen, indem Sie die Datei `$ORACLE_HOME/network/admin/tnsnames.ora` auf dem Datenbankserver öffnen und einen im folgenden Format vorliegenden Eintrag suchen:

```
(SERVICE_NAME = orcl.example.com)
```

Konfigurieren einer Microsoft SQL Server-Datenbank

SQL Server-Datenbanken haben spezifische Konfigurationsanforderungen, wenn sie mit vCloud Director eingesetzt werden. Installieren und konfigurieren Sie eine Datenbankinstanz, und erstellen Sie das vCloud Director-Datenbankbenutzerkonto, bevor Sie vCloud Director installieren.

Die Leistung der vCloud Director-Datenbank ist ein wichtiger Faktor für die Gesamtleistung und Skalierbarkeit von vCloud Director. vCloud Director verwendet zur Speicherung großer Resultsets 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>.

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.

Vorgehensweise

- 1 Konfigurieren Sie den Datenbankserver.

Ein mit 16 GB Arbeitsspeicher, 100 GB Speicher und 4 CPUs konfigurierter Datenbankserver sollte für die meisten vCloud Director-Cluster 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 [vcloud] for LOGIN [vcloud]
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 [vcloud]
GO
sp_addrolemember [db_owner], [vcloud]
GO
```

Erstellen von SSL-Zertifikaten

vCloud Director benötigt SSL, um die Kommunikation zwischen Clients und Servern zu schützen. Bevor Sie eine vCloud Director-Servergruppe installieren und konfigurieren, müssen Sie für jedes Mitglied der Gruppe zwei Zertifikate erstellen und diese in Host-Keystores importieren.

Jeder vCloud Director-Server benötigt zwei IP-Adressen, damit er zwei verschiedene SSL-Endpunkte unterstützen kann. Jeder Server benötigt zwei SSL-Zertifikate: eines für jeden SSL-Endpunkt.

HINWEIS Alle Verzeichnisse im Pfadnamen für die SSL-Zertifikate müssen für den Benutzer `vcloud.vcloud` lesbar sein. Dieser Benutzer wird vom vCloud Director-Installationsprogramm erstellt.

Vorgehensweise

- 1 Listen Sie die IP-Adressen für diesen Server auf.

Verwenden Sie einen Befehl wie `ifconfig` zur Erkennung der IP-Adressen dieses Servers.

- 2 Führen Sie für jede IP-Adresse den folgenden Befehl aus, um den vollqualifizierten Domännennamen abzurufen, an den die IP-Adresse gebunden ist.

```
nslookup ip-address
```

- 3 Notieren Sie sich die einzelnen IP-Adressen und den zugehörigen vollqualifizierten Domännennamen, und schreiben Sie ebenfalls auf, ob vCloud Director die Adresse für den HTTP-Dienst oder den Konsolen-Proxy-Dienst verwenden soll.

Sie benötigen die vollqualifizierten Domännennamen zum Erstellen der Zertifikate und die IP-Adressen zum Konfigurieren der Netzwerk- und der Datenbankverbindungen.

- 4 Erstellen Sie die Zertifikate.

Sie können von einer vertrauenswürdigen Zertifizierungsstelle signierte Zertifikate oder selbstsignierte Zertifikate verwenden. Signierte Zertifikate bieten die höchste Vertrauensebene. Eine Schlüssellänge von 2.048 Bit bietet einen hohen Grad an Sicherheit.

Erstellen und Importieren eines signierten SSL-Zertifikats

Signierte Zertifikate bieten die höchste Vertrauensebene für die SSL-Kommunikation.

Für jeden vCloud Director-Server werden zwei SSL-Zertifikate in einer Java-Keystore-Datei benötigt, eines pro IP-Adresse. Sie müssen für jeden Server, den Sie in der vCloud Director-Servergruppe verwenden möchten, zwei SSL-Zertifikate erstellen. Sie können von einer vertrauenswürdigen Zertifizierungsstelle signierte Zertifikate oder selbstsignierte Zertifikate verwenden. Signierte Zertifikate bieten die höchste Vertrauensebene.

Informationen darüber, wie Sie selbstsignierte Zertifikate erstellen und importieren, erhalten Sie unter [„Erstellen eines selbstsignierten SSL-Zertifikats“](#), auf Seite 21.

Voraussetzungen

- Generieren Sie eine Liste vollqualifizierter Domännennamen und der zugehörigen IP-Adressen auf diesem Server sowie eine Dienstwahl für jede IP-Adresse. Weitere Informationen erhalten Sie unter [„Erstellen von SSL-Zertifikaten“](#), auf Seite 18.

- Stellen Sie sicher, dass Sie Zugriff auf einen Computer haben, auf dem Version 6 der Java-Laufzeitumgebung installiert ist, damit Sie das Zertifikat mithilfe des Befehls `keytool` erstellen 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 Version 6 der Java-Laufzeitumgebung installiert ist. Die Verwendung von Zertifikaten, die mit einem `keytool` aus einer anderen Quelle erstellt wurden, wird für vCloud Director nicht unterstützt. Indem Sie die Zertifikate erstellen und importieren, bevor Sie die vCloud Director-Software installieren und konfigurieren, vereinfachen Sie den Installations- und Konfigurationsvorgang. Diese Befehlszeilenbeispiele setzen voraus, dass `keytool` im Pfad des Benutzers enthalten ist. Das Keystore-Kennwort wird in diesen Beispielen wie folgt dargestellt: `passwd`.

Vorgehensweise

- 1 Erstellen Sie ein nicht vertrauenswürdiges Zertifikat für den HTTP-Dienst.

Mit diesem Befehl wird ein nicht vertrauenswürdiges Zertifikat in einer Keystore-Datei namens `certificates.ks` erstellt.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -alias http
```

Das Zertifikat ist 90 Tage gültig.

- 2 Beantworten Sie die `keytool`-Fragen.

Wenn `keytool` Sie nach Ihrem Vor- und Nachnamen fragt, wählen Sie die IP-Adresse, die Sie für den HTTP-Dienst verwenden möchten, und geben Sie den mit dieser IP-Adresse verbundenen vollqualifizierten Domännennamen ein.

- 3 Beantworten Sie die übrigen Fragen entsprechend Ihrer Organisation und Ihrem Standort. Siehe folgendes Beispiel.

```
What is your first and last name? [Unknown]:mycloud.example.com
What is the name of your organizational unit? [Unknown]:Engineering
What is the name of your organization? [Unknown]:Example Corporation
What is the name of your City or Locality? [Unknown]:Palo Alto
What is the name of your State or Province? [Unknown]:California
What is the two-letter country code for this unit? [Unknown]:US
Is CN=mycloud.example.com, OU=Engineering, O="Example Corporation", L="Palo Alto", ST=California, C=US correct?[no]:yes
Enter key password for <http> (RETURN if same as keystore password):
```

- 4 Erstellen Sie eine Zertifikatsignieranforderung für den HTTP-Dienst.

Mit diesem Befehl wird eine Zertifikatsignieranforderung in der Datei `http.csr` erstellt.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -certreq -alias http -file http.csr
```

- 5 Erstellen Sie ein nicht vertrauenswürdiges Zertifikat für den Konsolen-Proxy-Dienst.

Mit diesem Befehl wird ein nicht vertrauenswürdiges Zertifikat zu der Keystore-Datei hinzugefügt, die hier erstellt wurde: [Schritt 1](#).

```
keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -alias consoleproxy
```

Das Zertifikat ist 90 Tage gültig.

- 6 Wenn `keytool` Sie nach Ihrem Vor- und Nachnamen fragt, wählen Sie die IP-Adresse, die Sie für den Konsolen-Proxy-Dienst verwenden möchten, und geben Sie den mit dieser IP-Adresse verbundenen vollqualifizierten Domännennamen ein.

- 7 Beantworten Sie die übrigen Fragen entsprechend Ihrer Organisation und Ihrem Standort. Siehe folgendes Beispiel: [Schritt 3](#).

- 8 Erstellen Sie eine Zertifikatsignieranforderung für den Konsolen-Proxy-Dienst.

Mit diesem Befehl wird eine Zertifikatsignieranforderung in der Datei `consoleproxy.csr` erstellt.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -certreq -alias consoleproxy -file consoleproxy.csr
```

- 9 Senden Sie die Zertifikatsignieranforderungen an die Zertifizierungsstelle.

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

- 10 Nachdem Sie die signierten Zertifikate erhalten haben, importieren Sie sie in die Keystore-Datei.

- a Importieren Sie das Stammzertifikat der Zertifizierungsstelle in die Keystore-Datei.

Mit diesem Befehl wird das Stammzertifikat aus der Datei `root.cer` in die Keystore-Datei `certificates.ks` importiert.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias root -file root.cer
```

- b (Optional) Wenn Sie Zwischenzertifikate erhalten haben, importieren Sie sie in die Keystore-Datei.

Mit diesem Befehl werden Zwischenzertifikate aus der Datei `intermediate.cer` in die Keystore-Datei `certificates.ks` importiert.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias intermediate -file intermediate.cer
```

- c Importieren Sie das Zertifikat für den HTTP-Dienst.

Mit diesem Befehl wird das Zertifikat aus der Datei `http.cer` in die Keystore-Datei `certificates.ks` importiert.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias http -file http.cer
```

- d Importieren Sie das Zertifikat für den Konsolen-Proxy-Dienst.

Mit diesem Befehl wird das Zertifikat aus der Datei `consoleproxy.cer` in die Keystore-Datei `certificates.ks` importiert.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias consoleproxy -file consoleproxy.cer
```

- 11 Um zu überprüfen, ob alle Zertifikate importiert wurden, listen Sie den Inhalt der Keystore-Datei auf.

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

- 12 Wiederholen Sie die Schritte [Schritt 1](#) bis [Schritt 11](#) auf allen übrigen vCloud Director-Servern.

Weiter

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. Weitere Informationen erhalten Sie unter „[Konfigurieren der Netzwerk- und Datenbankverbindungen](#)“, auf Seite 28.

HINWEIS Da das vCloud Director-Konfigurationsskript nicht mit einer privilegierten Identität ausgeführt wird, müssen die Keystore-Datei und das Verzeichnis, in dem sie gespeichert ist, von jedem Benutzer gelesen werden können.

Erstellen eines selbstsignierten SSL-Zertifikats

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

Für jeden vCloud Director-Server werden zwei SSL-Zertifikate in einer Java-Keystore-Datei benötigt, eines pro IP-Adresse. Sie müssen für jeden Server, den Sie in der vCloud Director-Servergruppe verwenden möchten, zwei SSL-Zertifikate erstellen. Sie können von einer vertrauenswürdigen Zertifizierungsstelle signierte Zertifikate oder selbstsignierte Zertifikate verwenden. Signierte Zertifikate bieten die höchste Vertrauensebene.

Informationen über das Erstellen und Importieren signierter Zertifikate erhalten Sie unter „[Erstellen und Importieren eines signierten SSL-Zertifikats](#)“, auf Seite 18.

Voraussetzungen

- Generieren Sie eine Liste vollqualifizierter Domännennamen und der zugehörigen IP-Adressen auf diesem Server sowie eine Dienstwahl für jede IP-Adresse. Weitere Informationen erhalten Sie unter „[Erstellen von SSL-Zertifikaten](#)“, auf Seite 18.
- Stellen Sie sicher, dass Sie Zugriff auf einen Computer haben, auf dem Version 6 der Java-Laufzeitumgebung installiert ist, damit Sie das Zertifikat mithilfe des Befehls `keytool` erstellen 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 Version 6 der Java-Laufzeitumgebung installiert ist. Die Verwendung von Zertifikaten, die mit einem `keytool` aus einer anderen Quelle erstellt wurden, wird für vCloud Director nicht unterstützt. Indem Sie die Zertifikate erstellen und importieren, bevor Sie die vCloud Director-Software installieren und konfigurieren, vereinfachen Sie den Installations- und Konfigurationsvorgang. Diese Befehlszeilenbeispiele setzen voraus, dass `keytool` im Pfad des Benutzers enthalten ist. Das Keystore-Kennwort wird in diesen Beispielen wie folgt dargestellt: *passwd*.

Vorgehensweise

- 1 Erstellen Sie ein nicht vertrauenswürdiges Zertifikat für den HTTP-Dienst.

Mit diesem Befehl wird ein nicht vertrauenswürdiges Zertifikat in einer Keystore-Datei namens `certificates.ks` erstellt.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -alias http
```

- 2 Erstellen Sie ein nicht vertrauenswürdiges Zertifikat für den Konsolen-Proxy-Dienst.

Mit diesem Befehl wird ein nicht vertrauenswürdiges Zertifikat zu der Keystore-Datei hinzugefügt, die hier erstellt wurde: [Schritt 1](#).

```
keytool -keystore certificates.ks -storetype JCEKS -storepass passwd -genkey -keyalg RSA -alias consoleproxy
```

Das Zertifikat ist 90 Tage gültig.

- 3 Um zu überprüfen, ob alle Zertifikate importiert wurden, listen Sie den Inhalt der Keystore-Datei auf.

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

- 4 Wiederholen Sie die Schritte [Schritt 1](#) bis [Schritt 3](#) auf allen übrigen vCloud Director-Servern.

Weiter

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. Weitere Informationen erhalten Sie unter „[Konfigurieren der Netzwerk- und Datenbankverbindungen](#)“, auf Seite 28.

HINWEIS Da das vCloud Director-Konfigurationsskript nicht mit einer privilegierten Identität ausgeführt wird, müssen die Keystore-Datei und das Verzeichnis, in dem sie gespeichert ist, von jedem Benutzer gelesen werden können.

Installieren und Konfigurieren von vShield Manager

vCloud Director benötigt vShield Manager, um Netzwerkdienste für die Cloud bereitzustellen. Installieren und konfigurieren Sie vShield Manager, bevor Sie mit der Installation von vCloud Director beginnen. vShield Manager ist im Download VMware vCloud Networking and Security enthalten.

Sie müssen jeden vCenter Server, den Sie zu vCloud Director hinzufügen, mit einer eindeutigen Instanz von vShield Manager verknüpfen. Informationen über die Netzwerkanforderungen und die unterstützten Versionen von vShield Manager erhalten Sie unter „[vCloud Director-Hardware- und Softwareanforderungen](#)“, auf Seite 9.

WICHTIG Das hier beschriebene Verfahren gilt nur für Neuinstallationen von vCloud Director. Wenn Sie eine vorhandene Installation von vCloud Director aktualisieren, können Sie optional die mit ihr verknüpfte vShield Manager-Installation aktualisieren. Eine neue Version von vShield Manager kann nicht mit einer bestehenden Version von vCloud Director zusammenarbeiten. Weitere Informationen erhalten Sie unter „[Aktualisieren von vShield Manager](#)“, auf Seite 46.

Voraussetzungen

Weitere Informationen über vShield Manager finden Sie im VMware vCloud Networking and Security-Dokumentationscenter unter https://www.vmware.com/support/pubs/vshield_pubs.html.

Vorgehensweise

- 1 Melden Sie sich über den vSphere Client beim vCenter Server an.
 - 2 Wählen Sie **[Datei] > [OVF-Vorlage bereitstellen]** aus.
 - 3 Navigieren Sie zum Speicherort der Datei `vShield Manager.ovf` und befolgen Sie die Eingabeaufforderungen zur Bereitstellung der OVF-Datei.
 - 4 Schalten Sie nach der Bereitstellung der OVF-Datei die virtuelle Maschine von vShield Manager ein und öffnen Sie die Konsole.
 - 5 Melden Sie sich mit dem Benutzernamen **admin** und dem Kennwort **default**. bei der Konsole an.
 - 6 Wenn die Eingabeaufforderung `manager` angezeigt wird, geben Sie **enable** ein.
 - 7 Geben Sie in der Password-Eingabeaufforderung den Text **default** ein, um den Setupmodus zu aktivieren.
- Wenn der Setupmodus aktiviert ist, wird die Zeichenfolge der Eingabeaufforderung in `manager#` geändert.
- 8 Geben Sie nach der Eingabeaufforderung `manager#` **setup** ein, um den Setupvorgang zu starten.
 - 9 Geben Sie die IP-Adresse, die Subnetzmaske und das Standard-Gateway der virtuellen Maschine von vShield Manager ein.

Sie benötigen diese Informationen zum Anfügen einer vCenter Server-Instanz zu Cloud Director.

- 10 Geben Sie **exit** ein, um sich abzumelden.
- 11 Schließen Sie die Konsole, und lassen Sie die virtuelle Maschine ausführen.
- 12 Synchronisieren Sie vShield Manager mit vCenter und registrieren Sie vShield Manager als ein vSphere-Client-Plug-In.

Folgen Sie den Anweisungen zum *Anmelden bei der vShield Manager-Benutzeroberfläche* und zum *Einrichten von vShield Manager* im *vShield Installations- und Upgrade-Handbuch*.

Weiter

Konfigurieren Sie die VXLAN-Unterstützung in vShield Manager. vCloud Director erstellt VXLAN-Netzwerkpools, um Netzwerkressourcen für Anbieter-VDCs bereitzustellen. Wenn die VXLAN-Unterstützung nicht in vShield 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 *vShield-Administratorhandbuch*.

Installieren und Konfigurieren eines AMQP-Brokers

AMQP (Advanced Message Queuing Protocol) bezeichnet einen offenen Standard für warteschlangenbasierte Kommunikation über Nachrichten, der flexibles Messaging für Unternehmenssysteme unterstützt. vCloud Director schließt einen AMQP-Dienst ein, den Sie für das Zusammenspiel mit einem AMQP-Broker, beispielsweise RabbitMQ, konfigurieren können, sodass Cloud-Betreiber mit einem Strom von Nachrichten zu Ereignissen innerhalb der Cloud versorgt werden. Um diesen Dienst nutzen zu können, müssen Sie einen AMQP-Broker installieren und konfigurieren.

Während die Verwendung eines AMQP Brokers mit vCloud Director optional ist, verwenden einige Integrationen AMQP für die Kommunikation mit vCloud Director. In der Dokumentation zur Installation und Konfiguration finden Sie weitere Hinweise zu Installationen, die Sie möglicherweise nutzen möchten.

Vorgehensweise

- 1 Laden Sie den RabbitMQ-Server von http://info.vmware.com/content/12834_rabbitmq herunter.
- 2 Befolgen Sie die Installationsanweisungen für RabbitMQ, um die Software auf einem geeigneten Host zu installieren.

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

Weiter

Der AMQP-Dienst von vCloud Director versendet standardmäßig unverschlüsselte Nachrichten. Wenn Sie den Dienst für die Verschlüsselung dieser Nachrichten mithilfe von SSL konfigurieren, überprüft dieser das Zertifikat des Brokers unter Verwendung des standardmäßigen JCEKS-Truststore der Java-Laufzeitumgebung auf dem vCloud Director-Server. Die Java-Laufzeitumgebung befindet sich in der Regel im Verzeichnis `$JRE_HOME/lib/security/cacerts`.

Um SSL in Verbindung mit dem AMQP-Dienst von vCloud Director zu verwenden, müssen Sie die Option **[SSL verwenden]** im Abschnitt AMQP Broker-Einstellungen auf der Seite Erweiterbarkeit der vCloud Director-Webkonsole auswählen und eine der beiden folgenden Angaben machen:

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

Wenn Sie das AMQP Broker-Zertifikat nicht prüfen müssen, können Sie **[Alle Zertifikate akzeptieren]** auswählen.

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.

Die digitale Signatur der vCloud Director-Installationsdatei oder einer anderen, von `vmware.com` heruntergeladenen signierten Datei kann mithilfe des Linux-Tools `rpm` und des öffentlichen Schlüssels von VMware überprüft werden. 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 Dateiinhalt mit dem auf der Website bereitgestellten Inhalt identisch ist. Sie liefert keine Aussage über die Gültigkeit der digitalen Signatur.

Vorgehensweise

- 1 Laden Sie die öffentlichen Schlüssel für VMware-Pakete herunter und importieren Sie sie.
 - a Erstellen Sie ein Verzeichnis zur Speicherung der öffentlichen Schlüssel für VMware-Pakete.
 - b Laden Sie unter Verwendung eines Webbrowsers alle öffentlichen Schlüssel für VMware-Pakete aus dem Verzeichnis <http://packages.vmware.com/tools/keys> herunter.
 - c Speichern Sie die Schlüsseldateien in dem von Ihnen erstellten Verzeichnis.
 - d 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.

- 2 (Optional) Überprüfen Sie die Gültigkeit der digitalen Signatur der heruntergeladenen Datei mithilfe des Linux-Tools `rpm`.

```
# rpm --checksig installation-file
```

Nachdem Sie die Gültigkeit der digitalen Signatur der Datei überprüft haben, können Sie die Datei zur Installation oder Aktualisierung von vCloud Director auf einem beliebigen Server verwenden, ohne den öffentlichen Schlüssel auf diesem Server installieren zu müssen. Das Installationsprogramm gibt eine Warnung aus, wenn kein Schlüssel installiert ist. Sie können diese Warnung ignorieren, wenn Sie die Signatur der Datei bereits überprüft haben.

Erstellen einer vCloud Director-Servergruppe

2

Eine vCloud Director-Servergruppe besteht aus einem oder mehreren vCloud Director-Servern, die eine gemeinsame Datenbank und andere Konfigurationsdetails teilen. Installieren und konfigurieren Sie für die Erstellung einer Servergruppe die vCloud Director-Software auf dem ersten Mitglied der Gruppe. Durch die Installation und Konfiguration des ersten Mitglieds der Gruppe wird eine Antwortdatei erstellt, mithilfe der Sie weitere Mitglieder der Gruppe konfigurieren können.

Voraussetzungen für das Erstellen einer vCloud Director-Servergruppe

WICHTIG Dieses Verfahren ist nur für Neuinstallationen bestimmt. Eine Beschreibung des entsprechenden Verfahrens für die Aktualisierung einer vorhandenen vCloud Director-Installation finden Sie unter [Kapitel 3, „Aktualisieren von vCloud Director“](#), auf Seite 37

Bevor Sie vCloud Director installieren und konfigurieren, führen Sie die folgenden Aufgaben durch.

- 1 Überprüfen Sie, ob ein unterstützter vCenter Server ausgeführt wird und ordnungsgemäß für den Einsatz mit vCloud Director konfiguriert ist. Eine Liste der unterstützten Versionen und Konfigurationsanforderungen finden Sie unter [„Unterstützte Plattformen“](#), auf Seite 9.
- 2 Überprüfen Sie, ob ein unterstützter vShield Manager-Server ausgeführt wird und ordnungsgemäß für den Einsatz mit vCloud Director konfiguriert ist. Eine Liste der unterstützten Versionen finden Sie unter [„Unterstützte Plattformen“](#), auf Seite 9. Einzelheiten zur Installation und Konfiguration finden Sie unter [„Installieren und Konfigurieren von vShield Manager“](#), auf Seite 22.
- 3 Überprüfen Sie, ob mindestens eine unterstützte vCloud Director-Serverplattform ausgeführt wird und mit der ausreichenden Arbeitsspeicher- und Speicherkapazität konfiguriert ist. Eine Liste der unterstützten Plattformen und Konfigurationsanforderungen finden Sie unter [„Unterstützte vCloud Director-Server-Betriebssysteme“](#), auf Seite 10.
 - Jedes Mitglied einer Servergruppe benötigt zwei IP-Adressen, eine zur Unterstützung einer SSL-Verbindung für den HTTP-Dienst und eine zweite für den Konsolen-Proxy-Dienst.
 - Jeder Server muss ein SSL-Zertifikat pro IP-Adresse besitzen. Alle Verzeichnisse im Pfadnamen für die SSL-Zertifikate müssen für alle Benutzer lesbar sein. Weitere Informationen erhalten Sie unter [„Erstellen von SSL-Zertifikaten“](#), auf Seite 18.
 - Jeder Server muss für den Übertragungsdienst ein NFS-Volume oder ein anderes gemeinsam genutztes Speicher-Volume unter `/opt/vmware/vcloud-director/data/transfer` einbinden. Dieses Volume benötigt die Schreibberechtigung für "Root". Weitere Informationen erhalten Sie unter [„Zusammenfassung der Netzwerkkonfigurationsanforderungen für vCloud Director“](#), auf Seite 12.
 - Jeder Server sollte Zugriff auf ein Microsoft Sysprep-Bereitstellungspaket haben. Weitere Informationen erhalten Sie unter [„Installation von Microsoft Sysprep-Dateien auf den Servern“](#), auf Seite 34.

- 4 Überprüfen Sie, ob eine vCloud Director-Datenbank erstellt wurde und ob alle Server in der Gruppe auf sie zugreifen können. Eine Liste der unterstützten Datenbanksoftware finden Sie unter [„Unterstützte vCloud Director-Datenbanken“](#), auf Seite 10.
 - Überprüfen Sie, ob Sie ein Datenbankkonto für den vCloud Director-Datenbankbenutzer erstellt haben und das Konto über alle erforderlichen Datenbankrechte verfügt. Weitere Informationen erhalten Sie unter [„Installieren und Konfigurieren einer vCloud Director-Datenbank“](#), auf Seite 15.
 - Überprüfen Sie, ob der Datenbankdienst beim Neustart des Datenbankservers gestartet wird.
- 5 Überprüfen Sie, ob alle vCloud Director-Server, der Datenbankserver und alle vCenter Server und vShield Manager-Server die Namen der jeweils anderen auflösen können. Siehe Beschreibung unter [„Zusammenfassung der Netzwerkkonfigurationsanforderungen für vCloud Director“](#), auf Seite 12.
- 6 Überprüfen Sie, ob alle vCloud Director-Server und der Datenbankserver mit einem Netzwerkzeitserver mit den in [„Zusammenfassung der Netzwerkkonfigurationsanforderungen für vCloud Director“](#), auf Seite 12 angegebenen Toleranzen synchronisiert sind.
- 7 Wenn Sie Benutzer oder Gruppen von einem LDAP-Dienst importieren möchten, überprüfen Sie, ob alle vCloud Director-Server auf diesen Dienst zugreifen können.
- 8 Öffnen Sie die Firewall-Ports gemäß der Beschreibung in [„Empfehlungen für die Netzwerksicherheit“](#), auf Seite 14. Port 443 muss zwischen vCloud Director und vCenter Server offen sein.

Dieses Kapitel behandelt die folgenden Themen:

- [„Installieren und Konfigurieren der vCloud Director-Software auf dem ersten Mitglied einer Servergruppe“](#), auf Seite 26
- [„Konfigurieren der Netzwerk- und Datenbankverbindungen“](#), auf Seite 28
- [„Installieren der vCloud Director-Software auf einem weiteren Mitglied einer Servergruppe“](#), auf Seite 33
- [„Installation von Microsoft Sysprep-Dateien auf den Servern“](#), auf Seite 34
- [„Starten oder Beenden der vCloud Director-Dienste“](#), auf Seite 35
- [„Deinstallieren der vCloud Director-Software“](#), auf Seite 36

Installieren und Konfigurieren der vCloud Director -Software auf dem ersten Mitglied einer Servergruppe

Alle vCloud Director-Mitglieder teilen die Datenbankverbindung und andere Konfigurationsdetails, die Sie bei der Installation und Konfiguration des ersten Mitglieds der Gruppe angeben. Diese Informationen werden in einer Antwortdatei festgehalten, die Sie beim Hinzufügen von Mitgliedern zu der Gruppe verwenden müssen.

Die vCloud Director-Software wird als digital signierte ausführbare Linux-Datei namens `vmware-vcloud-director-5.5.0-nnnnnn.bin` bereitgestellt, wobei *nnnnnn* eine Buildnummer darstellt.

Das vCloud Director-Installationsprogramm überprüft, ob der Zielsystem alle Voraussetzungen für die Plattform erfüllt, und installiert dann die vCloud Director-Software auf diesem Server. Nach der Installation der Software auf dem Zielsystem müssen Sie ein Skript ausführen, das die Netzwerk- und Datenbankverbindungen des Servers konfiguriert. Dieses Skript erstellt eine Antwortdatei, die Sie bei der Konfiguration weiterer Mitglieder dieser Servergruppe verwenden müssen.

Voraussetzungen

- Überprüfen Sie, ob der Zielsystem und das Netzwerk, zu dem dieser eine Verbindung herstellt, die folgenden Anforderungen erfüllen: [„Zusammenfassung der Netzwerkkonfigurationsanforderungen für vCloud Director“](#), auf Seite 12.

- Überprüfen Sie, ob Sie die für den Zielsystem benötigten Superuser-Anmeldeinformationen besitzen.
- Stellen Sie sicher, dass der Zielsystem das gemeinsam genutzte Übertragungsdienstspeicher-Volumen unter `/opt/vmware/vcloud-director/data/transfer` einbindet.
- Laden Sie den öffentlichen Schlüssel von VMware auf den Zielsystem herunter und installieren Sie ihn, damit das Installationsprogramm die digitale Signatur der Installationsdatei überprüft. Wenn Sie die digitale Signatur der Installationsdatei bereits überprüft haben, müssen Sie sie nicht erneut während der Installation überprüfen. Weitere Informationen erhalten Sie unter „[Herunterladen und Installieren des öffentlichen Schlüssels von VMware](#)“, auf Seite 24.

Vorgehensweise

- 1 Melden Sie sich beim Zielsystem als Root an.

- 2 Laden Sie die Installationsdatei auf den Zielsystem herunter.

Wenn Sie die Software auf CD oder einem anderen Medium gekauft haben, kopieren Sie die Installationsdatei an einen Speicherplatz, auf den alle Zielsystem zugreifen können.

- 3 Überprüfen Sie, ob die Prüfsumme der heruntergeladenen Datei mit der auf der Download-Seite 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 Download-Seite übereinstimmt. Mit einem Linux-Befehl im folgenden Format wird die Prüfsumme für *installation-file* unter Verwendung des von der Download-Seite kopierten MD5-Prüfsummenwerts *checksum-value* überprüft.

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

- 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 in einem Konsolen-, Shell- oder Terminalfenster aus.

Um die Installationsdatei auszuführen, geben Sie ihren vollständigen Pfadnamen ein, z. B.:

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

Diese Datei enthält ein Installationskript und ein eingebettetes RPM-Paket.

HINWEIS Sie können die Installationsdatei nicht von einem Verzeichnis ausführen, dessen Pfadname Leerzeichen einschließt.

Wenn Sie den öffentlichen Schlüssel von VMware nicht auf dem Zielsystem installiert haben, gibt das Installationsprogramm eine Warnung der folgenden Art aus.

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

Das Installationsprogramm führt bei Ausführung folgende Aktionen durch:

- a überprüft, ob der Host alle Anforderungen erfüllt
- b verifiziert die digitale Signatur auf der Installationsdatei
- c erstellt den/die vcloud-Nutzer/-Gruppe
- d entpackt das vCloud Director-RPM-Paket

e installiert die Software

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

Weiter

Geben Sie an, ob das Konfigurationsskript ausgeführt werden soll.

- Wenn Sie die unter „[Voraussetzungen für das Erstellen einer vCloud Director-Servergruppe](#)“, auf Seite 25 aufgeführten Voraussetzungen erfüllt haben, können Sie das Konfigurationsskript jetzt ausführen. Geben Sie **y** ein, und drücken Sie die Eingabetaste.
- Wenn Sie noch nicht bereit sind, das Konfigurationsskript auszuführen, geben Sie **n** ein und drücken Sie die Eingabetaste, um die Shell zu beenden.

Weitere Informationen über die Ausführung des Konfigurationsskripts erhalten Sie unter „[Konfigurieren der Netzwerk- und Datenbankverbindungen](#)“, auf Seite 28.

Konfigurieren der Netzwerk- und Datenbankverbindungen

Nach der Installation der vCloud Director-Software auf dem Server werden Sie vom Installationsprogramm aufgefordert, ein Skript auszuführen, das die Netzwerk- und Datenbankverbindungen des Servers konfiguriert.

Sie müssen die vCloud Director-Software auf dem Server installieren, damit Sie das Konfigurationsskript ausführen können. Das Installationsprogramm fordert Sie auf, das Skript nach Abschluss der Installation auszuführen. Sie können es jedoch auch später ausführen.

Um das Skript nach der Installation der vCloud Director-Software auszuführen, melden Sie sich als "root" an, öffnen Sie ein Konsolen-, Shell- oder Terminalfenster und geben Sie Folgendes ein:

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

Das Konfigurationsskript erstellt Netzwerk- und Datenbankverbindungen für einen einzelnen vCloud Director-Server. Außerdem erstellt das Skript eine Antwortdatei, in der Datenbankverbindungsinformationen für spätere Serverinstallationen aufbewahrt werden.

HINWEIS Nach der Ausführung des Konfigurationsskripts zur Konfiguration des ersten Mitglieds der Servergruppe müssen Sie die Option `-r` verwenden und den Pfadnamen der Antwortdatei angeben, wenn Sie zusätzliche Mitglieder der Gruppe konfigurieren. Weitere Informationen erhalten Sie unter „[Schützen und Wiederverwenden der Antwortdatei](#)“, auf Seite 32.

Voraussetzungen

- Überprüfen Sie, ob vom vCloud Director-Server aus auf eine Datenbank eines unterstützten Typs zugegriffen werden kann. Weitere Informationen erhalten Sie unter „[Installieren und Konfigurieren einer vCloud Director-Datenbank](#)“, auf Seite 15 und „[vCloud Director-Hardware- und Softwareanforderungen](#)“, auf Seite 9.
- Sie müssen die folgenden Informationen bereithalten:
 - Ort und Kennwort der Keystore-Datei, die die SSL-Zertifikate für diesen Server enthält. Weitere Informationen erhalten Sie unter „[Erstellen und Importieren eines signierten SSL-Zertifikats](#)“, auf Seite 18. Da das Konfigurationsskript nicht mit einer privilegierten Identität ausgeführt wird, müssen die Keystore-Datei und das Verzeichnis, in denen es gespeichert ist, von jedem Benutzer gelesen werden können.
 - Kennwort für die einzelnen SSL-Zertifikate.
 - Hostname oder IP-Adresse des Datenbankservers.
 - Datenbankname und Verbindungsport.

- Datenbank-Benutzeranmeldeinformationen (Benutzername und Kennwort). Dieser Benutzer muss spezifische Datenbankrechte haben. Weitere Informationen erhalten Sie unter „[Installieren und Konfigurieren einer vCloud Director-Datenbank](#)“, auf Seite 15.

Vorgehensweise

- 1 Geben Sie die IP-Adressen an, die für die auf diesem Host ausgeführten HTTP- und Konsolen-Proxy-Dienste verwendet werden sollen.

Für jedes Mitglied einer Servergruppe werden zwei IP-Adressen benötigt, damit zwei verschiedene SSL-Verbindungen unterstützt werden können: eine für den HTTP-Dienst und eine andere für den Konsolen-Proxy-Dienst. Um mit dem Konfigurationsvorgang zu beginnen, geben Sie an, welche der vom Skript erkannten IP-Adressen für die einzelnen Dienste verwendet werden sollen.

```
Please indicate which IP address available on this machine should be used
for the HTTP service and which IP address should be used for the remote console proxy.
```

```
The HTTP service IP address is used for accessing the user interface and the REST API.
The remote console proxy IP address is used for all remote console (VMRC) connections
and traffic.
```

```
Please enter your choice for the HTTP service IP address:
```

```
1: 10.17.118.158
```

```
2: 10.17.118.159
```

```
Choice [default=1]:2
```

```
Please enter your choice for the remote console proxy IP address
```

```
1: 10.17.118.158
```

```
Choice [default=1]:
```

- 2 Geben Sie den vollständigen Pfad zu der Java-Keystore-Datei an.

```
Please enter the path to the Java keystore containing your SSL certificates and
private keys:/opt/keystore/certificates.ks
```

- 3 Geben Sie das Keystore- und das Zertifikatkennwort ein.

```
Please enter the password for the keystore:
```

```
Please enter the private key password for the 'http' SSL certificate:
```

```
Please enter the private key password for the 'consoleproxy' SSL certificate:
```

4 Konfigurieren Sie die Optionen der Überwachungsmeldungsbehandlung.

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.

Option	Aktion
So protokollieren Sie Überwachungsmeldungen in syslog und in der vCloud Director-Datenbank.	Geben Sie den syslog-Hostnamen oder die IP-Adresse ein.
Überwachungsmeldungen nur in der vCloud Director-Datenbank protokollieren	Drücken Sie die Eingabetaste.

If you would like to enable remote audit logging to a syslog host please enter the hostname or IP address of the syslog server. Audit logs are stored by vCloud Director for 90 days. Exporting logs via syslog will enable you to preserve them for as long as necessary.

Syslog host name or IP address [press Enter to skip]:**10.150.10.10**

5 Geben Sie den Port an, an dem der syslog-Prozess den angegebenen Server überwacht.

Die Standardeinstellung ist Port 514.

What UDP port is the remote syslog server listening on? The standard syslog port is 514. [default=514]:
Using default value "514" for syslog port.

6 Geben Sie den Datenbanktyp an, oder drücken Sie die Eingabetaste, um den Standardwert zu übernehmen.

The following database types are supported:

1. Oracle
2. Microsoft SQL Server

Enter the database type [default=1]:
Using default value "1" for database type.

7 Geben Sie die Datenbankverbindungsinformationen an.

Die vom Skript benötigten Informationen richten Sie nach der Wahl des Datenbanktyps. In diesem Beispiel werden die Eingabeaufforderungen veranschaulicht, die bei Angabe einer Oracle-Datenbank angezeigt werden. Eingabeaufforderungen für andere Datenbanktypen sind ähnlich.

a Geben Sie den Hostnamen oder die IP-Adresse des Datenbankservers ein.

Enter the host (or IP address) for the database:**10.150.10.78**

b Geben Sie den Datenbankport ein, oder drücken Sie die Eingabetaste, um den Standardwert zu übernehmen.

Enter the database port [default=1521]:
Using default value "1521" for port.

- c Geben Sie den Datenbankdienstnamen ein.

Enter the database service name [default=oracle]:**orcl.example.com**

Wenn Sie die Eingabetaste drücken, verwendet das Konfigurationsskript einen Standardwert, der jedoch eventuell für einige Installationen nicht korrekt ist. Informationen darüber, wie Sie den Datenbankdienstnamen für eine Oracle-Datenbank finden, erhalten Sie unter [„Konfigurieren einer Oracle-Datenbank“](#), auf Seite 15.

- d Geben Sie den Benutzernamen und das Kennwort für die Datenbank ein.

Enter the database username:**vcld**

Enter the database password:

Das Skript prüft die von Ihnen bereitgestellten Informationen und führt anschließend drei weitere Schritte aus.

- 1 Es initialisiert die Datenbank und verbindet den Server mit ihr.
- 2 Es bietet an, die vCloud Director-Dienste auf diesem Host zu starten.
- 3 Es zeigt eine URL an, über die Sie eine Verbindung zum Setup-Assistenten herstellen können, nachdem der vCloud Director-Dienst gestartet wurde.

Das folgende Fragment veranschaulicht einen typischen Ablauf des Skripts.

```
Connecting to the database: jdbc:oracle:thin:vcld/vcld@10.150.10.78:1521/vcld
```

```
.....
```

```
Database configuration complete.
```

```
Once the vCloud Director server has been started you will be able to
access the first-time setup wizard at this URL:
```

```
http://vcld.example.com
```

```
Would you like to start the vCloud Director service now? If you choose not
to start it now, you can manually start it at any time using this command:
```

```
service vmware-vcd start
```

```
Start it now? [y/n]:y
```

```
Starting the vCloud Director service (this may take a moment).
```

```
The service was started; it may be several minutes before it is ready for use.
```

```
Please check the logs for complete details.
```

```
vCloud Director configuration is now complete. Exiting...
```

Weiter

HINWEIS Datenbankverbindungsinformationen und andere wiederverwendbare Antworten, die Sie während der Konfiguration angegeben haben, werden in einer Datei 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 weitere Server zu einer Servergruppe hinzufügen. Speichern Sie die Datei an einem sicheren Ort und stellen Sie sie nur bei Bedarf zur Verfügung.

Informationen darüber, wie Sie weitere Server zu dieser Gruppe hinzufügen, erhalten Sie unter [„Installieren der vCloud Director-Software auf einem weiteren Mitglied einer Servergruppe“](#), auf Seite 33.

Wenn die vCloud Director-Dienste auf allen Servern ausgeführt werden, können Sie den Setup-Assistenten über die URL öffnen, die bei Beendigung des Skripts angezeigt wird. Weitere Informationen erhalten Sie unter [Kapitel 4, „vCloud Director-Einrichtung“](#), auf Seite 49.

Schützen und Wiederverwenden der Antwortdatei

Die von Ihnen beim Konfigurieren des ersten vCloud Director-Servers angegebenen Netzwerk- und Datenbankverbindungsdetails werden in einer Antwortdatei gespeichert. Diese Datei enthält vertrauliche Informationen, die Sie wiederverwenden müssen, wenn Sie weitere Server zu einer Servergruppe hinzufügen. Speichern Sie die Datei an einem sicheren Ort und stellen Sie sie nur bei Bedarf zur Verfügung.

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 weitere Server zu der Gruppe hinzufügen, müssen Sie mithilfe einer Kopie der Antwortdatei Konfigurationsparameter zur Verfügung stellen, die alle Server gemeinsam nutzen.

Vorgehensweise

- 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 diese 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
```

Weiter

Nachdem Sie die zusätzlichen Server konfiguriert haben, löschen Sie die Kopie der Antwortdatei, mit der Sie sie konfiguriert haben.

Installieren der vCloud Director-Software 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 verwendet haben, damit diese Informationen für die Konfiguration weiterer Mitglieder zur Verfügung steht.

Voraussetzungen

- Stellen Sie sicher, dass Sie Zugriff auf die Antwortdatei haben, die bei der Installation und Konfiguration des ersten Mitglieds dieser Servergruppe erstellt wurde. Weitere Informationen erhalten Sie unter [„Schützen und Wiederverwenden der Antwortdatei“](#), auf Seite 32.
- Stellen Sie sicher, dass von diesem Server auf die vCloud Director-Datenbank zugegriffen werden kann.
- Stellen Sie sicher, dass die SSL-Zertifikate, die Sie für diesen Server erstellt haben, an einem Speicherort gespeichert sind, auf den das Installationsprogramm zugreifen kann. Weitere Informationen erhalten Sie unter [„Erstellen und Importieren eines signierten SSL-Zertifikats“](#), auf Seite 18. Da das Konfigurationsskript nicht mit einer privilegierten Identität ausgeführt wird, müssen die Keystore-Datei und der Pfad, in denen es gespeichert ist, von jedem Benutzer gelesen werden können. Durch die Verwendung desselben Keystore-Pfads (z. B.: /tmp/certificates.ks) für alle Mitglieder einer Servergruppe wird der Installationsvorgang vereinfacht.
- Sie müssen die folgenden Informationen bereithalten:
 - Das Kennwort der Keystore-Datei, die die SSL-Zertifikate für diesen Server enthält.
 - Kennwort für die einzelnen SSL-Zertifikate.

Vorgehensweise

- 1 Melden Sie sich beim Zielsystem als Root an.
- 2 Laden Sie die Installationsdatei auf den Zielsystem herunter.

Wenn Sie die Software auf CD oder einem anderen Medium gekauft haben, kopieren Sie die Installationsdatei an einen Speicherplatz, auf den alle Zielsystem zugreifen können.

- 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 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.

- 5 Führen Sie die Installationsdatei in einem Konsolen-, Shell- oder Terminalfenster mithilfe der Option `-r` aus und geben Sie den Pfadnamen der Antwortdatei an.

Um die Installationsdatei auszuführen, geben Sie ihren vollständigen Pfadnamen ein, z. B.:

```
[root@cell1 /tmp]# ./installation-file -r /path-to-response-file
```

Diese Datei enthält ein Installationskript und ein eingebettetes RPM-Paket.

HINWEIS Sie können die Installationsdatei nicht von einem Verzeichnis ausführen, dessen Pfadname Leerzeichen einschließt.

Wenn Sie den öffentlichen Schlüssel von VMware nicht auf dem Zielsystem installiert haben, gibt das Installationsprogramm eine Warnung der folgenden Art aus.

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

Bei Ausführung des Installationsprogramms mit der Option `-r` werden folgende Aktionen durchgeführt:

- a überprüft, ob der Host alle Anforderungen erfüllt
- b verifiziert die digitale Signatur auf der Installationsdatei
- c erstellt den/die vcloud-Nutzer/-Gruppe
- d entpackt das vCloud Director-RPM-Paket
- e installiert die Software
- f kopiert die Antwortdatei an einen von vcloud.vcloud lesbaren Ort
- g führt das Konfigurationsskript mit der Antwortdatei als Eingabe aus

Bei Ausführung des Konfigurationsskripts sucht dieses die Zertifikate unter dem in der Antwortdatei gespeicherten Pfad (z. B.: `/tmp/certificates.ks`) und fordert Sie dann auf, das Keystore- und das Zertifikatkenwort einzugeben. Findet das Konfigurationsskript keine gültigen Zertifikate unter dem in der Antwortdatei gespeicherten Pfadnamen, erscheint die Eingabeaufforderung für einen Pfadnamen für die Zertifikate.

- 6 (Optional) Wiederholen Sie den Vorgang, um dieser Servergruppe weitere Server hinzuzufügen.

Weiter

Installieren Sie Sysprep-Dateien auf allen Mitgliedern der Servergruppe, wenn Ihre Cloud Gast-Anpassung für bestimmte ältere Microsoft-Betriebssysteme unterstützen muss. Weitere Informationen erhalten Sie unter [„Installation von Microsoft Sysprep-Dateien auf den Servern“](#), auf Seite 34.

Wenn das Konfigurationsskript beendet ist und die vCloud Director-Dienste auf allen Servern ausgeführt werden, können Sie den Setup-Assistenten öffnen. Verwenden Sie dazu die URL, die bei Beendigung des Skripts angezeigt wird. Weitere Informationen erhalten Sie unter [Kapitel 4, „vCloud Director-Einrichtung“](#), auf Seite 49.

Installation von Microsoft Sysprep-Dateien auf den Servern

Damit vCloud Director eine Gastanpassung für virtuelle Maschinen mit bestimmten älteren Windows-Gastbetriebssystemen durchführen kann, müssen Sie die entsprechenden Microsoft Sysprep-Dateien für jedes 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.

Vorgehensweise

- 1 Melden Sie sich beim Zielserver 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 2-1. 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
```

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.

Starten oder Beenden der vCloud Director -Dienste

Nachdem Sie die Installation und die Einrichtung der Datenbankverbindung auf einem Server abgeschlossen haben, können Sie die vCloud Director-Dienste auf diesem Server starten. Sie können diese Dienste auch beenden, wenn sie ausgeführt werden.

Das Konfigurationsskript fordert Sie auf, die vCloud Director-Dienste zu starten. Sie können es dem Skript überlassen, diese Dienste für Sie zu starten, oder Sie können sie zu einem späteren Zeitpunkt selbst starten. Diese Dienste müssen ausgeführt werden, bevor Sie die Installation durchführen und initialisieren können.

vCloud Director-Dienste werden jedes Mal gestartet, wenn Sie einen Server neu starten.

WICHTIG Wenn Sie die vCloud Director-Dienste als Teil eines vCloud Director-Software-Upgrades beenden, müssen Sie das Zellenverwaltungstool verwenden, mit dem Sie die Zelle stilllegen können, bevor Sie die Dienste beenden. Weitere Informationen erhalten Sie unter „[Stilllegen und Herunterfahren eines Servers mithilfe des Zellenverwaltungstools](#)“, auf Seite 39.

Vorgehensweise

- 1 Melden Sie sich beim Zielsystem als Root an.
- 2 Starten oder beenden Sie die Dienste.

Option	Aktion
Dienste starten	Öffnen Sie ein Konsolen-, Shell- oder Terminalfenster, und führen Sie den folgenden Befehl aus. <code>service vmware-vcd start</code>
Dienste beenden, wenn Zelle verwendet wird	Verwenden Sie das Zellenverwaltungstool.
Dienste beenden, wenn Zelle nicht verwendet wird	Öffnen Sie ein Konsolen-, Shell- oder Terminalfenster, und führen Sie den folgenden Befehl aus. <code>service vmware-vcd stop</code>

Deinstallieren der vCloud Director -Software

Verwenden Sie den Linux-Befehl `rpm`, um die vCloud Director-Software von einem einzelnen Server zu deinstallieren.

Vorgehensweise

- 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 ein Konsolen-, Shell- oder Terminalfenster, und führen Sie den Befehl `rpm` aus.

```
rpm -e vmware-vcloud-director
```

Aktualisieren von vCloud Director

Um vCloud Director auf eine neue Version zu aktualisieren, installieren Sie die neue Version auf jedem Server in der vCloud Director-Servergruppe, aktualisieren Sie die vCloud Director-Datenbank, und starten Sie die vCloud Director-Dienste neu. Sie müssen auch die vSphere-Komponenten aktualisieren, die vCloud Director unterstützen, einschließlich vShield Manager.

Nachdem Sie einen vCloud Director-Server aktualisiert haben, müssen Sie auch seine 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. Damit gewährleistet ist, dass nach einem Upgrade keine ungültigen Aufgabeninformationen in der Datenbank verbleiben, müssen Sie sicherstellen, dass keine Aufgaben mehr auf dem Server aktiv sind, bevor Sie mit dem Upgrade beginnen.

WICHTIG Für den Upgradevorgang ist ein Upgrade von vCloud Director, vShield Manager, vCenter und allen Hosts erforderlich. Sie müssen den Benutzerzugriff auf vCloud Director so lange verhindern, bis das Upgrade von vShield Manager abgeschlossen ist.

Das Upgrade behält die folgenden Elemente bei:

- Lokale und globale Eigenschaftendateien werden in die neue Installation kopiert.
- Für die Gastanpassung verwendete Microsoft-sysprep-Dateien werden in die neue Installation kopiert.

Wenn Sie einen Lastausgleichsdienst zum Verteilen von Clientanforderungen über Mitglieder Ihrer vCloud Director-Servergruppe hinweg einsetzen, können Sie eine Untermenge der Servergruppe aktualisieren und dabei die vorhandenen Dienste auf den anderen Mitgliedern aufrechterhalten. Wenn Sie kein Lastausgleichsmodul einsetzen, ist eine ausreichend lange Ausfallzeit von vCloud Director für das Upgrade erforderlich, damit die Datenbank und mindestens ein Server aktualisiert werden können. Möglicherweise müssen Sie auch registrierte vCenter Server aktualisieren, wenn auf diesen keine kompatible Version der vCenter-Software ausgeführt wird. Beim Aktualisieren der vCenter Server und ESXi-Hosts kann es zu zusätzlichen Ausfallzeiten bei vCloud Director kommen, da virtuelle Maschinen nicht verfügbar sind, solange deren Hosts oder vCenter Server aktualisiert werden.

Aktualisieren einer vCloud Director -Servergruppe

- 1 Deaktivieren Sie den Benutzerzugriff auf vCloud Director. Sie können während des Upgradevorgangs auch eine Wartungsmeldung anzeigen. Weitere Informationen erhalten Sie unter [„Anzeigen der Wartungsmeldung während eines Upgrades“](#), auf Seite 39.
- 2 Legen Sie mithilfe des Zellenverwaltungstools alle Zellen still, und fahren Sie die vCloud Director-Dienste auf jedem Server herunter. Weitere Informationen erhalten Sie unter [„Stilllegen und Herunterfahren eines Servers mithilfe des Zellenverwaltungstools“](#), auf Seite 39.

- 3 Aktualisieren Sie die vCloud Director-Software auf allen Mitgliedern der Servergruppe. Weitere Informationen erhalten Sie unter [„Aktualisieren der vCloud Director-Software auf einem beliebigen Mitglied einer Servergruppe“](#), auf Seite 41. Sie können die Server einzeln oder parallel aktualisieren, jedoch dürfen Sie die vCloud Director-Dienste erst auf einem aktualisierten Mitglied der Gruppe neu starten, nachdem Sie die vCloud Director-Datenbank aktualisiert haben.
- 4 Aktualisieren Sie die vCloud Director-Datenbank. Weitere Informationen erhalten Sie unter [„Aktualisieren der vCloud Director-Datenbank“](#), auf Seite 44.
- 5 Starten Sie vCloud Director auf den aktualisierten Servern neu. Weitere Informationen erhalten Sie unter [„Starten oder Beenden der vCloud Director-Dienste“](#), auf Seite 35.
- 6 Aktualisieren Sie vShield Manager. Stellen Sie sicher, dass alle in dieser Servergruppe registrierten vShield Manager-Installationen auf eine Version der vShield Manager-Software aktualisiert werden, die mit der beim Upgrade installierten Version von vCloud Director kompatibel ist. Wenn das Upgradeprogramm eine nicht kompatible vShield Manager-Version erkennt, ist das Upgrade nicht zulässig. Sie müssen ein Upgrade auf die neueste Version von vShield Manager, die in [„Unterstützte Plattformen“](#), auf Seite 9 aufgelistet ist, durchführen, um die in dieser Version von vCloud Director eingeführten Netzwerkfunktionen verwenden zu können. Weitere Informationen erhalten Sie unter [„Aktualisieren von vShield Manager“](#), auf Seite 46.
- 7 Aktivieren Sie den Benutzerzugriff auf vCloud Director.
- 8 Aktualisieren Sie vCenter Server und Hosts. Weitere Informationen erhalten Sie unter [„Aktualisieren von vCenter, Hosts und vShield Edge-Appliances“](#), auf Seite 46. Alle in dieser Servergruppe registrierten vCenter Server müssen auf eine Version der vCenter-Software aktualisiert werden, die mit der beim Upgrade installierten Version von vCloud Director kompatibel ist. Auf inkompatible vCenter Server kann nach dem Upgrade nicht mehr von vCloud Director zugegriffen werden. Weitere Informationen erhalten Sie unter [„Unterstützte Plattformen“](#), auf Seite 9.

Verwenden eines Lastausgleichmoduls zur Verringerung der Dienstausfallzeit

Wenn Sie ein Lastausgleichsmodul oder ein anderes Tool verwenden, das Anforderungen an bestimmte Server erzwingen kann, können Sie eine Teilmenge der Servergruppe aktualisieren und gleichzeitig die vorhandenen Dienste auf der restlichen Teilmenge weiterhin zur Verfügung stellen. Mit diesem Verfahren wird die Ausfallzeit des vCloud Director-Diensts auf die für das Upgrade der vCloud Director-Datenbank benötigte Zeitspanne reduziert. Benutzer erleben möglicherweise eine leichte Beeinträchtigung der Leistung während des Upgrades, aber laufende Aufgaben werden weiterhin durchgeführt, solange eine Untermenge der Servergruppe betriebsbereit ist. Konsolensitzungen werden möglicherweise unterbrochen, aber Sie können sie neu starten.

- 1 Mit dem Lastausgleichsmodul können Sie die vCloud Director-Anforderungen an eine Teilmenge der Server in der Gruppe weiterleiten. Gehen Sie wie vom Lastausgleichsmodul empfohlen vor.
- 2 Legen Sie mithilfe des Zellenverwaltungstools die Zellen still, die keine Anforderungen mehr bearbeiten, und fahren Sie die vCloud Director-Dienste auf diesen Servern herunter.

HINWEIS Konsolensitzungen die über den Konsolen-Proxy eines Servers weitergeleitet werden, werden unterbrochen, wenn der Server heruntergefahren wird. Clients können das Konsolenfenster aktualisieren, um eine Wiederherstellung zu erzielen.

Weitere Informationen erhalten Sie unter [„Stilllegen und Herunterfahren eines Servers mithilfe des Zellenverwaltungstools“](#), auf Seite 39.

- 3 Aktualisieren Sie die vCloud Director-Software auf den Mitgliedern der Servergruppe, auf denen Sie vCloud Director beendet haben, aber starten Sie diese Dienste nicht neu. Weitere Informationen erhalten Sie unter [„Aktualisieren der vCloud Director-Software auf einem beliebigen Mitglied einer Servergruppe“](#), auf Seite 41.

- 4 Legen Sie mithilfe des Zellenverwaltungstools die Zellen still, die Sie noch nicht aktualisiert haben, und fahren Sie die vCloud Director-Dienste auf diesen Servern herunter.
- 5 Aktualisieren Sie die vCloud Director-Datenbank. Weitere Informationen erhalten Sie unter „Aktualisieren der vCloud Director-Datenbank“, auf Seite 44.
- 6 Starten Sie vCloud Director auf den aktualisierten Servern neu. Weitere Informationen erhalten Sie unter „Starten oder Beenden der vCloud Director-Dienste“, auf Seite 35.
- 7 Aktualisieren Sie vShield Manager. Weitere Informationen erhalten Sie unter „Aktualisieren von vShield Manager“, auf Seite 46.
- 8 Aktualisieren Sie vCenter Server und Hosts. Weitere Informationen erhalten Sie unter „Aktualisieren von vCenter, Hosts und vShield Edge-Appliances“, auf Seite 46.
- 9 Leiten Sie die vCloud Director-Anforderungen mithilfe des Lastausgleichsmoduls an die aktualisierten Server weiter.
- 10 Aktualisieren Sie die vCloud Director-Software auf den übrigen Servern in der Gruppe, und starten Sie vCloud Director neu, wenn die Aktualisierungen abgeschlossen sind. Weitere Informationen erhalten Sie unter „Aktualisieren der vCloud Director-Software auf einem beliebigen Mitglied einer Servergruppe“, auf Seite 41.

Anzeigen der Wartungsmeldung während eines Upgrades

Wenn Sie von einem längeren Upgradevorgang ausgehen und vom System eine Wartungsmeldung angezeigt werden soll, solange das Upgrade ausgeführt wird, stellen Sie sicher, dass mindestens eine Zelle verfügbar bleibt, während die anderen aktualisiert werden. Führen Sie den Befehl `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` für diese Zelle aus, um die Meldung zur Zellenwartung zu aktivieren.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
```

Diesen Befehl können Sie für eine Zelle ausführen, bevor oder nachdem diese aktualisiert wurde. Wenn Sie die Zelle aktualisieren oder eine aktualisierte Zelle wieder aktivieren möchten, führen Sie den folgenden Befehl für die Zelle aus, um die Wartungsmeldung zu deaktivieren.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell stop
```

Dieses Kapitel behandelt die folgenden Themen:

- „Stilllegen und Herunterfahren eines Servers mithilfe des Zellenverwaltungstools“, auf Seite 39
- „Aktualisieren der vCloud Director-Software auf einem beliebigen Mitglied einer Servergruppe“, auf Seite 41
- „Aktualisieren der vCloud Director-Datenbank“, auf Seite 44
- „Aktualisieren von vShield Manager“, auf Seite 46
- „Aktualisieren von vCenter, Hosts und vShield Edge-Appliances“, auf Seite 46

Stilllegen und Herunterfahren eines Servers mithilfe des Zellenverwaltungstools

Bevor Sie einen vCloud Director-Server aktualisieren, verwenden Sie das Zellenverwaltungstool, um die vCloud Director-Dienste auf der Zelle des Servers stillzulegen und herunterzufahren.

vCloud Director erstellt ein Aufgabenobjekt, um alle von einem Benutzer angeforderten asynchronen Vorgänge zu verfolgen und zu verwalten. Informationen über alle ausgeführten und kürzlich abgeschlossenen Aufgaben werden in der vCloud Director-Datenbank gespeichert. Da ein Datenbank-Upgrade diese Aufgabeninformationen ungültig macht, muss gewährleistet sein, dass keine Aufgaben ausgeführt werden, wenn Sie den Aktualisierungsvorgang starten.

Sie können das Aufgabenplanungstool mithilfe des Zellenverwaltungstools anhalten, sodass keine neuen Aufgaben gestartet werden können, und dann den Status aller aktiven Aufgaben prüfen. Sie können abwarten, bis die aktiven Aufgaben abgeschlossen sind, oder sich als Systemadministrator bei vCloud Director anmelden und die Aufgaben abrechnen. Weitere Informationen erhalten Sie unter [Kapitel 5, „Überblick über das Zellenverwaltungstool“](#), auf Seite 53. Wenn keine Aufgaben ausgeführt werden, können Sie die vCloud Director-Dienste mithilfe des Zellenverwaltungstools beenden.

Voraussetzungen

- Überprüfen Sie, ob Sie die für den Zielservers benötigten Superuser-Anmeldeinformationen besitzen.
- Überprüfen Sie, ob Sie über Systemadministrator-Anmeldeinformationen für vCloud Director verfügen.
- Sollten vCloud Director-Clients auf diese Zelle zugreifen können, während sie aktualisiert wird, verwenden Sie den Befehl `/opt/vmware/vcloud-director/bin/vmware-vcd-cell`, um die Meldung zur Zellenwartung zu aktivieren.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
```

Dieser Befehl führt dazu, dass die Zelle auf alle Anforderungen mit einer Wartungsmeldung antwortet. Wenn Sie einen Lastausgleichsdienst oder ein ähnliches Tool verwenden, um während des Upgrades keine Zugriffe auf die Zelle zuzulassen, müssen Sie die Meldung zur Zellenwartung nicht aktivieren.

Vorgehensweise

- 1 Melden Sie sich beim Zielservers als Root an.

2 Fahren Sie die Zelle mithilfe des Zellenverwaltungstools normal herunter.

- a Rufen Sie den derzeitigen Jobstatus ab.

Der folgende `cell-management-tool`-Befehl übergibt die Anmeldeinformationen für den Systemadministrator und liefert als Ergebnis die Anzahl der derzeit ausgeführten Jobs.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell --status
Job count = 3
Is Active = true
```

- b Beenden Sie das Aufgabenplanungstool, um die Zelle stillzulegen.

Verwenden Sie einen `cell-management-tool`-Befehl der folgenden Form.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell --quiesce true
```

Dieser Befehl verhindert den Start neuer Jobs. Vorhandene Jobs sind solange weiterhin aktiv, bis sie abgeschlossen wurden oder abgebrochen werden. Zum Abbrechen eines Jobs verwenden Sie die Webkonsole oder die REST-API von vCloud Director.

- c Wenn der Wert von `Job count` gleich 0 und der Wert von `Is Active` gleich `false` ist, können Sie die Zelle sicher herunterfahren.

Verwenden Sie einen `cell-management-tool`-Befehl der folgenden Form.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell --shutdown
```

HINWEIS Sie können das Kennwort für den vCloud Director-Systemadministrator in der Befehlszeile des `cell-management-tool` angeben. Es ist jedoch sicherer, das Kennwort wegzulassen. Damit werden Sie vom `cell-management-tool` aufgefordert, das Kennwort anzugeben, das während der Eingabe nicht auf dem Bildschirm angezeigt wird.

Konsolensitzungen die über den Konsolen-Proxy eines Servers weitergeleitet werden, werden unterbrochen, wenn der Server heruntergefahren wird. Wenn andere Mitglieder der Servergruppe noch aktiv sind, können Clients zwecks Wiederherstellung das Konsolenfenster aktualisieren.

Weiter

Nachdem das Zellenverwaltungstool die vCloud Director-Dienste auf diesem Server angehalten hat, können Sie ein Upgrade der vCloud Director-Software des Servers oder andere Wartungsaufgaben durchführen, die für den Server notwendig sind.

Aktualisieren der vCloud Director -Software auf einem beliebigen Mitglied einer Servergruppe

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

vCloud Director-Software wird als ausführbare Linux-Datei mit dem Namen `vmware-vcloud-director-5.5.0-nnnnnn.bin` verteilt, wobei *nnnnnn* eine Buildnummer darstellt. Nach der Installation des Upgrades auf einem Mitglied einer Servergruppe müssen Sie ein Tool ausführen, das die von der Gruppe verwendete vCloud Director-Datenbank aktualisiert, bevor Sie die vCloud Director-Dienste auf dem aktualisierten Server neu starten können.

Voraussetzungen

- Überprüfen Sie, ob Sie die für den Zielservers benötigten Superuser-Anmeldeinformationen besitzen.

- Laden Sie den öffentlichen Schlüssel von VMware auf den Zielserver herunter und installieren Sie ihn, damit das Installationsprogramm die digitale Signatur der Installationsdatei überprüft. Wenn Sie die digitale Signatur der Installationsdatei bereits überprüft haben, müssen Sie sie nicht erneut während der Installation überprüfen. Weitere Informationen erhalten Sie unter [„Herunterladen und Installieren des öffentlichen Schlüssels von VMware“](#), auf Seite 24.
- Legen Sie mithilfe des Zellenverwaltungstools die Serverzelle still und fahren Sie die vCloud Director-Dienste auf der Serverzelle herunter.

Vorgehensweise

- 1 Melden Sie sich beim Zielserver als Root an.

- 2 Laden Sie die Installationsdatei auf den Zielserver herunter.

Wenn Sie die Software auf CD oder einem anderen Medium gekauft haben, kopieren Sie die Installationsdatei an einen Speicherplatz, auf den alle Zielserver zugreifen können.

- 3 Überprüfen Sie, ob die Prüfsumme der heruntergeladenen Datei mit der auf der Download-Seite 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 Download-Seite übereinstimmt. Mit einem Linux-Befehl im folgenden Format wird die Prüfsumme für *installation-file* unter Verwendung des von der Download-Seite kopierten MD5-Prüfsummenwerts *checksum-value* überprüft.

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

- 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 Legen Sie mithilfe des Zellenverwaltungstools die Zelle still, und fahren Sie die vCloud Director-Dienste auf dem Server herunter.

Weitere Informationen erhalten Sie unter [„Stilllegen und Herunterfahren eines Servers mithilfe des Zellenverwaltungstools“](#), auf Seite 39.

- 6 Führen Sie die Installationsdatei in einem Konsolen-, Shell- oder Terminalfenster aus.

Um die Installationsdatei auszuführen, geben Sie ihren vollständigen Pfadnamen ein, z. B. *./installation-file*. 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 auf diesem Server installierte Version von vCloud Director erkennt, die gleich oder neuer als die Version der Installationsdatei ist, zeigt es eine Fehlermeldung an und wird beendet. Andernfalls fordert es Sie auf zu bestätigen, dass Sie für die Aktualisierung dieses Servers bereit sind.

```
Checking architecture...done
Checking for a supported Linux distribution...done
Checking for necessary RPM prerequisites...done
Checking free disk space...done
```

An older version of VMware vCloud Director has been detected. Would you like to upgrade it? The installer will stop the vmware-vcd service, back up any configuration files from the previous release and migrate the product configuration as necessary.

- 7 Machen Sie die von der Upgrade-Eingabeaufforderung gewünschten Eingaben.

Option	Aktion
Aktualisierung fortsetzen.	Geben Sie y ein.
Zur Shell zurückkehren, ohne Änderungen an der aktuellen Installation vorzunehmen.	Geben Sie n ein.

Nachdem Sie bestätigt haben, dass Sie für die Aktualisierung des Servers bereit sind, überprüft das Installationsprogramm, ob der Host alle Anforderungen erfüllt, entpackt das vCloud Director-RPM-Paket, beendet die vCloud Director-Dienste auf dem Server und aktualisiert die installierte vCloud Director-Software.

```

Would you like to upgrade now? (y/n) y
Extracting vmware-vcloud-director .....done
Upgrading VMware vCloud Director...
Installing the VMware vCloud Director
Preparing... #####
vmware-vcloud-director #####
Migrating settings and files from previous release...done
Migrating in-progress file transfers to /opt/vmware/vcloud-director/data/transfer...done
Uninstalling previous release...done
    
```

Wenn Sie den öffentlichen Schlüssel von VMware nicht auf dem Zielsystem installiert haben, gibt das Installationsprogramm eine Warnung der folgenden Art aus.

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

- 8 (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 /opt/vmware/vcloud-director/etc/log4j.properties.
Wenn Sie Protokollierungseigenschaften geändert haben	Führen Sie die Datei /opt/vmware/vcloud-director/etc/log4j.properties.rpmnew mit der vorhandenen Datei /opt/vmware/vcloud-director/etc/log4j.properties zusammen. Durch die Zusammenführung dieser Dateien bleiben Ihre Änderungen erhalten.

Wenn die Aktualisierung der vCloud Director-Software abgeschlossen ist, zeigt das Installationsprogramm eine Meldung an, in der der Speicherort der alten Konfigurationsdateien angegeben wird, und erinnert Sie dann an die Ausführung des Datenbank-Upgrade-Tools.

Weiter

- Aktualisieren Sie die von diesem Server verwendete vCloud Director-Datenbank, sofern Sie dies noch nicht getan haben.
- Wenn Sie die von dieser Servergruppe verwendete vCloud Director-Datenbank bereits aktualisiert haben, können Sie den aktualisierten Server neu starten. Weitere Informationen erhalten Sie unter „[Starten oder Beenden der vCloud Director-Dienste](#)“, auf Seite 35.

Aktualisieren der vCloud Director -Datenbank

Nachdem Sie einen Server in der vCloud Director-Servergruppe aktualisiert haben, müssen Sie die vCloud Director-Datenbank der Gruppe aktualisieren, bevor Sie die vCloud Director-Dienste auf dem Server neu starten.

Alle Server in einer vCloud Director-Servergruppe verwenden dieselbe Datenbank, daher müssen Sie die Datenbank unabhängig von der Anzahl der zu aktualisierenden Server nur einmal aktualisieren. Nachdem die Datenbank aktualisiert wurde, können vCloud Director-Server erst wieder Verbindungen mit dieser herstellen, nachdem sie selbst ebenfalls aktualisiert wurden.

Voraussetzungen

WICHTIG Sichern Sie die vorhandene Datenbank, bevor Sie sie aktualisieren. Gehen Sie dabei nach den Empfehlungen des Datenbanksoftwareherstellers vor.

Stellen Sie sicher, dass alle vCloud Director-Zellen inaktiv sind. Weitere Informationen erhalten Sie unter [„Stilllegen und Herunterfahren eines Servers mithilfe des Zellenverwaltungstools“](#), auf Seite 39

Vorgehensweise

- 1 Öffnen Sie ein Konsolen-, Shell- oder Terminalfenster, und geben Sie den folgenden Befehl ein, um das Datenbank-Upgrade-Skript auszuführen.

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

WICHTIG Wenn das Skript für das Datenbank-Upgrade erkennt, dass eine inkompatible vShield Manager-Version bei dieser Installation von vCloud Director registriert ist, wird das Upgrade mit einer Warnmeldung abgebrochen.

```
One or more vShield Manager servers registered to this vCloud
Director installation are not supported by the version of vCloud Director
you are upgrading to. Upgrade canceled, please follow the procedures in
the vShield Manager Upgrade Guide to upgrade those unsupported vShield
Manager servers.
```

- 2 Machen Sie die entsprechenden Eingaben, wenn die Datenbank-Upgrade-Eingabeaufforderung Sie dazu auffordert.

- a Bestätigen Sie, dass Sie mit der Datenbank-Aktualisierung fortfahren möchten.

Welcome to the vCloud Director upgrade utility

This utility will apply several updates to the database. Please ensure you have created a backup of your database prior to continuing.

Do you wish to upgrade the product now? [Y/N]:

Ergreifen Sie eine der folgenden Maßnahmen:

Option	Aktion
Aktualisierung fortsetzen.	Geben Sie y ein.
Zur Shell zurückkehren, ohne Änderungen in der aktuellen vCloud Director-Datenbank vorzunehmen.	Geben Sie n ein.

- b (Optional) Warten Sie, wenn nötig, bis Zellen inaktiv werden.

Falls das Tool zur Datenbank-Aktualisierung feststellt, dass es noch aktive Zellen gibt, werden Sie gefragt, ob Sie mit dem Upgrade fortfahren oder den Vorgang beenden möchten.

Found active cell. Name: "cell-01", IP Address: 10.150.151.190, Identifier: a2eb...

Do you wish to upgrade the database while cells are still active? [Y/N]

Erscheint diese Aufforderung, geben Sie n ein, um die Shell zu verlassen, und starten Sie das Tool zur Datenbank-Aktualisierung erneut. Gibt das Tool zur Datenbank-Aktualisierung weiterhin Warnungen vor aktiven Zellen aus, kehren Sie zum Prozess in „[Stilllegen und Herunterfahren eines Servers mithilfe des Zellenverwaltungstools](#)“, auf Seite 39 zurück und stellen Sie sicher, dass alle Zellen inaktiv sind.

Nachdem Sie auf alle Warnungen reagiert haben, wird das Tool zur Datenbank-Aktualisierung ausgeführt und die Fortschrittsmeldung wird angezeigt.

```
Executing upgrade task: Start UpdateStatementManager
...[3]
Successfully ran upgrade task
Executing upgrade task: ...
..... Successfully ran upgrade task
...
Executing upgrade task: Stop UpdateStatementManager
...[3]
...
Successfully ran upgrade task
```

- 3 (Optional) Erstellen Sie die Datenbankindizes neu und aktualisieren Sie die Datenbankstatistiken.

Nach dem Upgrade kann nach Durchführung dieser Prozeduren eine bessere Datenbankleistung erzielt werden.

Do you wish to rebuild the database indexes? This may take several minutes. [Y/N] **y**

Rebuilding database indexes

...

Do you wish to update the database statistics? This may take several minutes. [Y/N] **y**

Updating database statistics

...

Nach der Aktualisierung der Datenbank werden Sie gefragt, ob die vCloud Director-Dienste auf diesem Host gestartet werden sollen.

```
Would you like to start the vCloud Director service now? If you choose not  
to start it now, you can manually start it at any time using this command:
```

```
service vmware-vcd start
```

```
Start it now? [y/n]:y
```

```
Starting the vCloud Director service (this may take a moment).
```

Aktualisieren von vShield Manager

Vor einem Upgrade von vCenter Servern und Hosts, die bei vCloud Director registriert sind, müssen Sie an vCenter Server angehängte vShield Manager-Server aktualisieren.

Bevor Sie einen an vCloud Director angefügten vCenter Server aktualisieren, aktualisieren Sie den mit dem aktualisierten vCenter Server verknüpften vShield Manager-Server. Während der Aktualisierung von vShield Manager ist der Zugriff auf Verwaltungsfunktionen von vShield Manager nicht möglich. Der Zugriff auf Netzwerkdienste bleibt jedoch unbeeinträchtigt.

Voraussetzungen

Bevor Sie mit dieser Aktualisierung beginnen, muss mindestens eine aktualisierte Zelle in Ihrer vCloud Director-Installation ausgeführt werden. Die Zelle ist dafür zuständig, Informationen zum aktualisierten vShield Manager in die vCloud Director-Datenbank zu schreiben.

Vorgehensweise

- 1 Aktualisieren Sie vShield Manager.

Folgen Sie den im *vShield Installations- und Upgrade-Handbuch* beschriebenen Anweisungen. Nach Abschluss dieser Aktualisierung wird vCloud Director von vShield Manager über die neue Version informiert. Es kann mehrere Minuten dauern, bevor vShield Manager die entsprechende Benachrichtigung sendet und diese von vCloud Director verarbeitet wird.

- 2 Nach dem Upgrade von vShield Manager müssen Sie alle vCenter Server und Hosts aktualisieren, bevor Sie die vom aktualisierten vShield Manager verwalteten vShield Edge-Appliances aktualisieren.

Aktualisieren von vCenter, Hosts und vShield Edge-Appliances

Nach dem Upgrade von vCloud Director und vShield Manager aktualisieren Sie die vCenter Server und Hosts, die an Ihre Cloud angefügt sind, und aktualisieren Sie dann vShield Edge-Appliances auf aktualisierten vCenter Servern.

Vorgehensweise

- 1 Aktualisieren Sie vCenter Server.

Weitere Informationen erhalten Sie im *Installations- und Einrichtungshandbuch für vSphere*.

- 2 (Optional) Wenn Sie vCloud Director so konfiguriert haben, dass vCenter Single Sign On verwendet wird, müssen Sie die Registrierung von vCloud Director beim vCenter Lookup Service aufheben und vCloud Director erneut registrieren.
 - a Melden Sie sich als Systemadministrator über ein lokales oder ein LDAP-Konto bei vCloud Director an. Verwenden Sie für diese Anmeldung nicht vCenter Single Sign On.
 - b Heben Sie die Registrierung von vCloud Director beim vCenter Lookup Service auf.
Klicken Sie auf der Registerkarte **[Administration]** auf der Webkonsole von vCloud Director im linken Fensterbereich auf **[Verbund]** und dann auf **[Registrierung aufheben]** . Sie müssen über die notwendigen Administratoranmeldeinformationen für vCenter verfügen, um diesen Vorgang durchzuführen.
 - c Registrieren Sie vCloud Director beim vCenter Lookup Service.
Informationen finden Sie unter „Konfigurieren von vCloud Director für die Verwendung von vCenter Single Sign On“ im *vCloud Director-Administratorhandbuch*
- 3 Aktualisieren Sie die Registrierung des vCenter Server bei vCloud Director.
 - a Klicken Sie in der vCloud Director-Webkonsole auf die Registerkarte **[Verwalten und Überwachen]** und klicken Sie dann im linken Bereich auf **[vCenter]** .
 - b Klicken Sie mit der rechten Maustaste auf den Namen des vCenter Server und wählen Sie den Befehl **[Aktualisieren]** .
 - c Klicken Sie auf **[Ja]** .
- 4 Aktualisieren Sie jeden Host, der vom aktualisierten vCenter Server unterstützt wird.
Weitere Informationen erhalten Sie im *Installations- und Einrichtungshandbuch für vSphere*. Für das Upgrade jedes Hosts müssen die folgenden Schritte ausgeführt werden:
 - a Deaktivieren Sie den Host in der vCloud Director-Webkonsole.
Klicken Sie auf der Seite **[Verwalten und Überwachen]** auf **[Hosts]** , klicken Sie dann mit der rechten Maustaste auf den Host und wählen Sie **[Host deaktivieren]** aus.
 - b Verwenden Sie vCenter, um den Host in den Wartungsmodus zu versetzen und es zu ermöglichen, dass alle virtuellen Maschinen auf diesem Host auf einen anderen Host migriert werden.
 - c Aktualisieren Sie den Host.
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.
 - d Stellen Sie mit vCenter wieder die Verbindung mit dem Host her.
 - e Aktualisieren Sie den vCloud Director-Host-Agenten auf dem Host.
Weitere Informationen erhalten Sie unter „Aktualisieren eines ESX/ESXi-Host-Agenten“ im *vCloud Director-Administratorhandbuch*.
 - f Aktivieren Sie den Host in der vCloud Director-Webkonsole.
Klicken Sie auf der Seite **[Verwalten und Überwachen]** auf **[Hosts]** , klicken Sie dann mit der rechten Maustaste auf den Host und wählen Sie **[Host aktivieren]** aus.
 - g Beenden Sie mit vCenter den Wartungsmodus des Hosts.

- 5 Aktualisieren Sie alle vShield Edge-Appliances auf dem aktualisierten vCenter Server, die von vShield Manager verwaltet werden.

Führen Sie diese Aktualisierung über die Benutzeroberfläche von vShield Manager durch.

HINWEIS Wenn Sie die Webkonsole oder REST-API von vCloud Director zum Zurücksetzen eines von vShield Edge geschützten Netzwerks verwenden, findet diese Aktualisierung automatisch statt. Die Verwendung der Benutzeroberfläche von vShield Manager zur Verwaltung der vShield Edge-Appliances ermöglicht eine bessere administrative Kontrolle des Upgradevorgangs und der damit einhergehenden Netzwerkausfallzeiten.

Weiter

Wiederholen Sie diesen Prozess für die anderen für Ihre Cloud registrierten vCenter Server.

vCloud Director -Einrichtung

Nachdem Sie alle Server in der vCloud Director-Servergruppe aktualisiert und mit der Datenbank verbunden haben, können Sie die Datenbank der Servergruppe mit einem Lizenzschlüssel, dem Systemadministratorkonto und verwandten Informationen aktualisieren. Wenn dieser Vorgang abgeschlossen ist, können Sie die Erstbereitstellung Ihrer Cloud mithilfe der vCloud Director-Webkonsole abschließen.

Bevor Sie die vCloud Director-Webkonsole ausführen können, müssen Sie den Setup-Assistenten ausführen, der die von der Webkonsole für ihren Start benötigten Informationen sammelt. Wenn der Assistent beendet ist, wird die Webkonsole gestartet und zeigt den Anmeldebildschirm an. Die vCloud Director-Webkonsole bietet mehrere Tools zum Bereitstellen und Verwalten einer Cloud. Außerdem enthält sie eine Schnellstart-Funktion, die Sie durch Schritte wie das Anfügen von vCloud Director an vCenter und Erstellen einer Organisation führt.

Voraussetzungen

- Führen Sie die Installation aller vCloud Director-Server durch, und überprüfen Sie, ob die vCloud Director-Dienste auf allen Servern gestartet wurden.
- Überprüfen Sie, ob Sie die URL besitzen, die das Konfigurationsskript bei seinem Abschluss anzeigt.

HINWEIS Um die URL des Setup-Assistenten nach Beenden des Skripts zu finden, suchen Sie den mit der IP-Adresse, die Sie während der Installation des ersten Servers für den HTTP-Dienst angegeben haben, verknüpften vollqualifizierten Namen, und erstellen Sie mit diesem eine URL im Format `https://fully-qualified-domain-name`, z. B. `https://meinecloud.beispiel.com`. Sie können über diese URL eine Verbindung zum Assistenten herstellen.

Führen Sie die Installation aller vCloud Director-Server durch, und überprüfen Sie, ob die vCloud Director-Dienste auf allen Servern gestartet wurden.

Vorgehensweise

- 1 Öffnen Sie einen Webbrowser, und stellen Sie eine Verbindung zu der URL her, die das Konfigurationsskript bei seinem Abschluss anzeigt.
- 2 Folgen Sie den Eingabeaufforderungen, um die Einrichtung abzuschließen.

Dieses Kapitel behandelt die folgenden Themen:

- „[Lesen der Lizenzvereinbarung](#)“, auf Seite 50
- „[Eingeben des Lizenzschlüssels](#)“, auf Seite 50
- „[Erstellen eines Systemadministratorkontos](#)“, auf Seite 50
- „[Angaben der Systemeinstellungen](#)“, auf Seite 51
- „[Bereit zur Anmeldung bei vCloud Director](#)“, auf Seite 51

Lesen der Lizenzvereinbarung

Bevor Sie eine vCloud Director-Servergruppe konfigurieren können, müssen Sie die Endbenutzerlizenzvereinbarung lesen und akzeptieren.

Vorgehensweise

- 1 Lesen Sie die Lizenzvereinbarung.
- 2 Akzeptieren Sie die Lizenzvereinbarung, oder lehnen Sie sie ab.

Option	Aktion
So akzeptieren Sie die Lizenzvereinbarung:	Klicken Sie auf [Ja, ich akzeptiere die Bedingungen in dieser Lizenzvereinbarung] .
So lehnen Sie die Lizenzvereinbarung ab	[Nein, ich akzeptiere die Bedingungen in dieser Lizenzvereinbarung nicht] .

Wenn Sie die Lizenzvereinbarung ablehnen, können Sie nicht mit der vCloud Director-Konfiguration fortfahren.

Eingeben des Lizenzschlüssels

Jeder vCloud Director-Cluster benötigt einen Lizenzschlüssel, damit er ausgeführt werden kann. Die Lizenz ist als Produktseriennummer angegeben. Die Produktseriennummer ist in der vCloud Director-Datenbank gespeichert.

Die vCloud Director-Produktseriennummer und der vCenter Server-Lizenzschlüssel sind nicht identisch. Als Voraussetzung für den Betrieb einer vCloud benötigen Sie eine vCloud Director-Produktseriennummer und einen vCenter Server-Lizenzschlüssel. Sie können beide Lizenzschlüsseltypen vom VMware-Lizenzportal erhalten.

Vorgehensweise

- 1 Erhalten Sie eine vCloud Director-Produktseriennummer vom VMware-Lizenzportal.
- 2 Geben Sie die Produktseriennummer in das Textfeld **[Produktseriennummer]** ein.

Erstellen eines Systemadministratorkontos

Geben Sie den Benutzernamen, das Kennwort und die Kontaktinformationen für den vCloud Director-Systemadministrator an.

Der vCloud Director-Systemadministrator hat in der gesamten Cloud Superuser-Rechte. Er erstellt das erste Systemadministratorkonto bei der Einrichtung von vCloud Director. Wenn die Installation und Konfiguration abgeschlossen ist, kann dieser Systemadministrator nach Bedarf weitere Systemadministratorkonten erstellen.

Vorgehensweise

- 1 Geben Sie den Benutzernamen des Systemadministrators ein.
- 2 Geben Sie das Kennwort des Systemadministrators ein, und bestätigen Sie es.
- 3 Geben Sie den vollständigen Namen des Systemadministrators ein.
- 4 Geben Sie die E-Mail-Adresse des Systemadministrators ein.

Angeben der Systemeinstellungen

Sie können die Systemeinstellungen angeben, die die Interaktion von vCloud Director mit vSphere und vShield Manager steuern.

Dieser Konfigurationsvorgang erstellt in vCenter einen Ordner, der von vCloud Director verwendet werden soll, und gibt eine bei der Erstellung von MAC-Adressen für virtuelle Netzwerkadapter zu verwendende Installations-ID an.

Vorgehensweise

- 1 Geben Sie einen Namen für den vCloud Director vCenter-Ordner im Feld **[Systemname]** ein.
- 2 Geben Sie im Feld **[Installations-ID]** die Installations-ID für diese Installation von vCloud Director an.

Wenn ein Datacenter mehrere Installationen von vCloud Director umfasst, muss für jede Installation eine eindeutige Installations-ID angegeben werden.

Bereit zur Anmeldung bei vCloud Director

Nachdem Sie alle vom Setup-Assistenten angeforderten Informationen bereitgestellt haben, können Sie die Einstellungen bestätigen und den Assistenten beenden. Danach wird der Anmeldebildschirm der vCloud Director-Webkonsole angezeigt.

Auf der Seite "Bereit zur Anmeldung" werden alle Einstellungen angezeigt, die Sie dem Assistenten angegeben haben. Überprüfen Sie die Einstellungen sorgfältig.

Voraussetzungen

Prüfen Sie, ob Sie Zugriff auf vCenter und vShield Manager haben. Die vCloud Director-Webkonsole muss auf die Installationen von vCenter und vShield Manager zugreifen können, die Sie als Teil dieses vCloud Director-Servers konfigurieren möchten. Die Installationen müssen ausgeführt werden und so konfiguriert sein, dass sie zusammenarbeiten, bevor Sie diese Aufgabe beenden. Weitere Informationen erhalten Sie unter „[vCloud Director-Hardware- und Softwareanforderungen](#)“, auf Seite 9.

Vorgehensweise

- Um eine Einstellung zu ändern, klicken Sie so lange auf **[Zurück]**, bis Sie auf die Seite gelangen, von der die Einstellung stammt.
- Um alle Einstellungen zu bestätigen und den Konfigurationsvorgang abzuschließen, klicken Sie auf **[Fertigstellen]**.

Wenn Sie auf **[Fertigstellen]** klicken, wendet der Assistent die angegebenen Einstellungen an, startet danach die vCloud Director-Webkonsole und zeigt den Anmeldebildschirm an.

Weiter

Melden Sie sich bei der vCloud Director-Webkonsole mithilfe des für das Systemadministratorkonto angegebenen Benutzernamens und des Kennworts an. Nachdem Sie sich angemeldet haben, zeigt die Konsole mehrere Schritte für den Schnellstart an. Sie müssen sie durchführen, bevor Sie diese Cloud verwenden können. Nachdem Sie die Schritte durchgeführt haben, werden die Aufgaben mit Anleitung aktiviert, und die Cloud kann verwendet werden.

Überblick über das Zellenverwaltungstool

5

Das Zellenverwaltungstool ist ein Befehlszeilenprogramm, mit dem Sie eine Zelle und deren SSL-Zertifikate verwalten sowie Tabellen aus der vCloud Director-Datenbank exportieren können. Für einige Vorgänge sind Berechtigungen als Superuser oder Systemadministrator erforderlich.

Das Zellenverwaltungstool ist unter `/opt/vmware/vcloud-director/bin/cell-management-tool` installiert.

Auflisten der verfügbaren Befehle

Wenn Sie die für das Zellenverwaltungstool verfügbaren Befehle auflisten möchten, verwenden Sie die folgende Befehlszeile:

```
cell-management-tool -h
```

Beispiel: Hilfe zur Nutzung des Zellenverwaltungstools

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
```

```
usage: cell-management-tool
-h,--help          print this message
-p,--password <arg> administrator password
-u,--username <arg> administrator username
```

Available commands:

```
cell - Manipulates the Cell and core components
dbextract - Exports the data from the given set of tables
certificates - Reconfigures the SSL certificates for the cell
generate-certs - Generates self-signed SSL certificates for use with vCD cell
recover-password - Change a forgotten System Administrator password. Database credentials are required
```

For command specific help:

```
cell-management-tool [...] <commandName> -h
```

- [Befehle zum Verwalten von Zellen](#) auf Seite 54

Mit dem Befehl `cell` im Zellenverwaltungstool können Sie das Aufgabenplanungstool anhalten, damit keine neuen Aufgaben gestartet werden können, den Status aller aktiven Aufgaben prüfen, den Zellenwartungsmodus steuern sowie die Zelle normal herunterfahren.

- [Befehle zum Exportieren von Datenbanktabellen](#) auf Seite 55

Mit dem Befehl `dbextract` im Zellenverwaltungstool können Sie Daten aus der vCloud Director-Datenbank exportieren.

- [Befehle zum Ersetzen von SSL-Zertifikaten](#) auf Seite 58
Mit dem Befehl `certificates` im Zellenverwaltungstool können Sie die SSL-Zertifikate der Zelle ersetzen.
- [Befehle zum Generieren selbstsignierter SSL-Zertifikate](#) auf Seite 58
Mit dem Befehl `generate-certs` im Zellenverwaltungstool können Sie neue selbstsignierte SSL-Zertifikate für die Zelle generieren.
- [Wiederherstellen des Kennworts für den Systemadministrator](#) auf Seite 60
Wenn Sie den Benutzernamen und das Kennwort für die vCloud Director-Datenbank kennen, können Sie den Befehl `recover-password` des Zellenverwaltungstools verwenden, um das Kennwort des vCloud Director-Systemadministrators wiederherzustellen.

Befehle zum Verwalten von Zellen

Mit dem Befehl `cell` im Zellenverwaltungstool können Sie das Aufgabenplanungstool anhalten, damit keine neuen Aufgaben gestartet werden können, den Status aller aktiven Aufgaben prüfen, den Zellenwartungsmodus steuern sowie die Zelle normal herunterfahren.

Verwenden Sie zum Verwalten einer Zelle eine Befehlszeile im folgenden Format:

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell command
```

sysadmin-username Der Benutzername eines vCloud Director-Systemadministrators.

sysadmin-password Das Kennwort des vCloud Director-Systemadministrators.

HINWEIS Sie können das Kennwort für den vCloud Director-Systemadministrator in der Befehlszeile des `cell-management-tool` angeben. Es ist jedoch sicherer, das Kennwort wegzulassen. Damit werden Sie vom `cell-management-tool` aufgefordert, das Kennwort anzugeben, das während der Eingabe nicht auf dem Bildschirm angezeigt wird.

command cell-Unterbefehl.

Tabelle 5-1. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `cell`

Befehl	Argument	Beschreibung
<code>--help (-h)</code>	Keine	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--maintenance (-m)</code>	<code>true</code> oder <code>false</code>	Steuert den Zellenwartungsmodus. Mit dem Argument <code>true</code> wird die Zelle in den Wartungsmodus versetzt. (Zuerst müssen Sie die Zelle stilllegen.) Mit dem Argument <code>false</code> wird der Wartungsmodus für die Zelle beendet.
<code>--quiesce (-q)</code>	<code>true</code> oder <code>false</code>	Legt die Aktivität auf der Zelle still. Mit dem Argument <code>true</code> wird das Planungstool angehalten. Mit dem Argument <code>false</code> wird die Ausführung des Planungstools neu gestartet.

Tabelle 5-1. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `cell` (Fortsetzung)

Befehl	Argument	Beschreibung
<code>--shutdown (-s)</code>	Keine	Führt die vCloud Director-Dienste auf dem Server herunter.
<code>--status (-t)</code>	Keine	Zeigt Informationen zur Anzahl der derzeit in der Zelle ausgeführten Jobs und den Status der Zelle an.

Beispiel: Abrufen des Aufgabenstatus

Die folgende `cell-management-tool`-Befehlszeile übergibt die Anmeldeinformationen für den Systemadministrator und liefert als Ergebnis die Anzahl der derzeit ausgeführten Jobs. Wenn der Wert von `Job count` gleich 0 und der Wert von `Is Active` gleich `false` ist, können Sie die Zelle sicher herunterfahren.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell --status
Job count = 3
Is Active = true
```

Befehle zum Exportieren von Datenbanktabellen

Mit dem Befehl `dbextract` im Zellenverwaltungstool können Sie Daten aus der vCloud Director-Datenbank exportieren.

Verwenden Sie zum Exportieren von Datenbanktabellen eine Befehlszeile im folgenden Format:

```
cell-management-tool dbextract options
```

Tabelle 5-2. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `dbextract`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keine	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>-categories</code>	Eine durch Komma getrennte Liste der zu exportierenden Tabellenkategorien.	Optional. <code>NETWORKING</code> ist die einzige unterstützte Kategorie.
<code>-dataFile</code>	Ein absoluter Pfad zu einer Datei, die die zu exportierenden Daten beschreibt.	Optional. Wenn dies nicht angegeben wird, verwendet der Befehl <code>\$VCLLOUD_HOME/etc/data_to_export.properties</code> . Weitere Informationen erhalten Sie unter „ Angaben der zu exportierenden Tabellen und Spalten “, auf Seite 56.
<code>-dumpFile</code>	Ein absoluter Pfad zu einer Dumpdatei. Das beinhaltende Verzeichnis muss bestehen und von Root beschreibbar sein.	Alle Daten werden in diese Datei exportiert.
<code>-exportSettingsFile</code>	Ein absoluter Pfad zu einer Eigenschaftendatei für Datenexporteinstellungen.	Optional. Wenn dies nicht angegeben wird, verwendet der Befehl <code>\$VCLLOUD_HOME/etc/data_export_settings.ini</code> . Weitere Informationen erhalten Sie unter „ Einschränken und Sortieren der exportierten Zeilen “, auf Seite 57.

Tabelle 5-2. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `dbextract` (Fortsetzung)

Option	Argument	Beschreibung
<code>-properties</code>	Ein absoluter Pfad zu einer Eigenschaftendatei für Datenbankverbindungen.	Optional. Wenn dies nicht angegeben wird, verwendet der Befehl die Datenbankverbindungseigenschaften in <code>\$VCLLOUD_HOME/etc/global.properties</code> . Weitere Informationen erhalten Sie unter „ Angabe einer Eigenschaftendatei “, auf Seite 56.
<code>-tables</code>	Eine durch Komma getrennte Liste von Tabellen.	Optional. Exportieren Sie alle Tabellen, um einzelne Tabellennamen anzuzeigen.

Angabe einer Eigenschaftendatei

Standardmäßig extrahiert der Befehl `dbextract` Daten aus der vCloud Director-Datenbank mithilfe der Datenbankverbindungsinformationen in der Datei `$VCLLOUD_HOME/etc/global.properties` der aktuellen Zelle. Um Daten aus einer anderen vCloud Director-Datenbank zu extrahieren, geben Sie die Verbindungseigenschaften der Daten in einer Datei an und nutzen Sie die Option `-properties`, um den Pfadnamen zu der Datei in der Befehlszeile einzugeben. Bei der Eigenschaftendatei handelt es sich um eine UTF-8-Datei mit dem folgenden Format.

```
username=username
password=password
servicename=db_service_name
port=db_connection_port
database-ip=db_server_ip_address
db-type=db_type
```

<code>username</code>	Der Benutzername der vCloud Director-Datenbank.
<code>password</code>	Das Kennwort der vCloud Director-Datenbank.
<code>db_service_name</code>	Der Datenbankdienstname. Beispiel: <code>orcl.example.com</code> .
<code>db_connection_port</code>	Der Datenbankport.
<code>db_server_ip_address</code>	Die IP-Adresse des Datenbankservers.
<code>db_type</code>	Der Datenbanktyp. Muss <code>Oracle</code> oder <code>MS_SQL</code> sein.

Angabe der zu exportierenden Tabellen und Spalten

Verwenden Sie zum Einschränken des exportierten Datasets die Option `-exportSettingsFile` und erstellen Sie eine `data_to_export.properties`-Datei, in der die einzelnen Tabellen und optional die Spalten für den Export angegeben sind. Bei dieser Datei handelt es sich um eine UTF-8-Datei mit null oder mehr Zeilen im Format `TABLE_NAME: COLUMN_NAME`.

<code>TABLE_NAME</code>	Der Name einer Tabelle in der Datenbank. Exportieren Sie alle Tabellen, um eine Liste der Tabellennamen anzuzeigen.
<code>COLUMN_NAME</code>	Der Name einer Spalte im angegebenen <code>TABLE_NAME</code> .

In diesem Beispiel werden mit der Datei `data_to_export.properties` Spalten aus den Tabellen ACL und ADDRESS_TRANSLATION exportiert.

```
ACL:ORG_MEMBER_ID
ACL:SHARABLE_ID
ACL:SHARABLE_TYPE
ACL:SHARING_ROLE_ID
ADDRESS_TRANSLATION:EXTERNAL_ADDRESS
ADDRESS_TRANSLATION:EXTERNAL_PORTS
ADDRESS_TRANSLATION:ID
ADDRESS_TRANSLATION:INTERNAL_PORTS
ADDRESS_TRANSLATION:NIC_ID
```

Der Befehl erwartet `$VCLLOUD_HOME/etc/data_to_export.properties` als Speicherort für die Datei, Sie können jedoch auch einen anderen Pfad angeben.

Einschränken und Sortieren der exportierten Zeilen

Für jede Tabelle können Sie die Anzahl der zu exportierenden Zeilen sowie deren Reihenfolge angeben. Verwenden Sie die Option `-exportSettingsFile` und erstellen Sie eine Datei `data_export_settings.ini`, in der einzelne Tabellen angegeben sind. Bei dieser Datei handelt es sich um eine UTF-8-Datei mit null oder mehr Einträgen im folgenden Format:

```
[TABLE_NAME]
rowlimit=int
orderby=COLUMN_NAME
```

TABLE_NAME Der Name einer Tabelle in der Datenbank. Exportieren Sie alle Tabellen, um eine Liste der Tabellennamen anzuzeigen.

COLUMN_NAME Der Name einer Spalte im angegebenen `TABLE_NAME`.

In diesem Beispiel werden mit `data_export_settings.ini` die aus der Tabelle `AUDIT_EVENT` exportierten Daten auf die ersten 10.000 Zeilen beschränkt. Die Zeilen werden dann nach dem Wert in der Spalte `event_time` sortiert.

```
[AUDIT_EVENT]
rowlimit=100000
orderby=event_time
```

Der Befehl erwartet `$VCLLOUD_HOME/etc/data_export_settings.ini` als Speicherort für die Datei, Sie können jedoch auch einen anderen Pfad angeben.

Beispiel: Es werden alle Tabellen aus der aktuellen vCloud Director -Datenbank exportiert.

In diesem Beispiel werden alle Tabellen aus der vCloud Director-Datenbank in die Datei `/tmp/dbdump` exportiert.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool dbextract -dumpFile /tmp/dbdump
This utility outputs data from your vCloud Director system
that may contain sensitive data.
Do you want to continue and output the data (y/n)?
y
Exporting data now. Please wait for the process to finish
Exported 144 of 145 tables.
```

Befehle zum Ersetzen von SSL-Zertifikaten

Mit dem Befehl `certificates` im Zellenverwaltungstool können Sie die SSL-Zertifikate der Zelle ersetzen.

Mit dem Befehl `certificates` im Zellenverwaltungstool wird der Vorgang zum Ersetzen der vorhandenen Zertifikate einer Zelle durch neue Zertifikate automatisiert, die in einem JCEKS-Keystore gespeichert wurden. Mit dem Befehl `certificates` können Sie ein selbstsigniertes Zertifikat durch ein signiertes Zertifikat ersetzen. Informationen zum Erstellen eines JCEKS-Keystores mit signierten Zertifikaten finden Sie unter [„Erstellen und Importieren eines signierten SSL-Zertifikats“](#), auf Seite 18.

Verwenden Sie zum Ersetzen der SSL-Zertifikate der Zelle einen Befehl im folgenden Format:

```
cell-management-tool certificates options
```

Tabelle 5-3. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `certificates`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keine	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--config (-c)</code>	Vollständiger Pfadname zur Datei <code>global.properties</code> der Zelle.	Standardmäßig <code>\$VCLLOUD_HOME/etc/global.properties</code> .
<code>--responses (-r)</code>	Vollständiger Pfadname zur Datei <code>responses.properties</code> der Zelle.	Standardmäßig <code>\$VCLLOUD_HOME/etc/responses.properties</code> .
<code>--keystore (-s)</code>	<i>keystore-pathname</i>	Der vollständige Pfadname zu einem JCEKS-Keystore mit den signierten Zertifikaten.
<code>--keystore-pwd (-w)</code>	<i>keystore-password</i>	Das Kennwort für den JCEKS-Keystore, auf den mit der Option <code>--keystore</code> verwiesen wird.

Beispiel: Ersetzen von Zertifikaten

Sie können die Optionen `--config` und `--responses` auslassen, sofern diese Dateien nicht aus den Standardpfaden verschoben wurden. In diesem Beispiel wird von einem Keystore unter `/tmp/new.ks` mit dem Kennwort `kspw` ausgegangen. Dieses Beispiel ersetzt die vorhandenen Zertifikate der Zelle durch die Zertifikate in `/tmp/new.ks`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool certificates -s /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

HINWEIS Sie müssen die Zelle nach dem Ersetzen der Zertifikate neu starten.

Befehle zum Generieren selbstsignierter SSL-Zertifikate

Mit dem Befehl `generate-certs` im Zellenverwaltungstool können Sie neue selbstsignierte SSL-Zertifikate für die Zelle generieren.

Mit dem Befehl `generate-certs` im Zellenverwaltungstool wird das in [„Erstellen eines selbstsignierten SSL-Zertifikats“](#), auf Seite 21 beschriebene Verfahren automatisiert.

Wenn Sie neue selbstsignierte SSL-Zertifikate generieren und diese einem neuen oder vorhandenen Keystore hinzufügen möchten, verwenden Sie eine Befehlszeile im folgenden Format:

```
cell-management-tool generate-certs options
```

Tabelle 5-4. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `generate-certs`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keine	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>-issuer (-i)</code>	<code>name=value [, name=value, ...]</code>	X.509-DN (Distinguished Name) des Zertifikatsherausgebers. Standardmäßig CN=Unknown. Wenn Sie mehrere Attribut-Wert-Paare angeben, trennen Sie sie durch Komma und schließen Sie das gesamte Argument in Anführungszeichen ein.
<code>--out (-o)</code>	<code>keystore-pathname</code>	Der vollständige Pfadname des Keystores auf diesem Host.
<code>--key-size (-s)</code>	<code>key-size</code>	Die Größe des Schlüsselpaars als Ganzzahlwert der Bits. Standardmäßig 1024.
<code>--keystore-pwd (-w)</code>	<code>keystore-password</code>	Das Kennwort für den Keystore auf diesem Host.
<code>--expiration (-x)</code>	<code>days-until-expiration</code>	Die Anzahl der Tage bis zum Ablauf der Zertifikate. Standardmäßig 365.

Beispiel: Erstellen selbstsignierter Zertifikate

In diesen beiden Beispielen wird von einem Keystore unter `/tmp/cell.ks` mit dem Kennwort `kspw` ausgegangen. Dieser Keystore wird erstellt, wenn er nicht bereits vorhanden ist.

In diesem Beispiel werden die neuen Zertifikate mit den Standardwerten erstellt. Der Name des Ausstellers wird auf CN=Unknown festgelegt. Für das Zertifikat wird eine 1024-Bit-Verschlüsselung verwendet und das Zertifikat läuft ein Jahr nach der Erstellung ab.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool generate-certs -o /tmp/cell.ks -w kspw
New keystore created and written to /tmp/cell.ks.
```

In diesem Beispiel werden die neuen Zertifikate mit benutzerdefinierten Werten für Schlüsselgröße und Ausstellernamen erstellt. Der Name des Ausstellers wird auf CN=Test, L=London, C=GB festgelegt. Für das Zertifikat wird eine 2048-Bit-Verschlüsselung verwendet und das Zertifikat läuft 90 Tage nach der Erstellung ab.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool generate-certs -o /tmp/cell.ks -w kspw -i "CN=Test, L=London, C=GB" -s 2048 -x 90
New keystore created and written to /tmp/cell.ks.
```

Wiederherstellen des Kennworts für den Systemadministrator

Wenn Sie den Benutzernamen und das Kennwort für die vCloud Director-Datenbank kennen, können Sie den Befehl `recover-password` des Zellenverwaltungstools verwenden, um das Kennwort des vCloud Director-Systemadministrators wiederherzustellen.

Mit dem Befehl `recover-password` des Zellenverwaltungstools kann ein Benutzer, der den Benutzernamen und das Kennwort der vCloud Director-Datenbank kennt, das Kennwort des vCloud Director-Systemadministrators wiederherstellen.

Verwenden Sie zum Wiederherstellen des Systemadministratorkennworts eine Befehlszeile im folgenden Format:

```
cell-management-tool recover-password options
```

Tabelle 5-5. Optionen des Zellenverwaltungstools und zugehörige Argumente, Unterbefehl `recover-password`

Option	Argument	Beschreibung
<code>--help (-h)</code>	Keine	Stellt eine Zusammenfassung der verfügbaren Befehle in dieser Kategorie bereit.
<code>--dbuser</code>	Der Benutzername des vCloud Director-Datenbankbenutzers.	Muss in der Befehlszeile angegeben werden.
<code>--dbpassword</code>	Das Kennwort des vCloud Director-Datenbankbenutzers.	Wird vom Benutzer abgefragt, falls es nicht angegeben ist.

Index

A

Aktualisieren, Workflows **37**
AMQP Broker, installieren und konfigurieren **23**

D

Datenbank
aktualisieren **44**
Informationen **15**
Oracle **15**
SQL Server **16**
unterstützte Plattformen **9**
Verbindungsdetails **28**
Dienste, starten **35**

F

Firewall, Ports und Protokolle **14**

G

Gast-Anpassung, vorbereiten **34**

H

Host, aktualisieren **46**

I

Installation
Architekturdiagramm **7**
auf dem ersten Server **26**
deinstallieren **36**
erstellen **25**
konfigurieren **49**
Überblick **7**
und Kapazitätsplanung **8**
ungefähr **5**
weiterer Server **33**
Installations-ID, angeben **51**

J

Java, erforderliche JRE-Version **11**

K

Keystore **18**
Konfiguration, Bestätigen der Einstellungen und
Beenden **51**

L

Lizenzvereinbarung **50**

M

Microsoft Sysprep **34**

N

Netzwerk
Konfigurationsanforderungen **12**
Sicherheit der **14**

P

Produktseriennummer
eingeben **50**
erhalten **50**

R

RPM-Datei, zur Überprüfung der digitalen Signatur **24**

S

Systemadministratorkonto
erstellen **50**
Kennwort wiederherstellen **60**
Systemname, angeben **51**

U

Upgrade
auf dem ersten Server **41**
Datenbank **44**

V

vCenter
aktualisieren **46**
unterstützte Versionen **9**
vShield Manager
aktualisieren **46**
installieren und konfigurieren **22**
unterstützte Versionen **9**

W

Webbrowser, unterstützte **11**

Z

Zellenverwaltungstool
Befehl "cell" **54**
Befehl "certificates" **58**
Befehl "dbextract" **55**

Befehl "generate-certs" **58**
Optionen **53**
Zertifikat
selbstsigniertes **21**
signiertes **18**