

# Guida all'installazione, alla configurazione e all'aggiornamento di vCloud Director

28 MAR 2019

VMware Cloud Director 9.7

È possibile trovare la documentazione tecnica più aggiornata sul sito Web di VMware all'indirizzo:

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

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware, Inc.**  
Centro Leoni Palazzo A  
Via Spadolini 5  
Ground Floor  
Milan, MI 20121  
tel: +39 02 30412700  
fax: +39 02 30412701  
[www.vmware.com/it](http://www.vmware.com/it)

Copyright © 2010-2020 VMware, Inc. Tutti i diritti sono riservati. [Informazioni sul copyright e sui marchi](#)

# Sommario

Guida all'installazione, alla configurazione e all'aggiornamento di vCloud Director  
7

Informazioni aggiornate 8

## **1** Panoramica delle operazioni di installazione, configurazione e aggiornamento di vCloud Director 9

Architettura di vCloud Director 9

Pianificazione della configurazione 11

## **2** Requisiti hardware e software di vCloud Director 12

Requisiti di configurazione di rete per vCloud Director 13

Requisiti di sicurezza della rete 14

## **3** Prima dell'installazione di vCloud Director o della distribuzione dell'appliance vCloud Director 17

Preparazione del database di vCloud Director 17

Configurazione di un database PostgreSQL esterno per vCloud Director su Linux 18

Configurazione di un database Microsoft SQL Server esterno per vCloud Director per Linux 19

Preparazione dello storage del server di trasferimento 21

Download e installazione della chiave pubblica VMware 24

Installazione e configurazione di NSX Data Center for vSphere per vCloud Director 24

Installazione e configurazione di NSX-T Data Center per vCloud Director 25

## **4** Creazione e gestione di certificati SSL per vCloud Director in Linux 27

Prima di creare certificati SSL per vCloud Director in Linux 27

Creazione di certificati SSL autofirmati per vCloud Director in Linux 28

Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione per vCloud Director in Linux 29

Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione con chiavi private importate per vCloud Director in Linux 33

## **5** Installazione di vCloud Director in Linux 35

Installazione di vCloud Director nel primo membro di un gruppo di server 36

Configurazione delle connessioni di rete e database 38

Riferimento alla configurazione interattiva 40

Riferimenti per la configurazione automatica 42

Protezione e riutilizzo del file di risposta 45

Installazione di vCloud Director in un membro aggiuntivo di un gruppo di server 46

Impostazione di vCloud Director 48

**6 Distribuzione dell'appliance vCloud Director 51**

Distribuzioni dell'appliance e configurazione della disponibilità elevata del database 53

Prerequisiti per la distribuzione dell'appliance di vCloud Director 56

Distribuzione dell'appliance vCloud Director mediante vSphere Web Client o vSphere Client 56

Avviamento della distribuzione dell'appliance vCloud Director 57

Personalizzazione dell'appliance di vCloud Director e completamento della distribuzione 59

Distribuzione dell'appliance vCloud Director tramite VMware OVF Tool 61

**7 Creazione e gestione di certificati SSL dell'appliance vCloud Director 68**

Distribuzione dell'appliance vCloud Director con certificati con caratteri jolly firmati per la comunicazione HTTPS e proxy console 68

Creazione e importazione di certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director 70

Importazione di chiavi private e certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director 74

Sostituzione di un certificato autofirmato dell'interfaccia utente di gestione dell'appliance vCloud Director e di un database PostgreSQL incorporato 76

Rinnovo dei certificati dell'appliance vCloud Director 77

**8 Configurazione dell'appliance vCloud Director 79**

Visualizzazione dello stato delle celle in un cluster ad alta disponibilità del database 79

Ripristino da un errore di database primario in un cluster ad alta disponibilità 80

Backup e ripristino del database integrato dell'appliance vCloud Director 81

Backup del database incorporato dell'appliance vCloud Director 81

Ripristino di un ambiente dell'appliance vCloud Director con una configurazione del database ad alta disponibilità 82

Ripristino di un ambiente dell'appliance vCloud Director senza configurare un database a disponibilità elevata 85

Configurazione dell'accesso esterno al database di vCloud Director 88

Abilitazione o disabilitazione dell'accesso SSH all'appliance di vCloud Director 89

Modifica delle impostazioni DNS dell'appliance vCloud Director 89

Modifica delle route statiche per le interfacce di rete dell'appliance vCloud Director 90

Script di configurazione nell'appliance vCloud Director 92

Modifica delle configurazioni di PostgreSQL nell'appliance di vCloud Director 92

**9 Utilizzo di Replication Manager Tool Suite in una configurazione di cluster a disponibilità elevata 94**

Verifica dello stato di connettività di un cluster a disponibilità elevata del database 95

Verifica dello stato di replica di un nodo in un cluster a disponibilità elevata del database 96

Verifica dello stato di un cluster a disponibilità elevata del database 97

	Rilevamento di un precedente nodo primario che torna online in un cluster a disponibilità elevata	98
	Scambio dei ruoli tra cella primaria e cella di standby in un cluster a disponibilità elevata del database	100
	Annullamento della registrazione di un nodo di standby non riuscito o irraggiungibile in un cluster a disponibilità elevata del database	101
	Annullamento della registrazione di una cella primaria non riuscita in un cluster a disponibilità elevata del database	102
	Annullamento della registrazione di una cella di standby in esecuzione in un cluster a disponibilità elevata del database	103
<b>10</b>	<b>Dopo avere installato vCloud Director o distribuito l'appliance vCloud Director</b>	<b>105</b>
	Installazione dei file Microsoft Sysprep nei server	105
	Personalizzazione degli endpoint pubblici	106
	Installazione e configurazione di un broker AMQP RabbitMQ	109
	Installazione e configurazione di un database Cassandra per l'archiviazione dei dati relativi alle metriche cronologiche	110
	Esecuzione di configurazioni aggiuntive nel database PostgreSQL esterno	112
<b>11</b>	<b>Aggiornamento di vCloud Director e applicazione di patch all'appliance di vCloud Director</b>	<b>115</b>
	Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director	117
	Aggiornamento manuale di un'installazione di vCloud Director	120
	Aggiornamento di una cella di vCloud Director	121
	Esecuzione dell'aggiornamento del database vCloud Director	124
	Riferimento dell'utilità di aggiornamento del database	125
	Applicazione di patch alla distribuzione dell'appliance vCloud Director	128
<b>12</b>	<b>Migrazione all'appliance vCloud Director</b>	<b>131</b>
	Migrazione di vCloud Director con un database Microsoft SQL esterno all'appliance vCloud Director	131
	Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director	135
<b>13</b>	<b>Dopo l'aggiornamento o la migrazione di vCloud Director</b>	<b>140</b>
	Aggiornamento di ciascun NSX Manager associato a un sistema vCenter Server collegato	140
	Aggiornamento dei sistemi vCenter Server, degli host ESXi e degli NSX Edge	141
	Nuovi diritti in questa versione	143
<b>14</b>	<b>Risoluzione dei problemi relativi all'appliance vCloud Director</b>	<b>144</b>
	Esame dei file di registro nell'appliance vCloud Director	144
	La cella di vCloud Director non viene avviata dopo la distribuzione dell'appliance	145
	La riconfigurazione del servizio vCloud Director non riesce durante la migrazione o il ripristino dell'appliance vCloud Director	145

[Utilizzo dei file di registro per risolvere i problemi relativi agli aggiornamenti e alle patch di vCloud Director](#) 146

[Il controllo della disponibilità degli aggiornamenti di vCloud Director non riesce](#) 146

[L'installazione dell'aggiornamento più recente di vCloud Director non riesce](#) 147

## **15** Disinstallazione del software vCloud Director 148

# Guida all'installazione, alla configurazione e all'aggiornamento di vCloud Director

*Guida all'installazione, alla configurazione e all'aggiornamento di vCloud Director* fornisce informazioni sull'installazione e l'aggiornamento del software VMware vCloud Director<sup>®</sup> for Service Providers e sulla sua configurazione per l'utilizzo con VMware vSphere<sup>®</sup>, VMware NSX<sup>®</sup> for vSphere<sup>®</sup> e VMware NSX-T<sup>™</sup> Data Center.

## Destinatari della guida

La *Guida all'installazione, alla configurazione e all'aggiornamento di vCloud Director* è rivolta a chiunque desideri installare o aggiornare il software vCloud Director. Le informazioni in essa contenute sono state redatte per gli amministratori di sistema esperti che hanno familiarità con Linux, Windows, le reti IP e con vSphere.

# Informazioni aggiornate

Questa *Guida all'installazione, alla configurazione e all'aggiornamento di vCloud Director* viene aggiornata a ogni versione del prodotto oppure quando necessario.

Nella tabella viene riportata la cronologia degli aggiornamenti di *Guida all'installazione, alla configurazione e all'aggiornamento di vCloud Director*.

Versione	Descrizione
11 GIU 2019	<ul style="list-style-type: none"><li>■ Aggiunto l'argomento <a href="#">Rinnovo dei certificati dell'appliance vCloud Director</a>.</li><li>■ Aggiunto il capitolo <a href="#">Capitolo 9 Utilizzo di Replication Manager Tool Suite in una configurazione di cluster a disponibilità elevata</a>.</li></ul>
10 MAG 2019	<ul style="list-style-type: none"><li>■ Aggiunta del capitolo <a href="#">#unique_5</a>.</li><li>■ È stato aggiunto l'argomento <a href="#">Utilizzo dei file di registro per risolvere i problemi relativi agli aggiornamenti e alle patch di vCloud Director</a>.</li><li>■ È stato aggiunto l'argomento <a href="#">Il controllo della disponibilità degli aggiornamenti di vCloud Director non riesce</a>.</li><li>■ È stato aggiunto l'argomento <a href="#">L'installazione dell'aggiornamento più recente di vCloud Director non riesce</a>.</li></ul>
05 apr 2019	<ul style="list-style-type: none"><li>■ Aggiunta del capitolo <a href="#">Capitolo 12 Migrazione all'appliance vCloud Director</a>.</li><li>■ È stato aggiunto l'argomento <a href="#">Ripristino di un ambiente dell'appliance vCloud Director con una configurazione del database ad alta disponibilità</a>.</li><li>■ Argomento <a href="#">Distribuzioni dell'appliance e configurazione della disponibilità elevata del database</a> aggiornato per migliorare la grafica e il passaggio 2 nei flussi di lavoro.</li><li>■ Argomento <a href="#">Esame dei file di registro nell'appliance vCloud Director</a> aggiornato per aggiungere informazioni sul file che contiene i parametri OVF della distribuzione.</li></ul>
28 MAR 2019	Versione iniziale.



# Panoramica delle operazioni di installazione, configurazione e aggiornamento di vCloud Director

# 1

È possibile creare un gruppo di server vCloud Director installando il software vCloud Director in uno o più server Linux o distribuendo una o più istanze dell'appliance vCloud Director. Durante il processo di installazione, eseguire la configurazione iniziale di vCloud Director, che consente di stabilire le connessioni di rete e database.

Il software vCloud Director per Linux richiede un database esterno, mentre l'appliance vCloud Director utilizza un database PostgreSQL incorporato.

Dopo aver creato il gruppo di server vCloud Director, integrare l'installazione di vCloud Director con le risorse di vSphere. Per le risorse di rete, vCloud Director può utilizzare NSX Data Center for vSphere, NSX-T Data Center o entrambi.

Quando si aggiorna un'installazione di vCloud Director esistente, aggiornare il software vCloud Director e lo schema del database, mantenendo le relazioni esistenti tra i server, il database e vSphere.

Quando si esegue la migrazione di un'installazione di vCloud Director esistente su Linux all'appliance vCloud Director, si aggiorna il software vCloud Director e si esegue la migrazione del database nel database incorporato nell'appliance.

Questo capitolo include i seguenti argomenti:

- [Architettura di vCloud Director](#)
- [Pianificazione della configurazione](#)

## Architettura di vCloud Director

Un gruppo di server vCloud Director è costituito da uno o più server vCloud Director installati su Linux o distribuzioni dell'appliance di vCloud Director. Su ogni server del gruppo viene eseguita una raccolta di servizi denominata cella vCloud Director. Tutte le celle condividono un singolo database di vCloud Director e uno storage del server di trasferimento e si connettono a vSphere e alle risorse di rete.

---

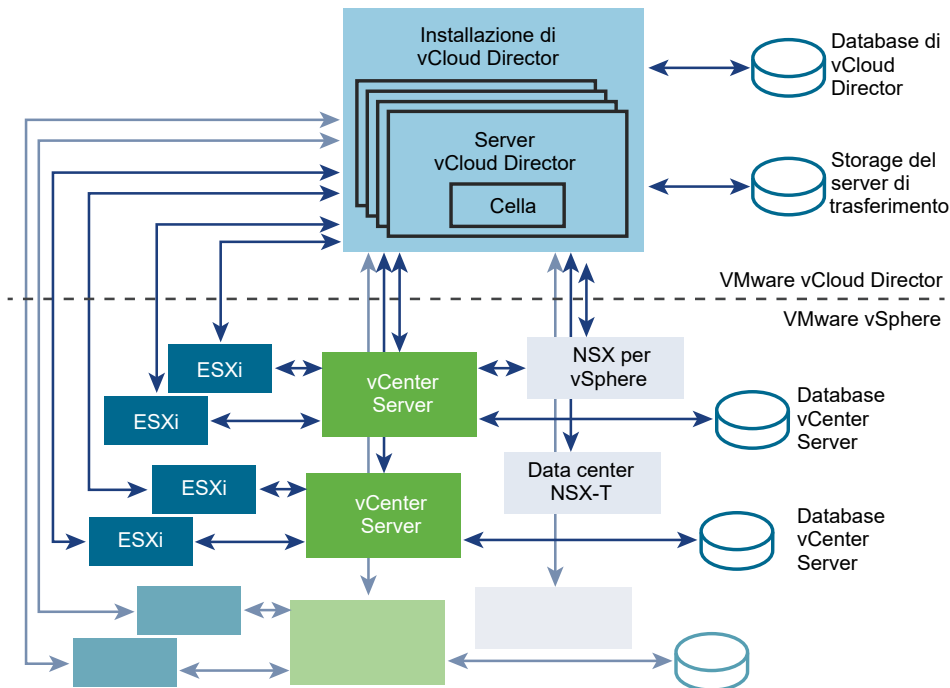
**Importante** Le installazioni vCloud Director miste su Linux e le distribuzioni di appliance vCloud Director in un gruppo di server non sono supportate.

---

Per garantire l'alta disponibilità di vCloud Director, è necessario installare almeno due celle di vCloud Director in un gruppo di server. Quando si utilizza un bilanciamento del carico di terze parti, è possibile garantire un failover automatico senza tempi di inattività.

È possibile connettere un'installazione di vCloud Director a più sistemi VMware vCenter Server<sup>®</sup> e agli host VMware ESXi<sup>™</sup> che gestiscono. Per i servizi di rete, vCloud Director può utilizzare NSX Data Center for vSphere associato a vCenter Server oppure è possibile registrare NSX-T Data Center in vCloud Director. Sono supportati anche NSX Data Center for vSphere e NSX-T Data Center misti.

Figura 1-1. Diagramma dell'architettura di vCloud Director



Un gruppo di server vCloud Director installato su Linux utilizza un database esterno.

Un gruppo di server vCloud Director costituito da distribuzioni dell'appliance utilizza il database incorporato nel primo membro del gruppo di server. È possibile configurare un database vCloud Director ad alta disponibilità distribuendo due istanze dell'appliance come celle di standby nello stesso gruppo di server. Vedere [Distribuzioni dell'appliance e configurazione della disponibilità elevata del database](#).

Figura 1-2. Appliance di vCloud Director che includono un cluster a disponibilità elevata di database incorporato

Il processo di installazione e configurazione di vCloud Director crea le celle, le connette al database condiviso e allo storage del server di trasferimento e crea l'account di **amministratore di sistema**. L'**amministratore di sistema** stabilisce quindi le connessioni al sistema vCenter Server, agli host ESXi e alle istanze di NSX Manager. Per informazioni sull'aggiunta di vSphere e delle risorse di rete, vedere *Guida per gli amministratori di vCloud Director*.

## Pianificazione della configurazione

vSphere fornisce capacità di rete, calcolo e storage a vCloud Director. Prima di iniziare l'installazione, valutare la capacità di vSphere e vCloud Director richiesta dal cloud, quindi pianificare una configurazione in grado di supportarla.

I requisiti di configurazione dipendono da molti fattori, tra cui il numero di organizzazioni incluse nel cloud, il numero di utenti presenti in ogni organizzazione e il livello di attività di tali utenti. Le linee guida seguenti possono essere utili come punto di partenza per la maggior parte delle configurazioni:

- Allocare una cella vCloud Director per ogni sistema vCenter Server che si desidera rendere accessibile nel cloud.
- Assicurarsi che tutti i server Linux di vCloud Director di destinazione soddisfino almeno i requisiti minimi di memoria e storage descritti dettagliatamente in *Note di rilascio di vCloud Director*.
- Se si intende installare vCloud Director in Linux, configurare il database di vCloud Director come descritto in [Preparazione del database di vCloud Director](#).

# Requisiti hardware e software di vCloud Director

## 2

Ogni server incluso in un gruppo di server vCloud Director deve soddisfare determinati requisiti hardware e software. È inoltre necessario che un database supportato sia accessibile da tutti i membri del gruppo. Ogni gruppo di server richiede l'accesso a un sistema vCenter Server, un'istanza di NSX Manager e uno o più host ESXi.

## Compatibilità con altri prodotti VMware

Per le informazioni più aggiornate sulla compatibilità tra vCloud Director e altri prodotti VMware, vedere le *Matrici di compatibilità dei prodotti VMware* alla pagina [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php).

## Requisiti di configurazione di vSphere

Le istanze di vCenter Server e gli host ESXi da utilizzare con vCloud Director devono soddisfare determinati requisiti di configurazione.

- Le reti vCenter Server da utilizzare come reti esterne o come pool di reti di vCloud Director devono essere disponibili per tutti gli host in qualsiasi cluster da utilizzare con vCloud Director. La possibilità di rendere tali reti disponibili per tutti gli host di un data center semplifica l'attività di aggiunta di nuove istanze di vCenter Server a vCloud Director.
- Le istanze di vSphere Distributed Switch sono necessarie per reti e pool di reti isolati supportati da NSX Data Center for vSphere.
- I cluster vCenter Server utilizzati con vCloud Director devono specificare un livello di automazione **completo** di vSphere DRS. Se abilitato, Storage DRS può essere configurato con qualsiasi livello di automazione.
- Le istanze di vCenter Server devono considerare attendibili i rispettivi host. Tutti gli host in tutti i cluster gestiti da vCloud Director devono essere configurati in modo da richiedere certificati host verificati. In particolare, è necessario determinare, confrontare e selezionare le identificazioni personali di tutti gli host. Per ulteriori informazioni, vedere la sezione sulla Configurazione delle impostazioni SSL nella documentazione relativa a *vCenter Server e gestione degli host*.

## Requisiti di licenza di vSphere

vCloud Director Service Provider Bundle include le licenze di vSphere necessarie.

## Piattaforme, database e browser supportati

Vedere le *Note di rilascio di vCloud Director 9.7* per informazioni sulle piattaforme server, i browser, i server LDAP e i database supportati da questa versione di vCloud Director.

## Requisiti di spazio su disco, memoria e CPU

I requisiti fisici come CPU, memoria e spazio su disco per le celle di vCloud Director sono elencati nelle *Note di rilascio di vCloud Director 9.7*.

## Storage condiviso

NFS o un altro volume di storage condiviso per il servizio di trasferimento di vCloud Director. Il volume dello storage deve essere espandibile e accessibile per tutti i server nel gruppo di server.

Questo capitolo include i seguenti argomenti:

- [Requisiti di configurazione di rete per vCloud Director](#)
- [Requisiti di sicurezza della rete](#)

## Requisiti di configurazione di rete per vCloud Director

Il funzionamento sicuro e affidabile di vCloud Director dipende dalla presenza di una rete sicura e affidabile che supporti la ricerca diretta e inversa dei nomi host, un servizio di riferimento orario di rete e altri servizi. Per poter installare vCloud Director, è necessario che la rete soddisfi i requisiti elencati di seguito.

La rete che connette i server vCloud Director, il server del database, i sistemi vCenter Server e i componenti NSX deve soddisfare diversi requisiti:

### Indirizzi IP

Ciascun server vCloud Director deve supportare due endpoint SSL differenti. Un endpoint è per il servizio HTTP. L'altro è per il servizio proxy della console. Entrambi possono essere costituiti da indirizzi IP separati o da un singolo indirizzo IP con due porte diverse. Per creare tali indirizzi è possibile utilizzare gli alias IP o più interfacce di rete. Non utilizzare il comando `ip addr add` di Linux per creare il secondo indirizzo.

L'appliance vCloud Director utilizza il suo indirizzo IP `eth0` con la porta personalizzata 8443 per il servizio proxy della console.

### Indirizzo proxy della console

L'indirizzo IP configurato come endpoint proxy della console non deve trovarsi dietro un proxy inverso o un servizio di bilanciamento del carico con terminazione SSL. Tutte le richieste proxy della console devono essere inoltrate direttamente all'indirizzo IP proxy della console.

Per un'installazione con un singolo indirizzo IP, è possibile personalizzare l'indirizzo proxy della console dalla console Web di vCloud Director. Ad esempio, per l'appliance vCloud Director, è necessario personalizzare l'indirizzo proxy della console impostandolo su `vcloud.example.com:8443`.

### Servizio di riferimento orario di rete

È necessario utilizzare un servizio di riferimento orario di rete quale NTP per sincronizzare gli orologi di tutti i server vCloud Director, incluso il server di database. La massima deviazione consentita tra gli orologi di server sincronizzati è pari a 2 secondi.

### Fusi orari del server

Tutti i server di vCloud Director, compreso il server del database, devono essere configurati con lo stesso fuso orario.

### Risoluzione dei nomi host

Tutti i nomi host specificati durante l'installazione e la configurazione devono essere risolvibili mediante DNS utilizzando la ricerca diretta e inversa del nome di dominio completo o del nome host non qualificato. Ad esempio, per un host denominato `vcloud.example.com`, è necessario eseguire entrambi i comandi seguenti su un host vCloud Director:

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

Inoltre, se l'host `vcloud.example.com` presenta l'indirizzo IP 192.168.1.1, il comando seguente deve restituire `vcloud.example.com`:

```
nslookup 192.168.1.1
```

Per l'appliance è necessaria la ricerca DNS inversa dell'indirizzo IP `eth0`. Il seguente comando deve avere esito positivo nell'ambiente:

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

## Requisiti di sicurezza della rete

Il funzionamento sicuro di vCloud Director richiede un ambiente di rete sicuro. Prima di iniziare la procedura di installazione di vCloud Director, configurare l'ambiente di rete ed eseguirne il test.

Connettere tutti i server vCloud Director a una rete sicura e monitorata. Le connessioni di rete di vCloud Director presentano diversi requisiti aggiuntivi:

- Non connettere vCloud Director direttamente alla rete Internet pubblica. Proteggere sempre le connessioni di rete di vCloud Director con un firewall. Per le connessioni in entrata deve essere aperta solo la porta 443 (HTTPS) e, se necessario, è possibile aprire anche le porte 22 (SSH) e 80 (HTTP). Inoltre, `cell-management-tool` richiede l'accesso all'indirizzo di loopback della cella. Tutto il resto del traffico in entrata da una rete pubblica, incluse le richieste a JMX (porta 8999), devono essere rifiutate dal firewall.

**Tabella 2-1. Porte che devono consentire il passaggio di pacchetti in entrata dagli host vCloud Director**

Porta	Protocollo	Commenti
111	TCP, UDP	Portmapper NFS utilizzato dal servizio di trasferimento
920	TCP, UDP	rpc.statd NFS utilizzato dal servizio di trasferimento
61611	TCP	AMQP
61616	TCP	AMQP

- Non connettere le porte utilizzate per le connessioni in uscita alla rete pubblica.

**Tabella 2-2. Porte che devono consentire il passaggio di pacchetti in uscita dagli host vCloud Director**

Porta	Protocollo	Commenti
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	Portmapper NFS utilizzato dal servizio di trasferimento
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	Connessioni di vCenter, NSX Manager e ESXi che utilizzano la porta standard. Se per questi servizi è stata scelta una porta differente, disabilitare la connessione alla porta 443 e abilitarla per la porta scelta.
514	UDP	Facoltativa. Consente l'utilizzo di syslog.
902	TCP	Connessioni vCenter ed ESXi.
903	TCP	Connessioni vCenter ed ESXi.
920	TCP, UDP	rpc.statd NFS utilizzato dal servizio di trasferimento.
1433	TCP	Porta di database predefinita di Microsoft SQL Server.

**Tabella 2-2. Porte che devono consentire il passaggio di pacchetti in uscita dagli host vCloud Director (continua)**

<b>Porta</b>	<b>Protocollo</b>	<b>Commenti</b>
5672	TCP, UDP	Facoltativa. Messaggi AMQP per le estensioni dei task.
61611	TCP	AMQP
61616	TCP	AMQP

- Instradare il traffico tra server vCloud Director e i seguenti server su una rete privata dedicata.
  - Server di database di vCloud Director
  - RabbitMQ
  - Cassandra
- Se possibile, instradare il traffico tra server vCloud Director, vSphere e NSX su una rete privata dedicata.
- I commutatori virtuali e i commutatori virtuali distribuiti che supportano le reti di provider devono essere isolati tra loro in quanto non possono condividere lo stesso segmento di rete fisica di livello 2.
- Utilizzare NFSv4 per lo storage del servizio di trasferimento. La versione di NFS più comune, NFSv3, non offre la crittografia in transito, il che in alcune configurazioni potrebbe abilitare l'individuazione o la manomissione dei dati durante il trasferimento. Le minacce inerenti la versione NFSv3 sono descritte nel white paper SANS [NFS Security in Both Trusted and Untrusted Environments](#). Informazioni aggiuntive sulla configurazione e la protezione del servizio di trasferimento di vCloud Director sono disponibili nell'articolo [2086127](#) della Knowledge Base di VMware.



# Prima dell'installazione di vCloud Director o della distribuzione dell'appliance vCloud Director

## 3

Prima di installare vCloud Director in un server Linux o di distribuire l'appliance vCloud Director, è necessario preparare l'ambiente.

Questo capitolo include i seguenti argomenti:

- [Preparazione del database di vCloud Director](#)
- [Preparazione dello storage del server di trasferimento](#)
- [Download e installazione della chiave pubblica VMware](#)
- [Installazione e configurazione di NSX Data Center for vSphere per vCloud Director](#)
- [Installazione e configurazione di NSX-T Data Center per vCloud Director](#)

## Preparazione del database di vCloud Director

Le celle di vCloud Director utilizzano un database per archiviare le informazioni condivise. Prima di installare vCloud Director su Linux, è necessario installare e configurare un database di vCloud Director esterno. L'appliance vCloud Director utilizza un database PostgreSQL incorporato.

Per informazioni sui database vCloud Director supportati, vedere le [matrici di interoperabilità dei prodotti VMware](#).

Indipendentemente dal software di database che si decide di utilizzare, è necessario creare uno schema di database dedicato distinto che possa essere utilizzato da vCloud Director. vCloud Director non può infatti condividere uno schema di database con altri prodotti VMware.

---

**Importante** vCloud Director supporta connessioni SSL solo a un database PostgreSQL. È possibile abilitare SSL nel database PostgreSQL durante una configurazione automatica di connessioni di rete e database o dopo la creazione del gruppo di server di vCloud Director. Vedere [Riferimenti per la configurazione automatica](#) e [Esecuzione di configurazioni aggiuntive nel database PostgreSQL esterno](#).

---

## Configurazione di un database PostgreSQL esterno per vCloud Director su Linux

I database PostgreSQL hanno requisiti di configurazione specifici quando vengono utilizzati con vCloud Director. Prima di installare vCloud Director su Linux, è necessario installare e configurare un'istanza del database e creare l'account utente del database di vCloud Director.

---

**Nota** Solo vCloud Director su Linux utilizza un database esterno. L'appliance vCloud Director utilizza il database PostgreSQL incorporato.

---

### Prerequisiti

È necessario conoscere i comandi, gli script e il funzionamento di PostgreSQL.

### Procedura

#### 1 Configurare il server di database.

Un server di database con 16 GB di memoria, 100 GB di storage e 4 CPU è appropriato per i gruppi di server vCloud Director tipici.

#### 2 Installare una distribuzione di PostgreSQL supportata nel server del database.

- Il valore `SERVER_ENCODING` del database deve essere UTF-8. Questo valore viene stabilito quando si installa il database e corrisponde sempre alla codifica utilizzata dal sistema operativo server del database.
- Utilizzare il comando `initdb` di PostgreSQL per impostare il valore di `LC_COLLATE` e `LC_CTYPE` su `en_US.UTF-8`. Ad esempio:

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

#### 3 Creare l'utente del database.

Il comando seguente crea l'utente `vcloud`.

```
create user vcloud;
```

#### 4 Creare l'istanza del database e assegnarle un proprietario.

Utilizzare un comando simile al seguente per specificare un utente del database denominato `vcloud` come proprietario del database.

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

#### 5 Assegnare una password all'account del proprietario del database.

Il comando seguente assegna la password `vcloudpass` al proprietario del database `vcloud`.

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

## 6 Consentire al proprietario del database di eseguire il login nel database.

Il comando seguente assegna l'opzione `login` al proprietario del database `vcloud`.

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

### Operazioni successive

Dopo la creazione del gruppo di server di vCloud Director, è possibile configurare il database PostgreSQL per richiedere connessioni SSL dalle celle di vCloud Director e regolare alcuni parametri di database per ottimizzare le prestazioni. Vedere [Esecuzione di configurazioni aggiuntive nel database PostgreSQL esterno](#).

## Configurazione di un database Microsoft SQL Server esterno per vCloud Director per Linux

I database SQL Server presentano requisiti di configurazione specifici quando vengono utilizzati con vCloud Director. Prima di installare vCloud Director su Linux, è necessario installare e configurare un'istanza del database e creare l'account utente del database di vCloud Director.

Le prestazioni del database di vCloud Director rappresentano un fattore importante per le prestazioni e la scalabilità generali di vCloud Director. In vCloud Director viene utilizzato il file `tmpdb` di SQL Server per l'archiviazione di set di risultati di grandi dimensioni, l'ordinamento dei dati e la gestione dei dati letti e modificati simultaneamente. La dimensione di questo file può aumentare notevolmente quando si verifica un notevole carico simultaneo per vCloud Director. È consigliabile creare il file `tmpdb` in un volume dedicato con prestazioni di lettura e scrittura veloci. Per ulteriori informazioni sul file `tmpdb` e sulle prestazioni di SQL Server, vedere <http://msdn.microsoft.com/en-us/library/ms175527.aspx>.

---

**Nota** Solo vCloud Director su Linux utilizza un database esterno. L'appliance vCloud Director utilizza il database PostgreSQL incorporato.

---

### Prerequisiti

- È necessario avere familiarità con i comandi, gli script e il funzionamento di Microsoft SQL Server.
- Per configurare Microsoft SQL Server, accedere al computer host SQL Server utilizzando le credenziali dell'amministratore. È possibile configurare SQL Server per l'esecuzione con l'identità `LOCAL_SYSTEM` o con qualsiasi identità che disponga del privilegio per l'esecuzione di un servizio Windows.
- Vedere l'articolo della Knowledge Base di VMware <https://kb.vmware.com/kb/2148767> per informazioni sull'uso dei Gruppi di disponibilità Always On di Microsoft SQL Server con il database di vCloud Director.

## Procedura

### 1 Configurare il server di database.

Un server di database configurato con 16 GB di memoria, 100 GB di storage e 4 CPU dovrebbe essere adatto per la maggior parte dei gruppi di server vCloud Director.

### 2 Specificare l'autenticazione Mixed Mode durante l'installazione di SQL Server.

L'autenticazione di Windows non è supportata quando si utilizza SQL Server con vCloud Director.

### 3 Creare l'istanza di database.

Lo script seguente consente di creare file di database e di registro, specificando la sequenza di confronto appropriata.

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

I valori visualizzati per SIZE sono indicativi. Potrebbe essere necessario utilizzare valori più alti.

### 4 Impostare il livello di isolamento della transazione.

Lo script seguente consente di impostare il livello di isolamento del database su READ\_COMMITTED\_SNAPSHOT.

```
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
```

Per ulteriori informazioni sull'isolamento delle transazioni, vedere <http://msdn.microsoft.com/en-us/library/ms173763.aspx>.

### 5 Creare l'account utente del database vCloud Director.

Lo script seguente consente di creare il nome utente del database vcloud con la password 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 Assegnare i permessi all'account utente del database vCloud Director.

Lo script seguente consente di assegnare il ruolo `db_owner` all'utente del database creato in [Passaggio 5](#).

```

USE [vcloud]
GO
sp_addrolemember [db_owner], [vcloud]
GO

```

## Preparazione dello storage del server di trasferimento

Per fornire uno storage temporaneo per i caricamenti, i download e gli elementi di catalogo pubblicati o sottoscritti esternamente, è necessario che un NFS o un altro volume di storage condiviso sia accessibile da tutti i server in un gruppo di server vCloud Director.

**Importante** L'appliance vCloud Director supporta solo il tipo di storage condiviso NFS. Il processo di distribuzione dell'appliance implica il montaggio dello storage NFS condiviso del server di trasferimento.

Quando NFS viene utilizzato per lo storage del server di trasferimento, è necessario configurare ogni cella di vCloud Director nel gruppo di server vCloud Director in modo che monti e utilizzi lo storage del server di trasferimento basato su NFS. Sono necessarie autorizzazioni di utenti e gruppi specifici per configurare ciascuna cella per montare la posizione basata su NFS e utilizzarla come storage del server di trasferimento.

Ogni membro del gruppo server deve montare questo volume nello stesso punto di montaggio, che in genere corrisponde a `/opt/vmware/vcloud-director/data/transfer`. Lo spazio di questo volume viene impiegato in due modi:

- Durante i trasferimenti, i caricamenti e i download occupano questo storage. Al termine del trasferimento, i caricamenti e i download vengono rimossi dallo storage. I trasferimenti che non presentano avanzamenti per 60 minuti sono contrassegnati come scaduti ed eliminati dal sistema. Le immagini trasferite possono essere di grandi dimensioni, quindi è utile assegnare a questo utilizzo varie centinaia di gigabyte.

- Gli elementi dei cataloghi che sono pubblicati esternamente e per cui è abilitata la memorizzazione nella cache dei contenuti pubblicati, occupano questo storage. Gli elementi dei cataloghi che sono pubblicati esternamente ma non abilitano la memorizzazione nella cache, non occupano questo storage. Se si consente alle organizzazioni nel cloud di creare cataloghi pubblicati esternamente, è possibile supporre che centinaia o addirittura migliaia di elementi di catalogo richiedano spazio in questo volume. La dimensione di ciascun elemento di catalogo è all'incirca la dimensione di una macchina virtuale in formato OVF compresso.

---

**Nota** Il volume dello storage del server di trasferimento deve avere capacità di espansione futura.

---

## In che modo vCloud Director utilizza le autorizzazioni del file system per la posizione di storage del server di trasferimento

Per tutte le celle di vCloud Director nel gruppo di server di vCloud Director:

- Nelle operazioni standard del cloud, come il caricamento di elementi nel catalogo, il daemon della cella vCloud Director scrive i file nello storage del server di trasferimento e legge i file da tale storage utilizzando l'utente **vcloud** nel gruppo **vcloud**. L'utente **vcloud** scrive i file con `umask 0077`. Quando il programma di installazione di vCloud Director viene eseguito e installa il software vCloud Director in un membro del gruppo di server, crea anche l'utente **vcloud** e il gruppo **vcloud**.
- Lo script dell'agente di raccolta dati del registro di vCloud Director `vmware-vcd-support` può raccogliere i registri da tutte le celle di vCloud Director in un'unica operazione e raggruppare i registri in un singolo file `tar.gz`. Quando si esegue lo script, scrive il file `tar.gz` risultante in una directory nella posizione di storage del server di trasferimento utilizzando l'ID utente dell'utente che richiama lo script. Per impostazione predefinita, l'unico utente che dispone delle autorizzazioni per eseguire lo script è l'utente **root**.
- L'utente **root** nella cella esegue lo script che scrive il file `tar.gz` nella directory `vmware-vcd-support` nella posizione di storage del server di trasferimento. Se si desidera utilizzare le opzioni per più celle per raccogliere i registri da tutte le celle contemporaneamente, l'utente **root** deve disporre di un'autorizzazione di lettura per recuperare il bundle del registro di diagnostica `tar.gz`.

## Requisiti per la configurazione del server NFS

Esistono requisiti specifici per la configurazione del server NFS, in modo che vCloud Director possa scrivere file in una posizione di storage del server di trasferimento basata su NFS e leggere i file da tale posizione. In base a questi requisiti, l'utente **vcloud** può eseguire le operazioni standard del cloud e l'utente **root** può eseguire la raccolta di registri da più celle.

- L'elenco di esportazione per il server NFS deve consentire a ciascun membro del server nel gruppo di server di vCloud Director l'accesso in lettura e scrittura alla posizione condivisa identificata nell'elenco di esportazione. Questa funzionalità consente all'utente **vcloud** di scrivere file nella posizione condivisa e di leggere file da tale posizione.

- Il server NFS deve consentire l'accesso in lettura e scrittura alla posizione condivisa dall'account di sistema **root** in ciascun server nel gruppo di server di vCloud Director. Questa funzionalità consente di raccogliere i registri da tutte le celle contemporaneamente in un singolo bundle utilizzando lo script `vmware-vcd-support` con le relative opzioni per più celle. È possibile soddisfare questo requisito utilizzando `no_root_squash` nella configurazione di esportazione NFS per questa posizione condivisa.

Ad esempio, se il server NFS dispone dell'indirizzo IP 192.168.120.7 e di una directory denominata `vCDspace` come spazio di trasferimento per il gruppo di server di vCloud Director con posizione `/nfs/vCDspace`, per esportare questa directory è necessario assicurarsi che la relativa proprietà e le autorizzazioni siano **root:root** e **750**. Il metodo per consentire l'accesso in lettura e scrittura alla posizione condivisa per due celle denominate `vcd-cell1-IP` e `vcd-cell2-IP` è il metodo `no_root_squash`. È necessario aggiungere una riga al file `/etc/exports`.

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

Non deve essere presente alcuno spazio tra l'indirizzo IP di ciascuna cella e la relativa parentesi aperta immediatamente successiva nella riga di esportazione. Se il server NFS viene riavviato mentre le celle scrivono i dati nella posizione condivisa, l'uso dell'opzione `sync` nella configurazione di esportazione impedisce il danneggiamento dei dati nella posizione condivisa. L'uso dell'opzione `no_subtree_check` nella configurazione di esportazione migliora l'affidabilità quando viene esportata una sottodirectory di un file system.

Ogni server nel gruppo di server di vCloud Director deve essere autorizzato a montare la condivisione NFS controllando l'elenco di esportazione per l'esportazione NFS. È possibile esportare il montaggio eseguendo `exportfs -a` per esportare nuovamente tutte le condivisioni NFS. I daemon NFS `rpcinfo -p localhost` o `service nfs status` devono essere in esecuzione sul server.

## Considerazioni sulla pianificazione dell'aggiornamento dell'installazione di vCloud Director a una versione successiva

Durante l'aggiornamento di un gruppo di server di vCloud Director, si esegue il file di installazione per la versione aggiornata per aggiornare tutti i membri del gruppo di server di vCloud Director. Per comodità, alcune organizzazioni scelgono di scaricare il file di installazione per l'aggiornamento nella posizione di storage del server di trasferimento ed eseguirlo da tale posizione, perché tutte le celle possono accedervi. Poiché l'utente **root** deve essere utilizzato per eseguire il file di installazione dell'aggiornamento, se si desidera utilizzare la posizione di storage del server di trasferimento per l'esecuzione di un aggiornamento, è necessario assicurarsi che l'utente **root** possa eseguire il file di installazione dell'aggiornamento quando si esegue l'aggiornamento. Se non è possibile eseguire l'aggiornamento come utente **root**, il file deve essere copiato in un'altra posizione in cui può essere eseguito come utente **root**, ad esempio un'altra directory esterna al montaggio NFS.

## Download e installazione della chiave pubblica VMware

Il file di installazione viene firmato digitalmente. Per verificare la firma, è necessario scaricare e installare la chiave pubblica VMware.

È possibile utilizzare lo strumento `rpm` di Linux e la chiave pubblica VMware per verificare la firma digitale del file di installazione di vCloud Director o qualsiasi altro file firmato scaricato da `vmware.com`. Se si installa la chiave pubblica nel computer in cui si intende installare vCloud Director, la verifica viene eseguita durante l'installazione o l'aggiornamento. È anche possibile verificare manualmente la firma prima di iniziare la procedura di installazione o di aggiornamento, quindi utilizzare il file verificato per tutte le installazioni o gli aggiornamenti.

---

**Nota** Nel sito di download viene anche pubblicato un valore di checksum per il download, disponibile in due formati comuni. La verifica del checksum consente di assicurarsi che il contenuto del file scaricato sia identico a quello del file pubblicato, ma non di verificare la firma digitale.

---

### Procedura

- 1 Creare una directory in cui archiviare le chiavi pubbliche del pacchetto VMware.
- 2 Utilizzare un browser Web per scaricare tutte le chiavi pubbliche del pacchetto VMware dalla directory <http://packages.vmware.com/tools/keys>.
- 3 Salvare i file di chiavi nella directory creata.
- 4 Per ogni chiave scaricata, eseguire il comando seguente per importarla.

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

*key\_path* è la directory in cui sono state salvate le chiavi.

*key\_name* è il nome file di una chiave.

## Installazione e configurazione di NSX Data Center for vSphere per vCloud Director

Se si pianifica l'installazione di vCloud Director per l'uso delle risorse di rete da NSX Data Center for vSphere, è necessario installare e configurare NSX Data Center for vSphere e associare un'istanza di NSX Manager univoca a ogni istanza di vCenter Server che si intende includere nell'installazione di vCloud Director.



NSX Manager è incluso nel download di NSX Data Center for vSphere. Per le informazioni più aggiornate sulla compatibilità tra vCloud Director e gli altri prodotti VMware, vedere le *Matrici di compatibilità dei prodotti VMware* all'indirizzo [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php). Per informazioni sui requisiti di rete, vedere [Requisiti di configurazione di rete per vCloud Director](#).

---

**Importante** Questa procedura è valida solo quando si effettua una nuova installazione di vCloud Director. Se si sta aggiornando un'installazione esistente di vCloud Director, vedere [Capitolo 11 Aggiornamento di vCloud Director e applicazione di patch all'appliance di vCloud Director](#).

---

### Prerequisiti

Verificare che ciascun sistema vCenter Server soddisfi i prerequisiti per l'installazione di NSX Manager.

### Procedura

- 1 Eseguire le attività di installazione per l'appliance virtuale di NSX Manager.  
*Vedere Guida all'installazione di NSX.*
- 2 Accedere all'appliance virtuale di NSX Manager installata e confermare le impostazioni specificate durante l'installazione.
- 3 Associare l'appliance virtuale di NSX Manager installata al sistema vCenter Server che si intende aggiungere a vCloud Director durante l'installazione pianificata di vCloud Director.
- 4 Configurare il supporto VXLAN nelle istanze di NSX Manager associate.  
  
vCloud Director crea pool di reti VXLAN per fornire risorse di rete ai VDC del provider. Se il supporto VXLAN non è configurato nel NSX Manager associato, i VDC del provider mostreranno un errore del pool di reti e sarà necessario creare un diverso tipo di pool di reti e associarlo al VDC del provider. Per informazioni dettagliate sulla configurazione del supporto VXLAN, vedere *Guida per l'amministratore di NSX*.
- 5 (Facoltativo) Se si desidera che i gateway edge nel sistema forniscano il routing distribuito, configurare un cluster di NSX Controller.  
  
*Vedere Guida per l'amministratore di NSX.*

## Installazione e configurazione di NSX-T Data Center per vCloud Director

Se si pianifica l'installazione di vCloud Director per l'uso delle risorse di rete da NSX-T Data Center, è necessario installare e configurare NSX-T Data Center con almeno un'istanza di NSX-T Manager.

NSX-T Manager è incluso nel download di NSX-T Data Center. Per le informazioni più aggiornate sulla compatibilità tra vCloud Director e gli altri prodotti VMware, vedere le *Matrici di compatibilità dei prodotti VMware* all'indirizzo [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php). Per informazioni sui requisiti di rete, vedere [Requisiti di configurazione di rete per vCloud Director](#).

---

**Importante** Questa procedura è valida solo quando si effettua una nuova installazione di vCloud Director. Se si sta aggiornando un'installazione esistente di vCloud Director, vedere [Capitolo 11 Aggiornamento di vCloud Director e applicazione di patch all'appliance di vCloud Director](#).

---

## Prerequisiti

È necessario avere familiarità con NSX-T Data Center.

## Procedura

- 1** Installare l'appliance virtuale NSX-T Manager.  
*Vedere Guida all'installazione di NSX-T.*
- 2** Preparare gli host ESXi che si desidera utilizzare con NSX-T Data Center.  
*Vedere Guida all'installazione di NSX-T.*
- 3** Creare i nodi di trasporto e le zone di trasporto in base ai requisiti del cloud.  
*Vedere Guida all'installazione di NSX-T.*
- 4** Configurare i cluster e i nodi edge.  
*Vedere Guida all'installazione di NSX-T.*
- 5** Configurare i router di livello 0 e 1.  
*Vedere Guida per l'amministratore di NSX-T.*
- 6** Configurare uno o più commutatori logici di sovrapposizione o VLAN che si desidera importare nell'installazione di vCloud Director.  
*Vedere Guida per l'amministratore di NSX-T.*

## Operazioni successive

Dopo avere installato vCloud Director, è possibile registrare l'istanza di NSX-T Manager nel cloud. Per informazioni sulla registrazione di un'istanza di NSX-T Manager, vedere *Guida alla programmazione dell'API di vCloud per i provider di servizi*.

# Creazione e gestione di certificati SSL per vCloud Director in Linux

# 4

vCloud Director utilizza SSL per proteggere le comunicazioni tra client e server. Ogni server vCloud Director deve supportare due endpoint SSL diversi, uno per le comunicazioni HTTPS e uno per quelle del proxy della console.

Gli endpoint possono essere costituiti da indirizzi IP separati o da un singolo indirizzo IP con due porte diverse. Ogni endpoint richiede il suo certificato SSL. È possibile utilizzare lo stesso certificato per entrambi gli endpoint, ad esempio utilizzando un certificato con caratteri jolly.

Questo capitolo include i seguenti argomenti:

- [Prima di creare certificati SSL per vCloud Director in Linux](#)
- [Creazione di certificati SSL autofirmati per vCloud Director in Linux](#)
- [Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione per vCloud Director in Linux](#)
- [Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione con chiavi private importate per vCloud Director in Linux](#)

## Prima di creare certificati SSL per vCloud Director in Linux

Quando si installa vCloud Director per Linux, è necessario creare due certificati per ogni membro del gruppo di server e importarli negli archivi chiavi dell'host.

---

**Nota** È necessario creare i certificati per i membri del gruppo di server solo dopo l'installazione di vCloud Director in Linux. L'appliance di vCloud Director crea certificati SSL autofirmati durante il primo avvio.

---

### Procedura

- 1 Accedere al server vCloud Director come **root**.
- 2 Visualizzare l'elenco degli indirizzi IP del server.

Per individuarli, utilizzare un comando come `ifconfig`.

- 3 Per ogni indirizzo IP, eseguire il comando seguente per recuperare il nome di dominio completo al quale è associato.

```
nslookup ip-address
```

- 4 Prendere nota di ogni indirizzo IP e del nome di dominio completo associato. Se non si utilizza un indirizzo IP singolo per entrambi i servizi, decidere quale indirizzo IP utilizzare per il servizio HTTPS e quale utilizzare per il servizio proxy della console.

Per la creazione dei certificati sono richiesti i nomi di dominio completi mentre quando si configurano le connessioni di rete e del database è necessario specificare gli indirizzi IP. Prendere nota di tutti gli altri eventuali nomi di dominio completi in grado di raggiungere l'indirizzo IP, perché è necessario specificarli se si desidera che il certificato includa un nome alternativo dell'oggetto.

#### Operazioni successive

Creare i certificati per i due endpoint. È possibile utilizzare certificati firmati da un'autorità di certificazione (CA) attendibile o certificati autofirmati.

---

**Nota** I certificati firmati da un'autorità di certificazione garantiscono il livello di attendibilità più elevato.

---

- Per informazioni sulla creazione e l'importazione di certificati SSL firmati da un'autorità di certificazione, vedere [Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione per vCloud Director in Linux](#).
- Per informazioni sulla creazione di certificati SSL autofirmati, vedere [Creazione di certificati SSL autofirmati per vCloud Director in Linux](#).
- Per informazioni sull'importazione di file di certificati con chiave privata e firmati da un'autorità di certificazione, vedere [Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione con chiavi private importate per vCloud Director in Linux](#).

## Creazione di certificati SSL autofirmati per vCloud Director in Linux

I certificati autofirmati possono semplificare la configurazione di SSL per vCloud Director negli ambienti in cui l'attendibilità rappresenta un problema solo marginale.

Ogni server vCloud Director richiede due certificati SSL in un file di archivio chiavi JCEKS, uno per il servizio HTTPS e uno per il servizio proxy della console.

È possibile utilizzare `cell-management-tool` per creare certificati SSL autofirmati. L'utilità `cell-management-tool` viene installata nella cella prima dell'esecuzione dell'agente di configurazione e dopo aver eseguito il file di installazione. Vedere [Installazione di vCloud Director nel primo membro di un gruppo di server](#).

**Importante** In questo esempio, sono specificate le dimensioni chiave a 2084 bit, ma è opportuno valutare i requisiti di sicurezza dell'installazione, prima di scegliere le dimensioni chiave corrette. Le dimensioni chiave inferiori a 1024 bit non sono più supportate, come riportato nella Pubblicazione speciale 800-131A del NIST.

#### Procedura

- 1 Accedere direttamente oppure mediante un client SSH al sistema operativo del server vCloud Director come **root**.
- 2 Eseguire il comando per creare una coppia di chiavi pubblica e privata per il servizio proxy HTTPS e della console.

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

Il comando crea o aggiorna un archivio chiavi in `certificates.ks` con password `passwd`. `cell-management-tool` crea i certificati utilizzando i valori predefiniti del comando. In base alla configurazione DNS dell'ambiente, il nome comune dell'autorità emittente è impostato sull'indirizzo IP o sul nome di dominio completo per ciascun servizio. Il certificato utilizza una lunghezza chiave a 2048 bit predefinita, che scade un anno dopo la sua creazione.

**Importante** Il file dell'archivio chiavi e la directory in cui è memorizzato devono essere leggibili dall'utente **vcloud.vcloud**. Il software di installazione vCloud Director crea questo utente e gruppo.

#### Operazioni successive

Prendere nota del nome del percorso dell'archivio chiavi. Quando si esegue lo script di configurazione per creare le connessioni di rete e del database per la cella di vCloud Director, è necessario il nome del percorso dell'archivio chiavi. Vedere [Configurazione delle connessioni di rete e database](#).

## Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione per vCloud Director in Linux

La creazione e l'importazione di certificati firmati dall'autorità di certificazione offre il livello di attendibilità più elevato per le comunicazioni SSL e consente di proteggere le connessioni nell'infrastruttura cloud.

Ogni server vCloud Director richiede due certificati SSL per proteggere le comunicazioni tra client e server. Ogni server vCloud Director deve supportare due endpoint SSL diversi, uno per le comunicazioni HTTPS e uno per quelle del proxy della console.

I due endpoint possono essere costituiti da indirizzi IP separati o da un singolo indirizzo IP con due porte diverse. Ogni endpoint richiede il suo certificato SSL. È possibile utilizzare lo stesso certificato per entrambi gli endpoint, ad esempio utilizzando un certificato con caratteri jolly.

I certificati per entrambi gli endpoint devono includere sia un'estensione di nome distinto X.500 sia un'estensione di nome alternativo dell'oggetto X.509.

È possibile utilizzare certificati firmati da un'autorità di certificazione (CA) attendibile o certificati autofirmati.

È possibile utilizzare `cell-management-tool` per creare certificati SSL autofirmati. L'utilità `cell-management-tool` viene installata nella cella prima dell'esecuzione dell'agente di configurazione e dopo aver eseguito il file di installazione. Vedere [Installazione di vCloud Director nel primo membro di un gruppo di server](#).

Se si dispone già di chiavi private e di file di certificati firmati dall'autorità di certificazione, seguire la procedura descritta in [Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione con chiavi private importate per vCloud Director in Linux](#).

---

**Importante** In questo esempio, sono specificate le dimensioni chiave a 2084 bit, ma è opportuno valutare i requisiti di sicurezza dell'installazione, prima di scegliere le dimensioni chiave corrette. Le dimensioni chiave inferiori a 1024 bit non sono più supportate, come riportato nella Pubblicazione speciale 800-131A del NIST.

---

#### Prerequisiti

- Assicurarsi di poter accedere a un computer con un ambiente di runtime Java versione 8 o successiva, in modo da poter utilizzare il comando `keytool` per importare i certificati. Il programma di installazione di vCloud Director inserisce una copia di `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`, ma è possibile eseguire questa procedura su qualsiasi computer con un ambiente di runtime Java installato. L'utilizzo di certificati creati con un `keytool` proveniente da qualsiasi altra origine non è supportato con vCloud Director. Nelle righe di comando di esempio riportate di seguito si suppone che `keytool` si trovi nel percorso dell'utente.
- Familiarizzare con il comando `keytool`.
- Per ulteriori dettagli sulle opzioni disponibili per il comando `generate-certs`, vedere [Generazione di certificati autofirmati per gli endpoint proxy della console e HTTPS](#).
- Per ulteriori dettagli sulle opzioni disponibili per il comando `certificates`, vedere [Sostituzione di certificati per gli endpoint proxy della console e HTTP](#).

#### Procedura

- 1 Accedere direttamente o tramite un client SSH al sistema operativo della cella del server vCloud Director come **root**.

- 2 Eseguire il comando per creare una coppia di chiavi pubblica e privata per il servizio proxy HTTPS e della console.

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

Il comando crea o aggiorna un archivio chiavi in `certificates.ks` con la password specificata. I certificati vengono creati utilizzando i valori predefiniti del comando. In base alla configurazione DNS dell'ambiente, il nome comune dell'autorità emittente è impostato sull'indirizzo IP o sul nome di dominio completo per ciascun servizio. Il certificato utilizza una lunghezza chiave a 2048 bit predefinita, che scade un anno dopo la sua creazione.

---

**Importante** Il file dell'archivio chiavi e la directory in cui è memorizzato devono essere leggibili dall'utente **vcloud.vcloud**. Il software di installazione vCloud Director crea questo utente e gruppo.

---

- 3 Creare una richiesta di firma del certificato per il servizio HTTPS e per il servizio proxy della console.

---

**Importante** Se si utilizzano indirizzi IP separati per il servizio HTTPS e per il servizio proxy della console, modificare i nomi host e gli indirizzi IP nei comandi seguenti.

---

- a Creare una richiesta di firma del certificato nel file `http.csr`.

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

- b Creare una richiesta di firma del certificato nel file `consoleproxy.csr`.

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

- 4 Inviare le richieste di firma del certificato all'autorità di certificazione.

Se l'autorità di certificazione richiede di specificare un tipo di Web server, usare Jakarta Tomcat.

Procurarsi i certificati firmati dall'autorità di certificazione.

**5** Importare i certificati firmati nell'archivio chiavi JCEKS.

- a Importare il certificato root dell'autorità di certificazione dal file `root.cer` nel file di archivio chiavi `certificates.ks`.

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

- b Se si ricevono certificati intermedi, importarli dal file `intermediate.cer` nel file di archivio chiavi `certificates.ks`.

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

- c Importare il certificato del servizio HTTPS.

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

- d Importare il certificato del servizio proxy della console.

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

I comandi sovrascrivono il file `certificates.ks` con le versioni dei certificati firmate dall'autorità di certificazione appena acquisite.

- 6** Per verificare se i certificati sono stati importati nell'archivio chiavi JCEKS, eseguire il comando per elencare il contenuto del file dell'archivio chiavi.

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

- 7** Ripetere questa procedura su tutti i server vCloud Director nel gruppo di server.

**Operazioni successive**

- Se l'istanza di vCloud Director non è ancora stata configurata, eseguire lo script `configure` per importare l'archivio chiavi dei certificati in vCloud Director. Vedere [Configurazione delle connessioni di rete e database](#).

---

**Nota** Se il file di archivio chiavi `certificates.ks` è stato creato su un computer diverso dal server sul quale è stato generato l'elenco di nomi di dominio completi con i relativi indirizzi IP associati, copiare il file di archivio chiavi in tale server. Durante l'esecuzione dello script di configurazione, è necessario specificare il nome del percorso del file di archivio chiavi.

---

- Se l'istanza di vCloud Director è già stata installata e configurata, utilizzare il comando `certificates` dello strumento di gestione delle celle per importare l'archivio chiavi dei certificati. Vedere [Sostituzione di certificati per gli endpoint proxy della console e HTTP](#).



## Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione con chiavi private importate per vCloud Director in Linux

Se si dispone del file delle chiavi private e del file del certificato firmato dall'autorità di certificazione, prima di importare gli archivi chiavi nell'ambiente vCloud Director, è necessario creare file di archivio chiavi in cui importare i certificati e le chiavi private sia per il servizio HTTPS sia per il servizio proxy della console.

### Prerequisiti

- Vedere [Prima di creare certificati SSL per vCloud Director in Linux](#).
- Assicurarsi di poter accedere a un computer con un ambiente di runtime Java versione 8 o successiva, in modo da poter utilizzare il comando `keytool` per importare i certificati. Il programma di installazione di vCloud Director inserisce una copia di `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`, ma è possibile eseguire questa procedura su qualsiasi computer con un ambiente di runtime Java installato. L'utilizzo di certificati creati con un `keytool` proveniente da qualsiasi altra origine non è supportato con vCloud Director. Nelle righe di comando di esempio riportate di seguito si suppone che `keytool` si trovi nel percorso dell'utente.
- Familiarizzare con il comando `keytool`.
- Scaricare e installare OpenSSL.
- Per ulteriori dettagli sulle opzioni disponibili per il comando `certificates`, vedere [Sostituzione di certificati per gli endpoint proxy della console e HTTP](#).

### Procedura

- 1 Se si dispone di certificati intermedi, eseguire il comando per combinare il certificato root firmato dall'autorità di certificazione con i certificati intermedi e creare una catena di certificati.

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

- 2 Utilizzare OpenSSL per creare i file dell'archivio chiavi PKCS12 intermedi per il servizio HTTPS e per il servizio proxy della console con la chiave privata, la catena di certificati e il rispettivo alias, quindi specificare una password per ciascun file di archivio chiavi.

- a Creare il file dell'archivio chiavi per il servizio HTTPS.

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

- b Creare il file dell'archivio dati per il servizio proxy della console.

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

- 3 Utilizzare keytool per importare gli archivi chiave PKCS12 nell'archivio chiavi JCEKS.

- a Eseguire il comando per importare l'archivio chiavi PKCS12 per il servizio HTTPS.

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

- b Eseguire il comando per importare l'archivio chiavi PKCS12 per il servizio proxy della console.

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

- 4 Per verificare se i certificati sono stati importati nell'archivio chiavi JCEKS, eseguire il comando per elencare il contenuto del file dell'archivio chiavi.

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

- 5 Ripetere la procedura per tutte le celle vCloud Director nell'ambiente.

#### Operazioni successive

- Se l'istanza di vCloud Director non è ancora stata configurata, eseguire lo script configure per importare l'archivio chiavi dei certificati in vCloud Director. Vedere [Configurazione delle connessioni di rete e database](#).

---

**Nota** Se il file dell'archivio chiavi certificates.ks è stato creato in un computer diverso dal server in cui è stato generato l'elenco di nomi di dominio completi e di indirizzi IP associati, copiare il file dell'archivio chiavi in tale server. Durante l'esecuzione dello script di configurazione, è necessario specificare il nome del percorso del file di archivio chiavi.

---

- Se l'istanza di vCloud Director è già stata installata e configurata, utilizzare il comando certificates dello strumento di gestione delle celle per importare l'archivio chiavi dei certificati. Vedere [Sostituzione di certificati per gli endpoint proxy della console e HTTP](#).

# Installazione di vCloud Director in Linux

# 5

È possibile creare un gruppo di server vCloud Director installando il software vCloud Director di uno o più server Linux. L'installazione e la configurazione del primo membro del gruppo crea un file di risposta da utilizzare per configurare membri aggiuntivi del gruppo.

Questa procedura è valida solo per le nuove installazioni. Se si sta aggiornando un'installazione di vCloud Director esistente, consultare [Capitolo 11 Aggiornamento di vCloud Director e applicazione di patch all'appliance di vCloud Director](#).

---

**Importante** Le installazioni vCloud Director miste su Linux e le distribuzioni di appliance vCloud Director in un gruppo di server non sono supportate.

---

## Prerequisiti

- Verificare che i server di destinazione per il gruppo di server soddisfino i [Capitolo 2 Requisiti hardware e software di vCloud Director](#).
- Assicurarsi di avere creato un certificato SSL per ogni endpoint dei server di destinazione per il gruppo di server. Tutte le directory incluse nel nome di percorso dei certificati SSL devono essere leggibili da qualsiasi utente. L'uso dello stesso percorso di archivio chiavi in tutti i membri di un gruppo di server semplifica il processo di installazione. Esempio di percorso: /tmp/certificates.ks. Vedere [Prima di creare certificati SSL per vCloud Director in Linux](#).
- Assicurarsi di avere preparato un NFS o un altro volume di storage condiviso accessibile per tutti i server di destinazione del gruppo di server vCloud Director. Vedere [Preparazione dello storage del server di trasferimento](#).
- Assicurarsi di avere creato un database vCloud Director accessibile per tutti i server del gruppo. Vedere [Preparazione del database di vCloud Director](#). Assicurarsi che il servizio di database venga avviato al riavvio del server di database.
- Verificare che tutti i server vCloud Director, il server di database, tutti i sistemi vCenter Server e le istanze di NSX Manager associate siano in grado di risolvere ogni nome host nell'ambiente, come descritto in [Requisiti di configurazione di rete per vCloud Director](#).
- Verificare che tutti i server vCloud Director e il server di database siano sincronizzati con un server di riferimento orario di rete, con le tolleranze descritte in [Requisiti di configurazione di rete per vCloud Director](#).

- Se si intende importare utenti o gruppi da un servizio LDAP, verificare che il servizio sia accessibile da ogni server vCloud Director.
- Aprire le porte firewall come descritto in [Requisiti di sicurezza della rete](#). La porta 443 deve essere aperta tra vCloud Director e i sistemi vCenter Server.

## Procedura

### 1 Installazione di vCloud Director nel primo membro di un gruppo di server

Dopo aver preparato l'ambiente e verificato i prerequisiti, è possibile iniziare a creare il gruppo di server vCloud Director eseguendo il programma di installazione di vCloud Director nel primo server Linux di destinazione.

### 2 Configurazione delle connessioni di rete e database

Dopo avere installato vCloud Director nel primo membro del gruppo di server, è necessario eseguire lo script di configurazione che crea le connessioni di rete e database per questa cella. Lo script crea un file di risposta da utilizzare durante la configurazione di altri membri del gruppo di server.

### 3 Installazione di vCloud Director in un membro aggiuntivo di un gruppo di server

È possibile aggiungere server a un gruppo di server vCloud Director in qualsiasi momento. Poiché tutti i server in un gruppo di server devono essere configurati con gli stessi dettagli di connessione del database, è necessario utilizzare il file di risposta creato quando è stato configurato il primo membro del gruppo.

### 4 Impostazione di vCloud Director

Dopo aver installato e configurato tutti i server nel gruppo di server vCloud Director, è necessario impostare l'installazione di vCloud Director. L'impostazione di vCloud Director inizializza il database di vCloud Director con una chiave di licenza, l'account dell'amministratore di sistema e le informazioni correlate.

## Operazioni successive

È possibile iniziare ad aggiungere risorse all'installazione di vCloud Director. Per iniziare a utilizzare vCloud Director, consultare *Guida per gli amministratori di vCloud Director*.

## Installazione di vCloud Director nel primo membro di un gruppo di server

Dopo aver preparato l'ambiente e verificato i prerequisiti, è possibile iniziare a creare il gruppo di server vCloud Director eseguendo il programma di installazione di vCloud Director nel primo server Linux di destinazione.

vCloud Director for Linux è distribuito come file eseguibile firmato digitalmente con formato del nome `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, dove *v.v.v* rappresenta la versione di prodotto e *nnnnnn* il numero di build. Ad esempio: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Questo eseguibile consente di installare o aggiornare vCloud Director.

Il programma di installazione di vCloud Director verifica che il server di destinazione soddisfi tutti i requisiti preliminari di piattaforma e vi installa il software vCloud Director.

### Prerequisiti

- Assicurarsi di disporre delle credenziali di utente con privilegi avanzati per il server di destinazione
- Se si desidera che il programma di installazione verifichi la firma digitale del file di installazione, scaricare e installare la chiave pubblica VMware nel server di destinazione. Se la firma digitale del file di installazione è stata già verificata, non è necessario verificarla di nuovo durante l'installazione. Vedere [Download e installazione della chiave pubblica VMware](#).

### Procedura

- 1 Eseguire il login al server di destinazione come utente **root**.

- 2 Scaricare il file di installazione nel server di destinazione.

Se il software è stato acquistato su supporto multimediale, copiare il file di installazione in una posizione accessibile dal server di destinazione.

- 3 Verificare che il checksum del download corrisponda a quello pubblicato nella pagina di download.

I valori per entrambi i checksum MD5 e SHA1 vengono pubblicati nella pagina di download. Utilizzare lo strumento appropriato per verificare che il checksum del file di installazione scaricato corrisponda a quello visualizzato nella pagina di download. Un comando Linux nel seguente formato visualizza il checksum per *file-installazione*.

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

Il comando restituisce il checksum del file di installazione che deve corrispondere al checksum MD5 della pagina di download.

- 4 Verificare che il file di installazione sia eseguibile.

Tale file richiede l'autorizzazione per l'esecuzione. Per verificare se tale autorizzazione è disponibile, aprire una console, una shell o una finestra del terminale ed eseguire il comando Linux riportato di seguito, dove *file-di-installazione* è il percorso completo del file di installazione di vCloud Director.

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

- 5 Eseguire il file di installazione.

Per eseguire il file di installazione, immetterne il percorso completo, ad esempio:

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

Il file include uno script di installazione e un pacchetto RPM incorporato.

---

**Nota** Non è possibile eseguire il file di installazione da una directory il cui percorso includa caratteri spazio incorporati.

---

Se la chiave pubblica di VMware non è installata nel server di destinazione, il programma di installazione stampa un avviso nel formato seguente:

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

Il programma di installazione esegue le seguenti azioni.

- a Verifica che l'host soddisfi tutti i requisiti.
- b Verifica la firma digitale nel file di installazione.
- c Crea l'utente e il gruppo vcloud.
- d Apre il pacchetto RPM di vCloud Director.
- e Installa il software.

Al termine dell'installazione, il programma di installazione richiede di eseguire lo script di configurazione, che configura le connessioni di database e rete.

- 6 Scegliere se eseguire lo script di configurazione.
  - a Per eseguire lo script di configurazione in modalità interattiva, immettere **y** e premere INVIO.
  - b Per eseguire lo script di configurazione in un secondo momento in modalità interattiva o automatica, immettere **n** e premere INVIO.

## Configurazione delle connessioni di rete e database

Dopo avere installato vCloud Director nel primo membro del gruppo di server, è necessario eseguire lo script di configurazione che crea le connessioni di rete e database per questa cella. Lo script crea un file di risposta da utilizzare durante la configurazione di altri membri del gruppo di server.

Tutti i membri del gruppo di server vCloud Director condividono la connessione al database e altri dettagli di configurazione. Quando si esegue lo script di configurazione nel primo membro del gruppo di server vCloud Director, lo script crea un file di risposta in cui vengono conservate le informazioni delle connessioni del database da utilizzare nelle installazioni del server successive.

È possibile eseguire lo script di configurazione in modalità interattiva o automatica. In caso di configurazione interattiva, eseguire il comando senza opzioni e lo script richiede le informazioni necessarie per l'installazione. In caso di configurazione automatica, le informazioni di configurazione vengono immesse utilizzando le opzioni di comando.

Se si desidera utilizzare un solo indirizzo IP con due porte diverse per il servizio HTTP e il servizio proxy della console, è necessario eseguire lo script di configurazione in modalità automatica.

---

**Nota** Lo strumento di gestione delle celle include sottocomandi utilizzabili per modificare i dati relativi alle connessioni di rete e database inizialmente configurati. Le modifiche apportate utilizzando questi sottocomandi sono scritte nel file di configurazione globale e nel file di risposta. Per informazioni sull'uso dello strumento di gestione delle celle, vedere la *Guida per gli amministratori di vCloud Director*.

---

### Prerequisiti

- Per una configurazione interattiva, fare riferimento a [Riferimento alla configurazione interattiva](#).
- Per una configurazione automatica, fare riferimento a [Riferimenti per la configurazione automatica](#).
- Per una configurazione automatica, verificare che il valore della variabile di ambiente VCLLOUD\_HOME sia impostato sul percorso completo della directory in cui è installato vCloud Director. Questo valore è generalmente /opt/vmware/vcloud-director.

### Procedura

- 1 Accedere al server vCloud Director come root.
- 2 Eseguire il comando configure:
  - Per la modalità interattiva, eseguire il comando e seguire le istruzioni fornendo le informazioni richieste.

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

- Per la modalità automatica, eseguire il comando con gli argomenti e le opzioni appropriate.

```
/opt/vmware/vcloud-director/bin/configureoptions -unattended
```

Lo script convalida le informazioni, quindi:

- a Inizializza il database e lo connette al server.
  - b Visualizza un URL che consente di connettersi alla procedura guidata **Configurazione di VMware vCloud Director** dopo l'avvio del servizio vCloud Director.
  - c Offre la possibilità di avviare la cella vCloud Director.
- 3 (Facoltativo) Prendere nota dell'URL della procedura guidata **Configurazione di VMware vCloud Director** e immettere **y** per avviare il servizio vCloud Director.

È possibile decidere di avviare il servizio in seguito eseguendo il comando `service vmware-vcd start`.

## Risultati

Le informazioni sulle connessioni del database e le altre informazioni riutilizzabili fornite durante la configurazione vengono conservate in un file di risposta nel percorso `/opt/vmware/vcloud-director/etc/responses.properties` in questo server. In tale file sono contenute informazioni riservate da riutilizzare per l'aggiunta di server a un gruppo di server.

## Operazioni successive

Salvare una copia del file di risposta in una posizione sicura. Limitare l'accesso a tale file e assicurarsi che ne venga eseguito il backup in una posizione sicura. Quando si esegue il backup del file, evitare l'invio di testo non crittografato attraverso una rete pubblica.

Per aggiungere server al gruppo di server, montare lo storage di trasferimento condiviso nel percorso `/opt/vmware/vcloud-director/data/transfer`.

## Riferimento alla configurazione interattiva

Quando si esegue lo script `configure` in modalità interattiva, lo script richiede le informazioni seguenti.

Premere INVIO per accettare un valore predefinito.

**Tabella 5-1. Informazioni richieste durante la configurazione interattiva della rete e del database**

Informazioni richieste	Descrizione
Indirizzo IP per il servizio HTTP	Per impostazione predefinita, viene utilizzato il primo indirizzo IP disponibile.
Indirizzo IP del servizio proxy della console	Per impostazione predefinita, viene utilizzato il primo indirizzo IP disponibile.  <b>Nota</b> Se si desidera utilizzare un solo indirizzo IP con due porte diverse per il servizio HTTP e il servizio proxy della console, è necessario eseguire lo script di configurazione in modalità automatica.
Percorso completo del file di archivio chiavi Java	Ad esempio, <code>/opt/keystore/certificates.ks</code> .
Password dell'archivio chiavi	Vedere <a href="#">Prima di creare certificati SSL per vCloud Director in Linux</a> .
Password della chiave privata per il certificato SSL HTTP	Vedere <a href="#">Prima di creare certificati SSL per vCloud Director in Linux</a> .
Password della chiave privata per il certificato SSL proxy della console	Vedere <a href="#">Prima di creare certificati SSL per vCloud Director in Linux</a> .



**Tabella 5-1. Informazioni richieste durante la configurazione interattiva della rete e del database (continua)**

Informazioni richieste	Descrizione
Abilitare la registrazione di controllo remoto in un host syslog	<p>I servizi di ogni cella vCloud Director registrano i messaggi di controllo nel database vCloud Director, in cui vengono conservati per 90 giorni. Per conservarli per un periodo di tempo maggiore, è possibile configurare i servizi di vCloud Director per l'invio di messaggi di controllo all'utilità syslog, oltre che al database di vCloud Director.</p> <ul style="list-style-type: none"> <li>■ Per ignorare, premere INVIO.</li> <li>■ Per abilitare, immettere l'indirizzo IP o il nome host di syslog.</li> </ul>
Se è abilitata la registrazione di controllo remoto, porta UDP dell'host syslog	L'impostazione predefinita è 514.
Tipo di database	<p>PostgreSQL o Microsoft SQL Server.</p> <p>L'impostazione predefinita è PostgreSQL.</p>
Nome host o indirizzo IP del server di database	Server che esegue il database.
Porta del database	<p>Per PostgreSQL, l'impostazione predefinita è 5432.</p> <p>Per Microsoft SQL Server, l'impostazione predefinita è 1433.</p>
Nome database	L'impostazione predefinita è vcloud.
Se il tipo di database è Microsoft SQL Server, istanza del database	L'impostazione predefinita è l'istanza predefinita.
Nome utente del database	Vedere <a href="#">Preparazione del database di vCloud Director</a> .
Password database	Vedere <a href="#">Preparazione del database di vCloud Director</a> .
Partecipare o meno all'Analisi utilizzo software (CEIP) di VMware	<p>Questo prodotto partecipa al programma CEIP (Customer Experience Improvement Program) di VMware. I dettagli sui dati raccolti tramite il programma CEIP e le finalità per le quali vengono utilizzati da VMware sono riportati nel centro di affidabilità e controllo all'indirizzo <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a>. È possibile utilizzare lo strumento di gestione delle celle per attivare o disattivare la partecipazione al programma CEIP VMware per questo prodotto in qualsiasi momento. Vedere "Guida di riferimento allo strumento di gestione delle celle" nella <i>Guida per gli amministratori di vCloud Director</i>.</p> <p>Per partecipare al programma, immettere <b>y</b>.</p> <p>Se non si desidera partecipare al programma CEIP di VMware, immettere <b>n</b>.</p>

## Riferimenti per la configurazione automatica

Quando si esegue lo script `configure` in modalità automatica, è necessario immettere le informazioni di configurazione nella riga di comando come opzioni e argomenti.

**Tabella 5-2. Argomenti e opzioni dell'utilità di configurazione**

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Visualizza un riepilogo degli argomenti e delle opzioni di configurazione
<code>--config-file (-c)</code>	Percorso del file <code>global.properties</code>	Le informazioni fornite durante l'esecuzione dell'utilità di configurazione vengono salvate in questo file. Se si omette questa opzione, il percorso predefinito è <code>/opt/vmware/vcloud-director/etc/global.properties</code> .
<code>--console-proxy-ip (-cons)</code>	Indirizzo IPv4 con un numero di porta facoltativo	Il sistema utilizza questo indirizzo per il servizio proxy della console di vCloud Director. Ad esempio, <code>10.17.118.159</code> .
<code>--console-proxy-port-https</code>	Numero intero compreso nell'intervallo 0-65535	Numero della porta da utilizzare per il servizio proxy della console di vCloud Director.
<code>--database-ssl</code>	<code>true</code> o <code>false</code>	Se si utilizza un database PostgreSQL, è possibile configurarlo in modo che richieda a vCloud Director una connessione SSL "well-signed" (con catena di certificazione che garantisce la massima sicurezza). Questa opzione viene ignorata se <code>--database-type</code> non è <code>postgres</code> . Se si desidera configurare il database PostgreSQL per utilizzare un certificato autofirmato o privato, vedere <a href="#">Esecuzione di configurazioni aggiuntive nel database PostgreSQL esterno</a> .
<code>--database-host (-dbhost)</code>	Indirizzo IP o nome di dominio completo dell'host database di vCloud Director	Vedere <a href="#">Preparazione del database di vCloud Director</a> .
<code>--database-domain (-dbdomain)</code>	Dominio dell'utente di database SQL Server	Opzione facoltativa se <code>--database-type</code> è <code>sqlserver</code> .
<code>--database-instance (-dbinstance)</code>	Istanza del database SQL Server	Opzione utilizzata se <code>--database-type</code> è <code>sqlserver</code> .

Tabella 5-2. Argomenti e opzioni dell'utilità di configurazione (continua)

Opzione	Argomento	Descrizione
--database-name (-dbname)	Il nome del servizio di database	Vedere <a href="#">Preparazione del database di vCloud Director</a> .
--database-password (-dbpassword)	Password per l'utente del database. Può essere nulla.	Vedere <a href="#">Preparazione del database di vCloud Director</a> .
--database-port (-dbport)	Numero di porta utilizzato dal servizio di database sull'host database	Vedere <a href="#">Preparazione del database di vCloud Director</a> .
--database-type (-dbtype)	Il tipo di database. Può essere: <ul style="list-style-type: none"> <li>■ postgres</li> <li>■ sqlserver</li> </ul>	Vedere <a href="#">Preparazione del database di vCloud Director</a> .
--database-user (-dbuser)	Il nome utente dell'utente del database.	Vedere <a href="#">Preparazione del database di vCloud Director</a> .
--enable-ceip	true o false	Questo prodotto partecipa al programma CEIP (Customer Experience Improvement Program) di VMware. I dettagli sui dati raccolti tramite il programma CEIP e le finalità per le quali vengono utilizzati da VMware sono riportati nel centro di affidabilità e controllo all'indirizzo <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> . È possibile utilizzare lo strumento di gestione delle celle per attivare o disattivare la partecipazione al programma CEIP VMware per questo prodotto in qualsiasi momento. Vedere "Guida di riferimento allo strumento di gestione delle celle" nella <i>Guida per gli amministratori di vCloud Director</i> .
--uuid (-g)	Nessuno	Genera un nuovo identificatore univoco per la cella
--primary-ip (-ip)	Indirizzo IPv4 con un numero di porta facoltativo	Il sistema utilizza questo indirizzo per il servizio dell'interfaccia Web di vCloud Director. Ad esempio, <i>10.17.118.159</i> .
--primary-port-http	Numero intero compreso nell'intervallo da 0 a 65535	Numero della porta da utilizzare per le connessioni HTTP (non protette) al servizio interfaccia Web di vCloud Director

Tabella 5-2. Argomenti e opzioni dell'utilità di configurazione (continua)

Opzione	Argomento	Descrizione
--primary-port-https	Numero intero compreso nell'intervallo 0-65535	Numero della porta da utilizzare per le connessioni HTTPS (protette) al servizio interfaccia Web di vCloud Director
--keystore (-k)	Percorso dell'archivio chiavi Java contenente i certificati SSL e le chiavi private	Il nome del percorso deve essere completo. Ad esempio, /opt/keystore/certificates.ks .
--syslog-host (-loghost)	Indirizzo IP o nome di dominio completo dell'host del server syslog	I servizi di ogni cella vCloud Director registrano i messaggi di controllo nel database vCloud Director, in cui vengono conservati per 90 giorni. Per conservarli per un periodo di tempo maggiore, è possibile configurare i servizi di vCloud Director per l'invio di messaggi di controllo all'utilità syslog, oltre che al database di vCloud Director.
--syslog-port (-logport)	Numero intero compreso nell'intervallo 0-65535	La porta sulla quale il processo syslog monitora il server specificato. Se non diversamente specificato, il valore predefinito è 514.
--response-file (-r)	Percorso del file di risposta	Il nome del percorso deve essere completo. Se non diversamente specificato, il valore predefinito è /opt/vmware/vcloud-director/etc/responses.properties. Tutte le informazioni fornite quando si esegue la configurazione vengono salvate in questo file.  <b>Importante</b> In tale file sono contenute informazioni riservate da riutilizzare per l'aggiunta di server a un gruppo di server. Conservare il file in un luogo sicuro in modo che sia disponibile all'occorrenza.
--unattended-installation (-unattended)	Nessuno	Specifica l'installazione automatica
--keystore-password (-w)	Password dell'archivio chiavi del certificato SSL	Password dell'archivio chiavi del certificato SSL.

## Esempio: Configurazione automatica con due indirizzi IP

Il seguente comando di esempio consente di eseguire una configurazione automatica di un server vCloud Director con due indirizzi IP diversi per il servizio HTTP e il servizio proxy della console.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 -cons 10.17.118.158 \
-dbtype sqlserver -dbhost 10.150.10.78 -dbname mssql-db -dbuser vcloud --enable-ceip true \
-dbpassword P055word -k /opt/keystore/certificates.ks -w $3Cret -loghost 10.150.10.10 -unattended
```

## Esempio: Configurazione automatica con un solo indirizzo IP

Il seguente comando di esempio consente di eseguire una configurazione automatica di un server vCloud Director con un solo indirizzo IP e due porte diverse per il servizio HTTP e il servizio proxy della console.

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./configure -ip 10.17.118.159 --primary-port-https 9000 -cons 10.17.118.159 \
--console-proxy-port-https 9010 -dbtype sqlserver -dbhost 10.150.10.78 -dbname mssql-db \
-dbuser vcloud -dbpassword P055word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

## Protezione e riutilizzo del file di risposta

I dettagli relativi alle connessioni di rete e database configurati nella prima cella di vCloud Director vengono salvati in un file di risposta. In tale file sono contenute informazioni riservate da riutilizzare per l'aggiunta di server al gruppo di server. È necessario conservare il file in una posizione sicura.

Il file di risposta viene creato nel percorso `/opt/vmware/vcloud-director/etc/responses.properties` sul primo server per il quale si configurano connessioni di rete e database. Quando si aggiungono server al gruppo, è necessario utilizzare una copia del file di risposta per specificare i parametri di configurazione condivisi tra tutti i server.

**Importante** Lo strumento di gestione delle celle include sottocomandi utilizzabili per modificare i dati relativi alle connessioni di rete e database inizialmente specificati. Poiché le modifiche apportate mediante questi strumenti vengono scritte nel file di configurazione globale e nel file di risposta, prima di utilizzare qualsiasi comando di modifica è necessario accertarsi che il file di risposta sia nella posizione corretta (in `/opt/vmware/vcloud-director/etc/responses.properties`) e che sia scrivibile.

### Procedura

#### 1 Proteggere il file di risposta.

Salvare una copia del file in una posizione sicura. Limitare l'accesso a tale file e assicurarsi che ne venga eseguito il backup in una posizione sicura. Quando si esegue il backup del file, evitare l'invio di testo non crittografato attraverso una rete pubblica.

## 2 Riutilizzare il file di risposta.

- a Copiare il file in una posizione accessibile dal server che verrà configurato.

**Nota** Occorre installare il software vCloud Director in un server prima di riutilizzare il file di risposta per configurarlo. Tutte le directory incluse nel nome di percorso del file di risposta devono essere leggibili dall'utente `vcloud.vcloud`, come mostrato in questo esempio.

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

Il software di installazione crea questo utente e il gruppo.

- b Eseguire lo script di configurazione, utilizzando l'opzione `-r` e specificando il percorso del file di risposta.

Accedere come root, aprire una console, una shell o una finestra del terminale e digitare:

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

### Operazioni successive

Dopo aver configurato gli altri server, eliminare la copia del file di risposta utilizzato per configurarli.

## Installazione di vCloud Director in un membro aggiuntivo di un gruppo di server

È possibile aggiungere server a un gruppo di server vCloud Director in qualsiasi momento. Poiché tutti i server in un gruppo di server devono essere configurati con gli stessi dettagli di connessione del database, è necessario utilizzare il file di risposta creato quando è stato configurato il primo membro del gruppo.

**Importante** Le installazioni vCloud Director miste su Linux e le distribuzioni di appliance vCloud Director in un gruppo di server non sono supportate.

### Prerequisiti

- Verificare che sia possibile accedere al file di risposta creato quando è stato configurato il primo membro di questo gruppo di server. Vedere [Configurazione delle connessioni di rete e database](#).
- Verificare che lo storage di trasferimento condiviso sia montato nel primo membro del gruppo di server vCloud Director in `/opt/vmware/vcloud-director/data/transfer`.

### Procedura

- 1 Eseguire il login al server di destinazione come utente **root**.

**2** Scaricare il file di installazione nel server di destinazione.

Se il software è stato acquistato su supporto multimediale, copiare il file di installazione in una posizione accessibile dal server di destinazione.

**3** Verificare che il file di installazione sia eseguibile.

Tale file richiede l'autorizzazione per l'esecuzione. Per verificare se tale autorizzazione è disponibile, aprire una console, una shell o una finestra del terminale ed eseguire il comando Linux riportato di seguito, dove *file-di-installazione* è il percorso completo del file di installazione di vCloud Director.

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

**4** Eseguire il file di installazione.

Per eseguire il file di installazione, immetterne il percorso completo, ad esempio:

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

Il file include uno script di installazione e un pacchetto RPM incorporato.

---

**Nota** Non è possibile eseguire il file di installazione da una directory il cui percorso includa caratteri spazio incorporati.

---

Se la chiave pubblica di VMware non è installata nel server di destinazione, il programma di installazione stampa un avviso nel formato seguente:

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

Il programma di installazione esegue le seguenti azioni.

- a Verifica che l'host soddisfi tutti i requisiti.
- b Verifica la firma digitale nel file di installazione.
- c Crea l'utente e il gruppo vcloud.
- d Apre il pacchetto RPM di vCloud Director.
- e Installa il software.

Al termine dell'installazione, il programma di installazione richiede di eseguire lo script di configurazione, che configura le connessioni di database e rete.

**5** Immettere **n** e premere INVIO per rifiutare l'esecuzione dello script di configurazione.

È possibile eseguire lo script di configurazione in un secondo momento fornendo il file di risposta come input.

**6** Montare lo storage di trasferimento condiviso in `/opt/vmware/vcloud-director/data/transfer`.

Tutti i server vCloud Director nel gruppo di server devono montare questo volume nello stesso punto.

- 7 Copiare il file di risposta in una posizione accessibile a questo server.

Tutte le directory incluse nel nome di percorso al file di risposta devono essere leggibili da qualsiasi root.

- 8 Eseguire lo script di configurazione.

- a Eseguire il comando `configure` fornendo il percorso del file di risposta.

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

Lo script copia il file di risposta in una posizione leggibile da `vcloud.vcloud` ed esegue lo script di configurazione utilizzando il file di risposta come input.

- b Quando vengono richiesti, fornire gli indirizzi IP per il protocollo HTTP e i servizi proxy della console.
- c Se lo script di configurazione non trova certificati validi nel percorso salvato nel file di risposta, fornire, quando richiesto, il percorso per i certificati e le password.

Lo script convalida le informazioni, connette il server al database e offre la possibilità di avviare la cella di vCloud Director.

- 9 (Facoltativo) Immettere **y** per avviare il servizio vCloud Director.

È possibile decidere di avviare il servizio in seguito eseguendo il comando `service vmware-vcd start`.

#### Operazioni successive

Ripetere la procedura per aggiungere più server al gruppo di server.

Una volta che i servizi di vCloud Director sono in esecuzione in tutti i server, è necessario inizializzare il database vCloud Director con un codice di licenza, un account di amministratore di sistema e le informazioni correlate. È possibile inizializzare il database in uno dei modi seguenti:

- Utilizzare un browser Web per aprire l'installazione guidata mediante l'URL visualizzato al termine dello script di configurazione. Vedere [Impostazione di vCloud Director](#).
- Utilizzare lo strumento di gestione delle celle con il sottocomando `system-setup`. Per informazioni sull'utilizzo dello strumento di gestione delle celle, vedere *Guida per gli amministratori di vCloud Director*.

## Impostazione di vCloud Director

Dopo aver installato e configurato tutti i server nel gruppo di server vCloud Director, è necessario impostare l'installazione di vCloud Director. L'impostazione di vCloud Director inizializza il database di vCloud Director con una chiave di licenza, l'account dell'amministratore di sistema e le informazioni correlate.



Prima di avviare la console Web di vCloud Director, eseguire la procedura guidata

**Configurazione di VMware vCloud Director**, che raccoglie le informazioni necessarie per avviare la console Web.

In alternativa all'uso della procedura guidata **Configurazione di VMware vCloud Director**, per configurare l'installazione di vCloud Director è possibile utilizzare il sottocomando `system-setup` dello strumento di gestione delle celle. Per informazioni sullo strumento di gestione delle celle, vedere *Guida per gli amministratori di vCloud Director*.

#### Prerequisiti

- Verificare che i servizi di vCloud Director siano avviati in tutti i server.
- Richiedere un numero di serie di prodotto vCloud Director dal portale delle licenze VMware.

#### Procedura

##### Procedura

- 1 Aprire un browser Web e accedere all'URL visualizzato dallo script di configurazione.

Per individuare l'URL della procedura guidata **Configurazione di VMware vCloud Director** è anche possibile cercare il nome di dominio completo associato all'indirizzo IP specificato per il servizio HTTP durante l'installazione del primo server. Per connettersi alla procedura guidata, passare a `https://fully-qualified-domain-name`, ad esempio `https://mycloud.example.com`.

---

**Nota** L'avvio della procedura guidata potrebbe richiedere alcuni minuti.

---

- 2 Controllare la pagina di benvenuto e fare clic su **Avanti**.
- 3 Leggere e accettare il contratto di licenza e fare clic su **Avanti**.

Se si rifiuta il contratto di licenza, non sarà possibile procedere con la configurazione di vCloud Director.

- 4 Immettere il numero di serie del prodotto vCloud Director e fare clic su **Avanti**.
- 5 Immettere il nome utente, la password e le informazioni di contatto dell'amministratore di sistema di vCloud Director e fare clic su **Avanti**.

L'amministratore di sistema di vCloud Director dispone dei privilegi di utente con privilegi avanzati in tutto il cloud. L'amministratore di sistema può creare ulteriori account di amministratore di sistema.

**6** Configurare le impostazioni di sistema che controllano l'interazione di vCloud Director con vSphere e NSX Manager e fare clic su **Avanti**.

- a Nella casella di testo **Nome sistema**, immettere un nome per la cartella di vCenter Server da utilizzare per questa installazione di vCloud Director.
- b Nella casella di testo **ID installazione**, impostare l'ID per questa installazione di vCloud Director da utilizzare quando si creano gli indirizzi MAC per le schede NIC virtuali.

Se si prevede di creare reti estese in installazioni di vCloud Director in distribuzioni multisito, prendere in considerazione l'idea di impostare un ID di installazione univoco per ogni installazione di vCloud Director.

**7** Nella pagina Pronto per l'accesso, controllare le impostazioni e fare clic su **Fine**.

### Risultati

Al termine del processo di configurazione, si verrà reindirizzati alla pagina di accesso della console Web di vCloud Director.

### Operazioni successive

Accedere alla console Web di vCloud Director con il nome utente e la password dell'amministratore di sistema e iniziare il provisioning del cloud. Per informazioni sull'aggiunta di risorse a vCloud Director, vedere *Guida per gli amministratori di vCloud Director*.

# Distribuzione dell'appliance vCloud Director

# 6

È possibile creare un gruppo di server vCloud Director distribuendo una o più istanze dell'appliance vCloud Director. L'appliance vCloud Director viene distribuita utilizzando vSphere Client (HTML5), vSphere Web Client (Flex) o VMware OVF Tool.

---

**Importante** Le installazioni vCloud Director miste su Linux e le distribuzioni di appliance vCloud Director in un gruppo di server non sono supportate.

---

L'appliance vCloud Director è una macchina virtuale preconfigurata ottimizzata per l'esecuzione dei servizi di vCloud Director.

L'appliance viene distribuita con un nome nel formato VMware vCloud Director-*v.v.v.v-  
nnnnnn\_OVF10.ova*, dove *v.v.v.v* rappresenta la versione di prodotto e *nnnnnn* il numero di build. Ad esempio: VMware vCloud Director-9.7.0.0-9229800\_OVA10.ova.

Il pacchetto dell'appliance vCloud Director contiene il seguente software:

- Sistema operativo Photon™ di VMware.
- Gruppo di servizi di vCloud Director
- PostgreSQL 10

Le dimensioni primaria-piccola e standby-piccola dell'appliance di vCloud Director sono adatte per sistemi di laboratorio o di testing. Le dimensioni primaria-grande e standby-grande soddisfano i requisiti di dimensione minimi per i sistemi di produzione. In base al carico di lavoro, potrebbe essere necessario aggiungere altre risorse.

---

**Importante** L'installazione di un componente di terze parti nell'appliance vCloud Director non è supportata. È possibile installare solo i componenti VMware supportati in base alle [Tabelle di interoperabilità dei prodotti VMware](#). Ad esempio, è possibile installare una versione supportata di un agente di monitoraggio di VMware vRealize® Operations Manager™ o VMware vRealize® Log Insight™.

---

## Configurazione del database dell'appliance

A partire dalla versione 9.7, l'appliance vCloud Director include un database PostgreSQL incorporato con funzionalità a disponibilità elevata (HA). Per creare una distribuzione dell'appliance con un cluster HA del database, è necessario distribuire un'istanza dell'appliance vCloud Director come cella primaria e due istanze come celle di standby. È possibile distribuire istanze aggiuntive dell'appliance vCloud Director nel gruppo di server come celle dell'applicazione vCD, che eseguono solo il gruppo di servizi di vCloud Director senza il database incorporato. Le celle dell'applicazione vCD si connettono al database nella cella primaria. Vedere [Distribuzioni dell'appliance e configurazione della disponibilità elevata del database](#).

Per impostazione predefinita, l'appliance vCloud Director utilizza TLS, al posto del protocollo SSL obsoleto, per le connessioni al database, inclusa la replica. Questa funzionalità è attiva immediatamente dopo la distribuzione, con un certificato PostgreSQL autofirmato. Per utilizzare un certificato firmato da un'autorità di certificazione (CA), vedere [Sostituzione di un certificato autofirmato dell'interfaccia utente di gestione dell'appliance vCloud Director e di un database PostgreSQL incorporato](#).

---

**Nota** L'appliance vCloud Director non supporta i database esterni.

---

## Configurazione della rete dell'appliance

A partire dalla versione 9.7, l'appliance vCloud Director viene distribuita con due reti, eth0 e eth1, in modo da poter isolare il traffico HTTP dal traffico del database. Servizi diversi sono in ascolto su una o entrambe le interfacce di rete corrispondenti.

Servizio	Porta su eth0	Porta su eth1
SSH	22	22
HTTP	80	n/a
HTTPS	443	n/a
PostgreSQL	n/a	5432
Interfaccia utente di gestione	5480	5480
Proxy console	8443	n/a
JMX	8998, 8999	n/a
JMS/ActiveMQ	61616	n/a

L'appliance vCloud Director supporta la personalizzazione dell'utente delle regole del firewall mediante iptables. Per aggiungere regole iptables personalizzate, è possibile aggiungere i propri dati di configurazione alla fine del file `/etc/systemd/scripts/iptables`.

Questo capitolo include i seguenti argomenti:

- [Distribuzioni dell'appliance e configurazione della disponibilità elevata del database](#)
- [Prerequisiti per la distribuzione dell'appliance di vCloud Director](#)

- [Distribuzione dell'appliance vCloud Director mediante vSphere Web Client o vSphere Client](#)
- [Distribuzione dell'appliance vCloud Director tramite VMware OVF Tool](#)

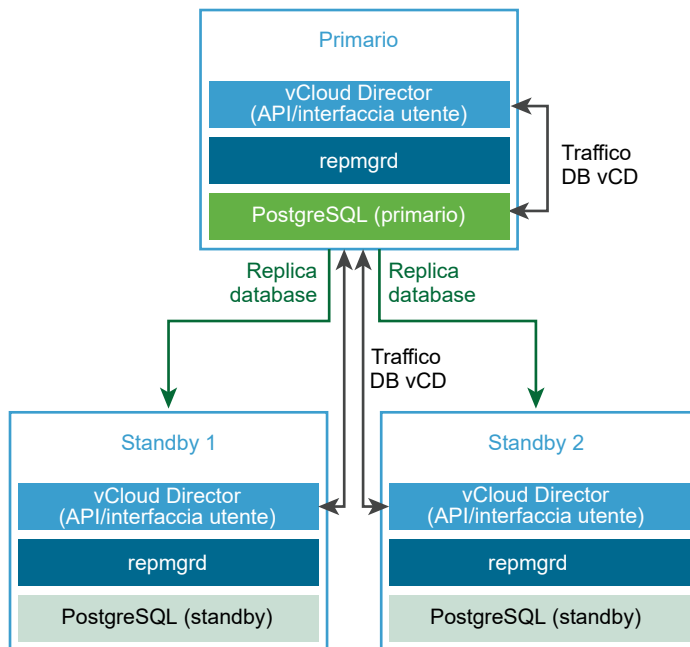
## Distribuzioni dell'appliance e configurazione della disponibilità elevata del database

L'appliance vCloud Director include un database PostgreSQL incorporato. Il database PostgreSQL incorporato include la suite di strumenti di Replication Manager (repmgr), che fornisce una funzionalità a disponibilità elevata (HA) a un cluster di server PostgreSQL. È possibile creare una distribuzione di appliance con un cluster HA del database che fornisce funzionalità di failover al database di vCloud Director.

È possibile distribuire l'appliance vCloud Director come cella primaria, cella di standby o cella dell'applicazione vCD. Vedere [Distribuzione dell'appliance vCloud Director mediante vSphere Web Client o vSphere Client](#), [Distribuzione dell'appliance vCloud Director tramite VMware OVF Tool](#) o [Distribuzione dell'appliance vCloud Director con certificati con caratteri jolly firmati per la comunicazione HTTPS e proxy console](#).

Per configurare la disponibilità elevata per il database di vCloud Director, quando si crea il gruppo di server, è possibile configurare un cluster HA del database distribuendo un'istanza primaria e due istanze di standby dell'appliance vCloud Director.

Figura 6-1. Un cluster HA di un database dell'appliance vCloud Director



## Creazione di una distribuzione dell'appliance vCloud Director con database HA

Per creare un gruppo di server vCloud Director con una configurazione di database HA, eseguire questo workflow:

- 1 Distribuire l'appliance vCloud Director come cella primaria.

La cella primaria è il primo membro del gruppo di server di vCloud Director. Il database incorporato è configurato come database di vCloud Director. Il nome del database è `vcld` e l'utente del database è `vcld`.

- 2 Verificare che la cella primaria sia in esecuzione.

- a Per verificare l'integrità del servizio vCloud Director, accedere con le credenziali dell'**amministratore di sistema** alla console Web di vCloud Director all'indirizzo `https://primary_eth0_ip_address/cld`.

- b Per verificare l'integrità del database PostgreSQL, accedere come **root** all'interfaccia utente di gestione dell'appliance all'indirizzo `https://primary_eth1_ip_address: 5480`.

Il nodo primario deve essere in stato di esecuzione.

- 3 Distribuire due istanze dell'appliance vCloud Director come celle di standby.

I database incorporati vengono configurati in modalità di replica con il database primario.

---

**Nota** Dopo la distribuzione iniziale dell'appliance di standby, Replication Manager inizia a sincronizzare il proprio database con il database dell'appliance primaria. Durante questo periodo, il database di vCloud Director e quindi l'interfaccia utente di vCloud Director non sono disponibili.

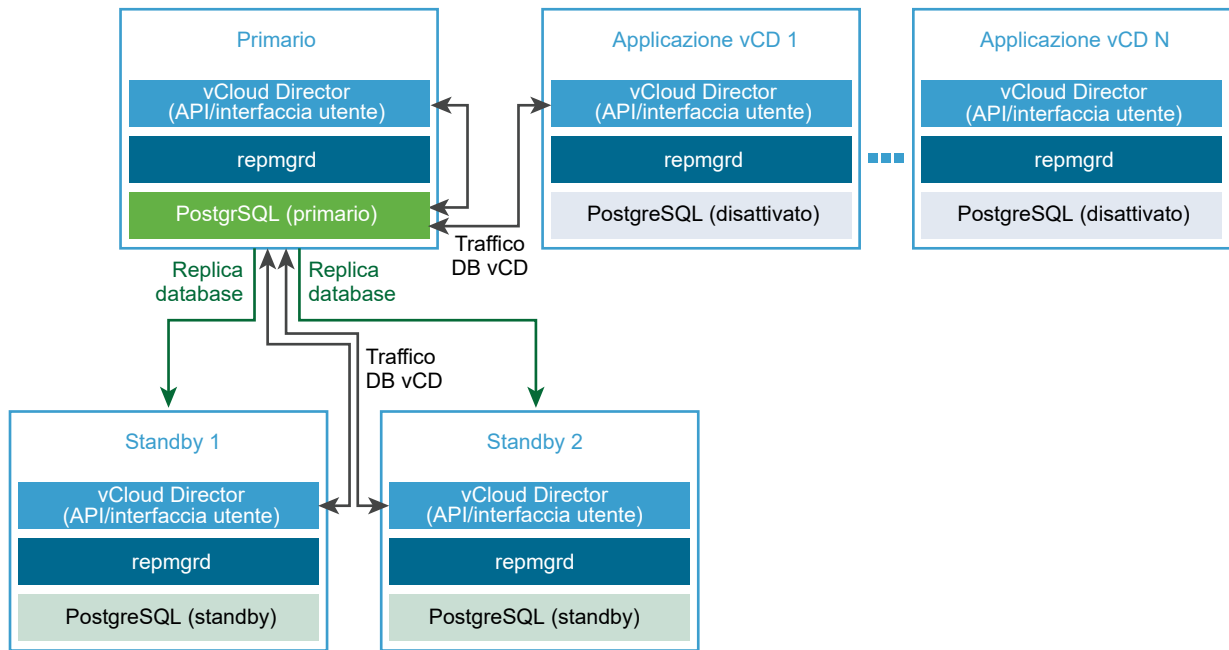
---

- 4 Verificare che tutte le celle nel cluster HA siano in esecuzione.

Vedere [Visualizzazione dello stato delle celle in un cluster ad alta disponibilità del database](#).

- 5 (Facoltativo) Distribuire una o più istanze dell'appliance vCloud Director come celle dell'applicazione vCD.

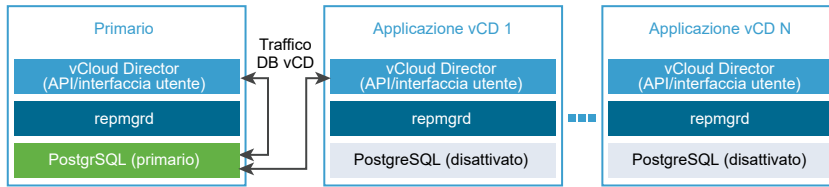
I database incorporati non vengono utilizzati. La cella dell'applicazione vCD si connette al database primario.



## Creazione di una distribuzione dell'appliance vCloud Director senza database HA

Per creare un server di vCloud Director senza una configurazione di database HA, eseguire questo workflow:

- 1 Distribuire l'appliance vCloud Director come cella primaria.  
 La cella primaria è il primo membro del gruppo di server di vCloud Director. Il database incorporato è configurato come database di vCloud Director. Il nome del database è `vcld` e l'utente del database è `vcld`.
- 2 Verificare che la cella primaria sia in esecuzione.
  - a Per verificare l'integrità del servizio vCloud Director, accedere con le credenziali dell'**amministratore di sistema** alla console Web di vCloud Director all'indirizzo `https://primary_eth0_ip_address/cld`.
  - b Per verificare l'integrità del database PostgreSQL, accedere come **root** all'interfaccia utente di gestione dell'appliance all'indirizzo `https://primary_eth1_ip_address:5480`.  
 Il nodo primario deve essere in stato di esecuzione.
- 3 (Facoltativo) Distribuire una o più istanze dell'appliance vCloud Director come celle dell'applicazione vCD.  
 Il database incorporato non viene utilizzato. La cella dell'applicazione vCD si connette al database primario.



## Prerequisiti per la distribuzione dell'appliance di vCloud Director

Per garantire la corretta distribuzione dell'appliance di vCloud Director, è necessario eseguire alcune attività e controlli preliminari prima di avviare la distribuzione.

- Assicurarsi di potere accedere al file `.ova` di vCloud Director.
- Prima di distribuire l'appliance primaria, preparare lo storage del servizio di trasferimento condiviso NFS. Vedere [Preparazione dello storage del server di trasferimento](#).

---

**Nota** Lo storage del servizio di trasferimento condiviso non deve contenere né un file `responses.properties` né una directory `appliance-nodes`.

---

- [Installazione e configurazione di un broker AMQP RabbitMQ](#).

## Metodi di distribuzione dell'appliance vCloud Director

- [Distribuzione dell'appliance vCloud Director mediante vSphere Web Client o vSphere Client](#)
- [Distribuzione dell'appliance vCloud Director tramite VMware OVF Tool](#)
- [Distribuzione dell'appliance vCloud Director con certificati con caratteri jolly firmati per la comunicazione HTTPS e proxy console](#)

## Distribuzione dell'appliance vCloud Director mediante vSphere Web Client o vSphere Client

È possibile distribuire l'appliance vCloud Director come modello OVF utilizzando vSphere Web Client (Flex) o vSphere Client (HTML5).

È necessario distribuire il primo membro di un gruppo di server di vCloud Director come cella primaria. È possibile distribuire un membro successivo di un gruppo di server di vCloud Director come cella di applicazione vCD o standby. Vedere [Distribuzioni dell'appliance e configurazione della disponibilità elevata del database](#).

---

**Importante** Le installazioni vCloud Director miste su Linux e le distribuzioni di appliance vCloud Director in un gruppo di server non sono supportate.

---

Per informazioni sulla distribuzione dei modelli OVF in vSphere, vedere *vSphere Virtual Machine Administration*.



In alternativa, è possibile distribuire l'appliance utilizzando VMware OVF Tool. Vedere [Distribuzione dell'appliance vCloud Director tramite VMware OVF Tool](#).

---

**Nota** La distribuzione dell'appliance vCloud Director in vCloud Director non è supportata.

---

### Prerequisiti

Vedere [Prerequisiti per la distribuzione dell'appliance di vCloud Director](#).

### Procedura

#### 1 [Avviamento della distribuzione dell'appliance vCloud Director](#)

Per avviare la distribuzione dell'appliance, aprire la procedura guidata di distribuzione in vSphere Web Client (Flex) o in vSphere Client (HTML5).

#### 2 [Personalizzazione dell'appliance di vCloud Director e completamento della distribuzione](#)

Per configurare i dettagli di vCloud Director, è possibile personalizzare il modello dell'appliance.

### Operazioni successive

- Configurare l'indirizzo del proxy della console pubblica, perché l'appliance vCloud Director utilizza la sua NIC eth0 con porta personalizzata 8443 per il servizio proxy della console. Vedere [Personalizzazione degli endpoint pubblici](#).
- Per aggiungere membri al gruppo di server vCloud Director, ripetere la procedura.
- Per inserire il codice di licenza, accedere alla console Web di vCloud Director.
- Per sostituire il certificato autofirmato che viene creato durante il primo avvio dell'appliance, è possibile [Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione per vCloud Director in Linux](#).

## Avviamento della distribuzione dell'appliance vCloud Director

Per avviare la distribuzione dell'appliance, aprire la procedura guidata di distribuzione in vSphere Web Client (Flex) o in vSphere Client (HTML5).

### Procedura

- 1 In vSphere Web Client o in vSphere Client, fare clic con il pulsante destro del mouse su un oggetto qualsiasi dell'inventario e scegliere **Distribuisci modello OVF**.
- 2 Immettere il percorso del file .ova di vCloud Director e fare clic su **Avanti**.
- 3 Immettere un nome per la macchina virtuale e passare al repository vCenter Server per selezionare il data center o la cartella in cui si desidera distribuire l'appliance, quindi fare clic su **Avanti**.
- 4 Selezionare l'host o il cluster ESXi in cui si desidera distribuire l'appliance e fare clic su **Avanti**.
- 5 Controllare i dettagli del modello e fare clic su **Avanti**.

- 6 Leggere e accettare i contratti di licenza e fare clic su **Avanti**.
- 7 Selezionare il tipo e le dimensioni della distribuzione e fare clic su **Avanti**.

Le dimensioni primaria-piccola e standby-piccola dell'appliance di vCloud Director sono adatte per sistemi di laboratorio o di testing. Le dimensioni primary-grande e standby-grande soddisfano i requisiti di dimensione minimi per i sistemi di produzione. In base al carico di lavoro, potrebbe essere necessario aggiungere altre risorse.

Opzione	Descrizione
<b>Primaria-piccola</b>	Distribuisce l'appliance con 12 GB di RAM e 2 vCPU come primo membro in un gruppo di server di vCloud Director. Il database incorporato nella cella primaria è configurato come database di vCloud Director. Il nome del database è vcloud e l'utente del database è vcloud.
<b>Primaria-grande</b>	Distribuisce l'appliance con 24 GB di RAM e 4 vCPU come primo membro in un gruppo di server di vCloud Director. Il database incorporato nella cella primaria è configurato come database di vCloud Director. Il nome del database è vcloud e l'utente del database è vcloud.
<b>Standby-piccola</b>	Utilizzato per unire una cella primaria-piccola nel cluster HA di un database. Distribuisce l'appliance con 12 GB di RAM e 2 vCPU come secondo o terzo membro in un gruppo di server di vCloud Director con una configurazione a disponibilità elevata del database. Il database incorporato in una cella di standby è configurato in modalità di replica con il database primario.
<b>Standby-grande</b>	Utilizzato per unire una cella primaria grande nel cluster HA di un database. Distribuisce l'appliance con 24 GB di RAM e 4 vCPU come secondo o terzo membro in un gruppo di server di vCloud Director con una configurazione a disponibilità elevata del database. Il database incorporato in un'appliance di standby è configurato in modalità di replica con il database primario.
<b>Applicazione cella vCD</b>	Distribuisce l'appliance con 8 GB di RAM e 2 vCPU come membro successivo in un gruppo di server di vCloud Director. Il database incorporato in una cella dell'applicazione vCD non viene utilizzato. La cella dell'applicazione vCD si connette al database primario.

**Importante** Le celle primaria e di standby in un gruppo di server di vCloud Director devono avere le stesse dimensioni. Un cluster HA di un database può essere costituito da una cella primaria-piccola e da due celle standby-piccole oppure da una cella primaria-grande e da due celle standby-grandi.

Dopo la distribuzione, è possibile riconfigurare le dimensioni dell'appliance.

- 8 Selezionare il formato del disco e l'archivio dati per i file di configurazione delle macchine virtuali e i dischi virtuali, quindi fare clic su **Avanti**.

I formati thick migliorano le prestazioni mentre i formati thin consentono di risparmiare spazio di storage.

- 9 Nei menu a discesa nelle celle **Rete di destinazione**, selezionare le reti di destinazione per le NIC eth1 e eth0 dell'appliance.

L'elenco di reti di origine potrebbe essere in ordine inverso. Verificare di aver selezionato la rete di destinazione corretta per ciascuna rete di origine.

---

**Importante** Le due reti di destinazione devono essere diverse.

---

- 10 Nei menu a discesa **Impostazioni allocazione IP** selezionare un'allocazione IP **Statica - Manuale** e un protocollo **IPv4**.

- 11 Fare clic su **Avanti**.

Si verrà reindirizzati alla pagina **Personalizza modello** per configurare i dettagli di vCloud Director.

## Personalizzazione dell'appliance di vCloud Director e completamento della distribuzione

Per configurare i dettagli di vCloud Director, è possibile personalizzare il modello dell'appliance.

Quando si personalizza l'appliance di vCloud Director, si configurano le impostazioni dell'appliance, il database e le proprietà di rete. Le impostazioni di sistema iniziali vengono configurate solo quando si distribuisce un'appliance primaria, che è il primo membro di un gruppo di server.

---

**Nota** Solo il [Passaggio 3](#) di questa procedura è facoltativo. È necessario completare tutti gli altri passaggi per personalizzare l'appliance di vCloud Director.

---

### Procedura

- 1 Nella sezione **Impostazioni appliance VCD**, configurare i dettagli dell'appliance.

Impostazione	Descrizione
<b>Server NTP</b>	Nome host o indirizzo IP del server NTP da utilizzare.
<b>Password root iniziale</b>	<p>La password root iniziale per l'appliance. Deve contenere almeno otto caratteri, un carattere maiuscolo, un carattere minuscolo, una cifra numerica e un carattere speciale.</p> <hr/> <p><b>Importante</b> La password root iniziale diventa la password dell'archivio chiavi. La distribuzione del cluster richiede che tutte le celle abbiano la stessa password root durante la distribuzione iniziale. Al termine del processo di avvio, è possibile modificare la password root in qualsiasi cella desiderata.</p> <hr/> <p><b>Nota</b> La procedura guidata di distribuzione OVF non convalida la password root iniziale rispetto ai criteri della password.</p> <hr/>
<b>Scadenza password root al primo accesso</b>	Se si desidera continuare a utilizzare la password iniziale dopo il primo accesso, è necessario verificare che la password iniziale soddisfi i criteri della password root. Per continuare a utilizzare la password root iniziale dopo il primo accesso, deselezionare questa opzione.

Impostazione	Descrizione
<b>Abilita SSH</b>	Disabilitata per impostazione predefinita.
<b>Montaggio NFS per il percorso del trasferimento file</b>	Vedere <a href="#">Preparazione dello storage del server di trasferimento</a> .

**Nota** Per informazioni su come modificare data, ora o fuso orario dell'appliance, vedere <https://kb.vmware.com/kb/59674>.

- Se si distribuisce il primo membro di un gruppo di server, nella sezione **Configurazione VCD - Richiesta solo per appliance primarie**, immettere i dettagli del database, creare l'account dell'**amministratore di sistema** e configurare le impostazioni di sistema.

Il nome del database è vcloud e l'utente del database è vcloud.

Impostazione	Descrizione
<b>Password DB "vcloud" per l'utente "vcloud"</b>	La password dell'utente del database di vcloud.
<b>Nome utente amministratore</b>	Nome utente per l'account dell' <b>amministratore di sistema</b> . Impostazione predefinita: administrator.
<b>Nome completo amministratore</b>	Nome completo dell' <b>amministratore di sistema</b> . Impostazione predefinita: vCD Admin.
<b>Password utente amministratore</b>	Password dell'account dell' <b>amministratore di sistema</b> .
<b>E-mail amministratore</b>	Indirizzo e-mail dell' <b>amministratore di sistema</b> .
<b>Nome sistema</b>	Nome della cartella di vCenter Server da creare per questa installazione di vCloud Director. Impostazione predefinita: vcd1.
<b>ID installazione</b>	ID per questa installazione di vCloud Director da utilizzare quando si creano gli indirizzi MAC per le schede NIC virtuali. Impostazione predefinita: 1. Se si prevede di creare reti estese in installazioni di vCloud Director in distribuzioni multisito, prendere in considerazione l'idea di impostare un ID di installazione univoco per ogni installazione di vCloud Director.

- (Facoltativo) Nella sezione **Proprietà di rete aggiuntive**, se la topologia di rete lo richiede, immettere le route statiche per le interfacce di rete eth0 e eth1 e fare clic su **Avanti**.

Potrebbe essere necessario fornire route statiche se si desidera raggiungere gli host su una route del gateway non predefinita. Ad esempio, l'infrastruttura di gestione è accessibile solo tramite l'interfaccia eth1, mentre il gateway predefinito è in eth0. Nella maggior parte dei casi, questa impostazione può rimanere vuota.

Le route statiche devono trovarsi in un elenco di specifiche delle route separate da virgole. Una specifica di route deve essere costituita dall'indirizzo IP del gateway di destinazione e, facoltativamente, da una specifica di rete CIDR (Classless Inter-Domain Routing). Ad esempio, **172.16.100.253 172.16.100.0/19, 172.16.100.253 192.168.100.0/24**.

- 4 Nella sezione **Proprietà di rete**, immettere i dettagli della rete per le schede NIC eth0 e eth1, quindi fare clic su **Avanti**.

**Nota** Tutte le impostazioni sono obbligatorie.

Impostazione	Descrizione
<b>Gateway predefinito</b>	Indirizzo IP del gateway predefinito per l'appliance.
<b>Nome dominio</b>	Il nome del dominio, ad esempio <i>mydomain.com</i> .
<b>Percorso di ricerca dominio</b>	Elenco di nomi di dominio separati da virgola o da uno spazio per il percorso di ricerca del dominio dell'appliance.
<b>Server nome di dominio</b>	Indirizzo IP del server dei nomi di dominio per l'appliance.
<b>Indirizzo IP di rete eth0</b>	Indirizzo IP dell'interfaccia eth0.
<b>Network mask eth0</b>	La maschera di rete o il prefisso per l'interfaccia eth0.
<b>Indirizzo IP di rete eth1</b>	Indirizzo IP dell'interfaccia eth1.
<b>Network mask eth1</b>	La maschera di rete o il prefisso per l'interfaccia eth1.

- 5 Nella pagina **Pronto per il completamento** controllare le impostazioni di configurazione per l'appliance vCloud Director e fare clic su **Fine** per avviare la distribuzione.

#### Operazioni successive

Attivare la macchina virtuale appena creata.

## Distribuzione dell'appliance vCloud Director tramite VMware OVF Tool

È possibile distribuire l'appliance vCloud Director come modello OVF utilizzando VMware OVF Tool.

È necessario distribuire il primo membro di un gruppo di server di vCloud Director come cella primaria. È possibile distribuire un membro successivo di un gruppo di server di vCloud Director come cella di applicazione vCD o standby. Vedere [Distribuzioni dell'appliance e configurazione della disponibilità elevata del database](#).

Per informazioni sull'installazione di OVF Tool, vedere il documento *Note di rilascio di VMware OVF Tool*.

Per informazioni sull'utilizzo di OVF Tool, vedere la *Guida per l'utente di OVF Tool*.

Prima di eseguire il comando di distribuzione, vedere [Prerequisiti per la distribuzione dell'appliance di vCloud Director](#).

Dopo aver distribuito l'appliance, controllare i messaggi di avviso o di errore nel file di registro di firstboot. Vedere [Esame dei file di registro nell'appliance vCloud Director](#).

## Opzioni di comando e proprietà di ovftool per la distribuzione dell'appliance vCloud Director

Opzione	Valore	Descrizione
--noSSLVerify	n/a	Ignora la verifica SSL per le connessioni vSphere.
--acceptAllEulas	n/a	Accetta tutti i contratti di licenza per l'utente finale (EULA).
--datastore	<i>target_vc_datastore</i>	Il nome dell'archivio dati di destinazione in cui archiviare i dischi virtuali e i file di configurazione delle macchine virtuali.
--allowAllExtraConfig	n/a	Converte tutte le opzioni di configurazione aggiuntive in formato VMX.
--net:"eth0 Network"	<i>portgroup_on_vc_for_eth0</i>	La rete di destinazione per la rete eth0 dell'appliance.  <b>Importante</b> Deve essere diversa dalla rete di destinazione di eth1.
--net:"eth1 Network"	<i>portgroup_on_vc_for_eth1</i>	La rete di destinazione per la rete eth1 dell'appliance.  <b>Importante</b> Deve essere diversa dalla rete di destinazione di eth0.
--name	<i>vm_name_on_vc</i>	Il nome della macchina virtuale per l'appliance.
--diskMode	thin o thick	Il formato del disco per i dischi virtuali e i file di configurazione delle macchine virtuali.
--prop:"vami.ip0.VMware_vCloud_Director"	<i>eth0_ip_address</i>	Indirizzo IP di eth0. Utilizzato per l'accesso dell'API e dell'interfaccia utente. In questo indirizzo, la ricerca DNS inversa determina e imposta il nome host dell'appliance.
--prop:"vami.ip1.VMware_vCloud_Director"	<i>eth1_ip_address</i>	Indirizzo IP di eth1. Utilizzato per accedere ai servizi interni, incluso il servizio del database PostgreSQL incorporato.
--prop:"vami.DNS.VMware_vCloud_Director"	<i>dns_ip_address</i>	Indirizzo IP del server dei nomi di dominio per l'appliance.
--prop:"vami.domain.VMware_vCloud_Director"	<i>domain_name</i>	Dominio di ricerca DNS. Viene visualizzato come primo elemento nel percorso di ricerca.
--prop:"vami.gateway.VMware_vCloud_Director"	<i>gateway_ip_address</i>	Indirizzo IP del gateway predefinito per l'appliance.

Opzione	Valore	Descrizione
--prop:"vami.netmask0.VMware_vCloud_Director"	<del>netmask</del>	La maschera di rete o il prefisso per l'interfaccia eth0.
--prop:"vami.netmask1.VMware_vCloud_Director"	<del>netmask</del>	La maschera di rete o il prefisso per l'interfaccia eth1.
--prop:"vami.searchpath.VMware_vCloud_Director"	<del>list" of domain names</del>	Il percorso di ricerca del dominio dell'appliance. Un elenco di nomi di dominio separati da una virgola o da uno spazio.
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"	<del>enable</del>	Abilita o disabilita l'accesso <b>root</b> SSH all'appliance.
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"	<del>expire</del>	Determina se continuare o meno a utilizzare la password iniziale dopo il primo accesso.
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"	<del>ip_address:nfs_mount_path</del>	L'indirizzo IP e il percorso di esportazione del server NFS esterno. Utilizzato solo per una cella primaria.
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"	<del>ip_address</del>	L'indirizzo IP del server temporale.
--prop:"vcloudapp.varroot-password.VMware_vCloud_Director"	<del>password</del>	La password root iniziale per l'appliance. Deve contenere almeno otto caratteri, un carattere maiuscolo, un carattere minuscolo, una cifra numerica e un carattere speciale.  <b>Importante</b> La password root iniziale diventa la password dell'archivio chiavi. La distribuzione del cluster richiede che tutte le celle abbiano la stessa password root durante la distribuzione iniziale. Al termine del processo di avvio, è possibile modificare la password root in qualsiasi cella desiderata.
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"	<del>password</del>	La password del database dell'utente <b>vcloud</b> . Utilizzata solo per una cella primaria.
--prop:"vcloudwiz.admin_email.VMware_vCloud_Director"	<del>admin_email_address</del>	Indirizzo e-mail dell'account dell' <b>amministratore di sistema</b> . Utilizzato solo per una cella primaria.
--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director"	<del>admin_first_name</del>	Il nome dell'account dell' <b>amministratore di sistema</b> . Utilizzato solo per una cella primaria.
--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director"	<del>admin_password</del>	Password dell'account dell' <b>amministratore di sistema</b> . Utilizzata solo per una cella primaria.

Opzione	Valore	Descrizione
<code>--prop:"vcloudwiz.admin_username.VMware_vCloud_Director_admin_username"</code>	<code>admin_username</code>	Nome utente per l'account dell' <b>amministratore di sistema</b> . Utilizzato solo per una cella primaria.
<code>--prop:"vcloudwiz.inst_id.VMware_vCloud_Director_inst_ID"</code>	<code>inst_id</code>	L'ID di installazione di vCloud Director. Utilizzato solo per una cella primaria.
<code>--prop:"vcloudconf.sys_name.VMware_vCloud_Director_sys_name"</code>	<code>sys_name</code>	Nome della cartella di vCenter Server da creare per questa installazione di vCloud Director.
<code>--prop:"vcloudnet.routes0.VMware_vCloud_Director_routes0_cidr, ip_address2, ..."</code>	<code>routes0_cidr, ip_address2, ...</code>	Facoltativa. Route statiche per l'interfaccia eth0. Deve essere un elenco delle specifiche delle route separate da virgola. La specifica di una route deve essere costituita da una indirizzo IP del gateway e, facoltativamente, da una specifica di rete CIDR (Classless Inter-Domain Routing) (prefisso/bit). Ad esempio, <b>172.16.100.253 172.16.100/19, 172.16.200.253</b> .
<code>--prop:"vcloudnet.routes1.VMware_vCloud_Director_routes1_cidr, ip_address2, ..."</code>	<code>routes1_cidr, ip_address2, ...</code>	Facoltativa. Route statiche per l'interfaccia eth1. Deve essere un elenco delle specifiche delle route separate da virgola. La specifica di una route deve essere costituita da una indirizzo IP del gateway e, facoltativamente, da una specifica di rete CIDR (Classless Inter-Domain Routing) (prefisso/bit). Ad esempio, <b>172.16.100.253 172.16.100/19, 172.16.200.253</b> .



Opzione	Valore	Descrizione
--deploymentOption	primary-small,primary-large, standby-small, standby-large o cell	<p>Il tipo e le dimensioni dell'appliance che si desidera distribuire.</p> <p>Le dimensioni primaria-piccola e standby-piccola dell'appliance sono adatte per sistemi di laboratorio o di testing. Le dimensioni primaria-grande e standby-grande soddisfano i requisiti di dimensione minimi per i sistemi di produzione. In base al carico di lavoro, potrebbe essere necessario aggiungere altre risorse.</p> <ul style="list-style-type: none"> <li>■ <b>primary-small</b> distribuisce l'appliance con 12 GB di RAM e 2 vCPU come primo membro in un gruppo di server di vCloud Director. Il database incorporato nella cella primaria è configurato come database di vCloud Director. Il nome del database è vcloud e l'utente del database è vcloud.</li> <li>■ <b>primary-large</b> distribuisce l'appliance con 24 GB di RAM e 4 vCPU come primo membro in un gruppo di server di vCloud Director. Il database incorporato nella cella primaria è configurato come database di vCloud Director. Il nome del database è vcloud e l'utente del database è vcloud.</li> <li>■ <b>standby-small</b> distribuisce l'appliance con 12 GB di RAM e 2 vCPU come secondo o terzo membro in un gruppo di server di vCloud Director con una configurazione a disponibilità elevata del database. Il database incorporato in una cella di standby è configurato in modalità di replica con il database primario.</li> <li>■ <b>standby-large</b> distribuisce l'appliance con 24 GB di RAM e 4 vCPU come secondo o terzo membro in un gruppo di server di vCloud Director con una configurazione a disponibilità elevata del database. Il database incorporato in una cella di standby è configurato in modalità di replica con il database primario.</li> <li>■ <b>cell</b> distribuisce l'appliance con 8 GB di RAM e 2 vCPU come membro successivo in un gruppo di</li> </ul>

Opzione	Valore	Descrizione
		server di vCloud Director. Il database incorporato in una cella dell'applicazione vCD non viene utilizzato. La cella dell'applicazione vCD si connette al database primario.
		<p><b>Importante</b> Le celle primaria e di standby in un gruppo di server di vCloud Director devono avere le stesse dimensioni. Un cluster HA di un database può essere costituito da una cella primaria-piccola e da due celle standby-piccole oppure da una cella primaria-grande e da due celle standby-grandi.</p> <p>Dopo la distribuzione, è possibile riconfigurare le dimensioni dell'appliance.</p>
--powerOn	<i>path_to_ova</i>	Attiva la macchina virtuale dopo la distribuzione.

## Comando di esempio per la distribuzione dell'appliance primaria vCloud Director

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp_server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot_password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="Xj052mXAP7n#" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="o@e@vJW26Pnb" \
```

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

## Comando di esempio per la distribuzione di un'appliance di standby vCloud Director

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

# Creazione e gestione di certificati SSL dell'appliance vCloud Director

# 7

L'appliance vCloud Director utilizza SSL per proteggere le comunicazioni tra client e server. Ogni appliance vCloud Director deve supportare due endpoint SSL diversi, per le comunicazioni proxy HTTPS e della console.

Entrambi possono essere costituiti da indirizzi IP separati o da un singolo indirizzo IP con due porte diverse. Ogni endpoint richiede il suo certificato SSL. È possibile utilizzare lo stesso certificato (ad esempio un certificato con caratteri jolly) per entrambi gli endpoint.

Questo capitolo include i seguenti argomenti:

- [Distribuzione dell'appliance vCloud Director con certificati con caratteri jolly firmati per la comunicazione HTTPS e proxy console](#)
- [Creazione e importazione di certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director](#)
- [Importazione di chiavi private e certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director](#)
- [Sostituzione di un certificato autofirmato dell'interfaccia utente di gestione dell'appliance vCloud Director e di un database PostgreSQL incorporato](#)
- [Rinnovo dei certificati dell'appliance vCloud Director](#)

## Distribuzione dell'appliance vCloud Director con certificati con caratteri jolly firmati per la comunicazione HTTPS e proxy console

È possibile distribuire l'appliance vCloud Director con certificati con caratteri jolly firmati. È possibile utilizzare questi certificati per proteggere un numero illimitato di server che sono sottodomini del nome di dominio indicato nel certificato.

Per impostazione predefinita, quando si distribuiscono le appliance vCloud Director, vCloud Director genera certificati autofirmati e li utilizza per configurare la cella vCloud Director per la comunicazione HTTPS e proxy console.

Quando si distribuisce correttamente un'appliance primaria, la logica di configurazione dell'appliance copia il file `responses.properties` dall'appliance primaria allo storage comune del servizio di trasferimento condiviso NFS in `/opt/vmware/vcloud-director/data/transfer`. Le altre appliance distribuite per questo gruppo di server vCloud Director utilizzano questo file per eseguire la configurazione automaticamente. Il file `responses.properties` include un percorso per l'archivio chiavi del certificato SSL, che include i certificati autofirmati generati automaticamente `user.keystore.path`. Per impostazione predefinita, questo percorso reindirizza a un file dell'archivio chiavi locale per ogni appliance.

Dopo aver distribuito l'appliance primaria, è possibile riconfigurarla in modo che utilizzi certificati firmati. Per ulteriori informazioni sulla creazione dell'archivio chiavi con certificati firmati, vedere [Creazione e importazione di certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director](#).

Se i certificati firmati utilizzati nell'appliance primaria vCloud Director sono certificati con caratteri jolly firmati, possono essere applicati a tutte le altre appliance nel gruppo di server di vCloud Director, ovvero celle di standby e celle dell'applicazione vCloud Director. È possibile utilizzare la distribuzione dell'appliance con certificati con caratteri jolly firmati per la comunicazione HTTPS e proxy console per configurare le celle aggiuntive con i certificati SSL con caratteri jolly firmati.

#### Prerequisiti

- Verificare che l'archivio chiavi contenente i certificati SSL con caratteri jolly firmati per gli alias HTTPS e proxy console sia disponibile nell'appliance primaria, ovvero `/opt/vmware/vcloud-director/certificates.ks`.
  - Se è necessario creare coppie di chiavi e importare file di certificati firmati da un'autorità di certificazione, vedere [Creazione e importazione di certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director](#).
  - Se si dispone già di chiavi private e di file di certificati firmati da un'autorità di certificazione, vedere [Importazione di chiavi private e certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director](#).
- Verificare che la password privata per le chiavi all'interno dell'archivio chiavi corrisponda alla password dell'archivio chiavi. La password dell'archivio chiavi deve coincidere con la password root iniziale utilizzata durante la distribuzione di tutte le appliance, ad esempio

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

#### Procedura

- 1 Copiare il nuovo file `certificates.ks` contenente i certificati correttamente firmati dall'appliance primaria alla condivisione di trasferimento in `/opt/vmware/vcloud-director/data/transfer/`.

- 2 Impostare il proprietario e le autorizzazioni di gruppo nel file dell'archivio chiavi su **vccloud**.

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

- 3 Verificare che il proprietario del file dell'archivio chiavi disponga delle autorizzazioni di lettura e scrittura.

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

- 4 Nell'appliance primaria, eseguire il comando per importare i nuovi certificati firmati nell'istanza di vCloud Director.

Questo comando aggiorna anche il file `responses.properties` nella condivisione di trasferimento, modificando la variabile `user.keystore.path` in modo che punti al file dell'archivio chiavi nella condivisione di trasferimento.

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

- 5 Per applicare i nuovi certificati firmati, riavviare il servizio `vmware-vcd` nell'appliance primaria.

```
service vmware-vcd restart
```

- 6 Distribuire le appliance della cella di standby e della cella dell'applicazione, utilizzando la password root iniziale che corrisponde alla password dell'archivio chiavi.

## Risultati

Tutte le appliance appena distribuite che utilizzano lo stesso storage del servizio di trasferimento condiviso NFS sono configurate con gli stessi certificati SSL con caratteri jolly utilizzati dall'appliance primaria.

## Creazione e importazione di certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director

La creazione e l'importazione di certificati firmati da un'autorità di certificazione (CA) offrono il livello di attendibilità più elevato per le comunicazioni SSL e consentono di proteggere le connessioni nel cloud.

Ogni server vCloud Director richiede due certificati SSL per proteggere le comunicazioni tra client e server. Ogni server vCloud Director deve supportare due endpoint SSL diversi, per le comunicazioni proxy HTTPS e della console.

Nell'appliance di vCloud Director, questi due endpoint condividono lo stesso indirizzo IP o nome host, ma utilizzano due porte distinte, ovvero 443 per le comunicazioni HTTPS e 8443 per le comunicazioni proxy della console. Ogni endpoint deve disporre del proprio certificato SSL. È possibile utilizzare lo stesso certificato per entrambi gli endpoint, ad esempio utilizzando un certificato con caratteri jolly.

I certificati per entrambi gli endpoint devono includere sia un'estensione di nome distinto X.500 sia un'estensione di nome alternativo dell'oggetto X.509.

Se si dispone già di chiavi private e di file di certificati firmati dall'autorità di certificazione, seguire la procedura descritta in [Importazione di chiavi private e certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director](#).

---

**Importante** Al momento della distribuzione, l'appliance di vCloud Director genera certificati autofirmati con una dimensione di chiave di 2048 bit. È necessario valutare i requisiti di sicurezza dell'installazione prima di scegliere una dimensione di chiave appropriata. Le dimensioni chiave inferiori a 1024 bit non sono più supportate, come riportato nella Pubblicazione speciale 800-131A del NIST.

---

La password dell'archivio chiavi utilizzata in questa procedura è la password dell'utente **root** ed è rappresentata come *root\_passwd*.

### Prerequisiti

Familiarizzare con il comando `keytool`. È possibile utilizzare `keytool` per importare certificati SSL firmati dall'autorità di certificazione nell'appliance vCloud Director. vCloud Director inserisce una copia di `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`.

### Procedura

- 1 Accedere direttamente o con SSH alla console dell'appliance vCloud Director come **root**.
- 2 In base alle esigenze dell'ambiente, scegliere una delle seguenti opzioni.

Quando si distribuisce l'appliance di vCloud Director, vCloud Director genera automaticamente certificati autofirmati con una dimensione di chiave di 2048 bit per il servizio HTTPS e il servizio proxy della console.

- Se si desidera che l'autorità di certificazione firmi i certificati generati al momento della distribuzione, andare al [Passaggio Passaggio 5](#).
- Se si desidera generare nuovi certificati con opzioni personalizzate, ad esempio una dimensione di chiave maggiore, continuare con il [Passaggio Passaggio 3](#).

- 3 Eseguire il comando per creare un backup del file `certificates.ks` esistente.

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

- 4 Eseguire il comando per creare una coppia di chiavi pubblica e privata per il servizio HTTPS e per il servizio proxy della console.

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

Il comando crea o aggiorna un archivio chiavi in `certificates.ks` con la password specificata. I certificati vengono creati utilizzando i valori predefiniti del comando. In base alla configurazione DNS dell'ambiente, il nome comune dell'autorità emittente è impostato sull'indirizzo IP o sul nome di dominio completo per ciascun servizio. Il certificato utilizza una lunghezza chiave a 2048 bit predefinita, che scade un anno dopo la sua creazione.

---

**Importante** A causa delle limitazioni della configurazione nell'appliance di vCloud Director, è necessario utilizzare la posizione `/opt/vmware/vcloud-director/certificates.ks` per l'archivio chiavi dei certificati.

---

**Nota** È possibile utilizzare la password **root** dell'appliance come password dell'archivio chiavi.

---

- 5 Creare richieste di firma del certificato (CSR) per il servizio HTTPS e per il servizio proxy della console.

---

**Importante** L'appliance di vCloud Director utilizza lo stesso indirizzo IP e nome host sia per il servizio HTTPS sia per il servizio proxy della console. Per questo motivo, i comandi di creazione delle richieste CSR devono disporre degli stessi DNS e IP per l'argomento dell'estensione del nome alternativo del soggetto (SAN).

---

- a Creare una richiesta di firma del certificato nel file `http.csr`.

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

- b Creare una richiesta di firma del certificato nel file `consoleproxy.csr`.

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

- 6 Inviare le richieste di firma del certificato all'autorità di certificazione.

Se l'autorità di certificazione richiede di specificare un tipo di Web server, usare Jakarta Tomcat.

Procurarsi i certificati firmati dall'autorità di certificazione.

- 7 Copiare i certificati firmati dall'autorità di certificazione, il certificato root dell'autorità di certificazione e tutti i certificati intermedi nell'appliance di vCloud Director.



**8** Eseguire i comandi per importare i certificati firmati nell'archivio chiavi JCEKS.

- a Importare il certificato root dell'autorità di certificazione dal file `root.cer` nel file dell'archivio chiavi `certificates.ks`.

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

- b Se si ricevono certificati intermedi, importarli dal file `intermediate.cer` nel file di archivio chiavi `certificates.ks`.

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

- c Importare il certificato del servizio HTTPS.

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

- d Importare il certificato del servizio proxy della console.

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

I comandi sovrascrivono il file `certificates.ks` con le versioni dei certificati firmate dall'autorità di certificazione appena acquisite.

- 9** Per verificare se i certificati sono stati importati, eseguire il comando per elencare il contenuto del file di archivio chiavi.

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

- 10** Eseguire il comando per importare i certificati nell'istanza di vCloud Director.

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

- 11** Per applicare i nuovi certificati firmati, riavviare il servizio `vmware-vcd` nell'appliance di vCloud Director.

```
service vmware-vcd restart
```

**Operazioni successive**

- Se si utilizzano certificati con caratteri jolly, vedere [Distribuzione dell'appliance vCloud Director con certificati con caratteri jolly firmati per la comunicazione HTTPS e proxy console](#).
- Se non si utilizzano certificati con caratteri jolly, ripetere questa procedura in tutti i server vCloud Director nel gruppo di server.

- Per ulteriori informazioni sulla sostituzione dei certificati per il database PostgreSQL incorporato e per l'interfaccia utente di gestione dell'appliance di vCloud Director, vedere [Sostituzione di un certificato autofirmato dell'interfaccia utente di gestione dell'appliance vCloud Director e di un database PostgreSQL incorporato](#).

## Importazione di chiavi private e certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director

Se si dispone dei file delle chiavi private e dei file dei certificati firmati dall'autorità di certificazione, prima di importare gli archivi chiavi nell'ambiente di vCloud Director, è necessario creare i file di archivio chiavi in cui importare i certificati e le chiavi private per il servizio HTTPS e per il servizio proxy della console.

### Prerequisiti

- Familiarizzare con il comando `keytool`. È possibile utilizzare `keytool` per importare certificati SSL firmati dall'autorità di certificazione nell'appliance vCloud Director. vCloud Director inserisce una copia di `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`.
- Copiare nell'appliance i certificati intermedi, il certificato CA root, il servizio HTTPS firmato dall'autorità di certificazione, nonché le chiavi private e i certificati del servizio proxy della console.

### Procedura

- 1 Accedere direttamente o con SSH alla console dell'appliance vCloud Director come **root**.
- 2 Se si dispone di certificati intermedi, eseguire il comando per combinare il certificato root firmato dall'autorità di certificazione con i certificati intermedi e creare una catena di certificati.

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

- 3 Utilizzare OpenSSL per creare i file dell'archivio chiavi PKCS12 intermedi per il servizio HTTPS e per il servizio proxy della console con la chiave privata, la catena di certificati e il rispettivo alias, quindi specificare una password per ciascun file di archivio chiavi.

- a Creare il file dell'archivio chiavi per il servizio HTTPS.

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

- b Creare il file dell'archivio dati per il servizio proxy della console.

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

- 4 Eseguire il comando per creare un backup del file `certificates.ks` esistente.

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

- 5 Utilizzare il comando `keytool` per importare gli archivi chiavi PKCS12 nell'archivio chiavi JCEKS.

- a Importare l'archivio chiavi PKCS12 per il servizio HTTPS.

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

- b Importare l'archivio chiavi PKCS12 per il servizio proxy della console.

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

- 6 Verificare che l'importazione dei certificati venga eseguita correttamente.

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

- 7 Eseguire il comando per importare i certificati firmati nell'istanza di vCloud Director.

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

- 8 Per applicare i certificati firmati dall'autorità di certificazione, riavviare il servizio `vmware-vcd` nell'appliance di vCloud Director.

```
service vmware-vcd restart
```

#### Operazioni successive

- Se si utilizzano certificati con caratteri jolly, vedere [Distribuzione dell'appliance vCloud Director con certificati con caratteri jolly firmati per la comunicazione HTTPS e proxy console](#).
- Se non si utilizzano certificati con caratteri jolly, ripetere questa procedura in tutte le celle dell'appliance di vCloud Director nel gruppo di server.
- Per ulteriori informazioni sulla sostituzione dei certificati per il database PostgreSQL incorporato e per l'interfaccia utente di gestione dell'appliance di vCloud Director, vedere [Sostituzione di un certificato autofirmato dell'interfaccia utente di gestione dell'appliance vCloud Director e di un database PostgreSQL incorporato](#).

## Sostituzione di un certificato autofirmato dell'interfaccia utente di gestione dell'appliance vCloud Director e di un database PostgreSQL incorporato

Per impostazione predefinita, il database PostgreSQL incorporato e l'interfaccia utente di gestione dell'appliance vCloud Director condividono un set di certificati SSL autofirmati. Per maggiore sicurezza, è possibile sostituire i certificati autofirmati predefiniti con certificati firmati dall'autorità di certificazione (CA).

Quando si distribuisce l'appliance vCloud Director, genera certificati autofirmati con un periodo di validità di 365 giorni. L'appliance vCloud Director utilizza due set di certificati SSL. Il servizio vCloud Director utilizza un set di certificati per le comunicazioni HTTPS e del proxy della console. Il database PostgreSQL incorporato e l'interfaccia utente di gestione dell'appliance vCloud Director condividono l'altro set di certificati SSL.

---

**Nota** Il processo di sostituzione del database e dei certificati dell'interfaccia utente di gestione dell'appliance non influisce sui certificati per le comunicazioni HTTPS e proxy della console. La sostituzione di uno dei set di certificati non significa che è necessario sostituire l'altro set.

---

### Procedura

- 1 Inviare la richiesta di firma del certificato che si trova in `/opt/vmware/appliance/etc/ssl/vcd_ova.csr` all'autorità di certificazione per la firma.
- 2 Se si sta sostituendo il certificato per il database primario, attivare la modalità di manutenzione per tutti gli altri nodi per evitare la possibile perdita di dati.
- 3 Sostituire il certificato in formato PEM esistente in `/opt/vmware/appliance/etc/ssl/vcd_ova.crt` con il certificato firmato, ottenuto dall'autorità di certificazione nel [passaggio 1](#).
- 4 Per ritirare il nuovo certificato, riavviare i servizi `vpostgres`, `nginx` e `vcd_ova_ui`.

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

```
systemctl restart vpostgres.service
```

- 5 Se si sta sostituendo il certificato per il database primario, disattivare la modalità di manutenzione per tutti gli altri nodi.

### Risultati

Il nuovo certificato viene importato nell'archivio attendibilità di vCloud Director in altre celle di vCloud Director alla successiva esecuzione della funzionalità `appliance-sync`. L'operazione potrebbe richiedere fino a 60 secondi.

## Rinnovo dei certificati dell'appliance vCloud Director

Quando si distribuisce l'appliance vCloud Director, genera certificati autofirmati con un periodo di validità di 365 giorni. Se nell'ambiente sono presenti certificati in scadenza o scaduti, è possibile generare nuovi certificati autofirmati. È necessario rinnovare i certificati per ogni cella di vCloud Director singolarmente.

L'appliance vCloud Director utilizza due set di certificati SSL. Il servizio vCloud Director utilizza un set di certificati per le comunicazioni HTTPS e per le comunicazioni proxy della console. Il database PostgreSQL incorporato e l'interfaccia utente di gestione dell'appliance vCloud Director condividono l'altro set di certificati SSL.

È possibile modificare entrambi i set di certificati autofirmati. In alternativa, se si utilizzano certificati firmati da un'autorità di certificazione per le comunicazioni HTTPS e del proxy della console di vCloud Director, è possibile modificare solo il database PostgreSQL incorporato e il certificato dell'interfaccia utente di gestione dell'appliance. I certificati firmati da un'autorità di certificazione includono una catena di attendibilità completa la cui root è un'autorità di certificazione pubblica nota.

### Prerequisiti

Se si sta rinnovando il certificato per il nodo primario in un cluster a disponibilità elevata del database, attivare la modalità di manutenzione per tutti gli altri nodi per evitare la perdita di dati. Vedere [Gestione di una cella](#).

### Procedura

- 1 Accedere direttamente o tramite SSH al sistema operativo dell'appliance vCloud Director come **root**.
- 2 Per arrestare i servizi vCloud Director, eseguire il comando seguente.

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

- 3 Per generare nuovi certificati autofirmati, eseguire il comando seguente.

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

Questo comando mette automaticamente in uso i certificati appena generati per il database PostgreSQL incorporato e l'interfaccia utente di gestione dell'appliance. PostgreSQL e i server Nginx vengono riavviati. Il comando genera un nuovo archivio chiavi di certificati `/opt/vmware/vcloud-director/certificates.ks` con nuovi certificati autofirmati per la comunicazione HTTPS e proxy console di vCloud Director, utilizzati in [Passaggio 4](#).

- 4 Se non si utilizzano certificati firmati da un'autorità di certificazione, eseguire il comando per importare i certificati autofirmati appena generati in vCloud Director.

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

## 5 Riavviare il servizio vCloud Director.

```
service vmware-vcd start
```

### Risultati

I certificati autofirmati rinnovati sono visibili nell'interfaccia utente di vCloud Director.

Il nuovo certificato PostgreSQL viene importato nell'archivio attendibilità di vCloud Director in altre celle di vCloud Director alla successiva esecuzione della funzionalità `appliance-sync`. L'operazione potrebbe richiedere fino a 60 secondi.

### Operazioni successive

Se necessario, è possibile sostituire un certificato autofirmato con un certificato firmato da un'autorità di certificazione esterna o interna.

# Configurazione dell'appliance vCloud Director



È possibile visualizzare lo stato delle celle in un cluster HA del database, eseguire il backup e ripristinare il database integrato e riconfigurare le impostazioni dell'appliance.

Dopo aver distribuito l'appliance vCloud Director, non è possibile modificare gli indirizzi IP di rete eth0 e eth1 o il nome host dell'appliance. Se si desidera che l'appliance vCloud Director disponga di indirizzi o nome host diversi, è necessario distribuire una nuova appliance.

Se è necessario eseguire la manutenzione di un'appliance che richiede l'arresto del cluster a disponibilità elevata del database, per evitare problemi di sincronizzazione, arrestare innanzitutto l'appliance primaria e quindi le appliance di standby.

Questo capitolo include i seguenti argomenti:

- [Visualizzazione dello stato delle celle in un cluster ad alta disponibilità del database](#)
- [Ripristino da un errore di database primario in un cluster ad alta disponibilità](#)
- [Backup e ripristino del database integrato dell'appliance vCloud Director](#)
- [Configurazione dell'accesso esterno al database di vCloud Director](#)
- [Abilitazione o disabilitazione dell'accesso SSH all'appliance di vCloud Director](#)
- [Modifica delle impostazioni DNS dell'appliance vCloud Director](#)
- [Modifica delle route statiche per le interfacce di rete dell'appliance vCloud Director](#)
- [Script di configurazione nell'appliance vCloud Director](#)
- [Modifica delle configurazioni di PostgreSQL nell'appliance di vCloud Director](#)

## Visualizzazione dello stato delle celle in un cluster ad alta disponibilità del database

Per visualizzare lo stato delle celle primarie e di standby in un cluster di database dell'appliance ad alta disponibilità (HA), è possibile accedere all'interfaccia utente di gestione dell'appliance di qualsiasi cella dal cluster di HA del database.

Il cluster di HA del database dell'appliance vCloud Director è costituito da una cella primaria e due celle standby. Vedere [Distribuzioni dell'appliance e configurazione della disponibilità elevata del database](#).

## Procedura

- 1 In un browser Web, passare all'interfaccia utente di gestione dell'appliance all'indirizzo `https://vcd_ip_address:5480`.
- 2 Effettuare l'accesso come utente **root**.
- 3 Per visualizzare i dettagli relativi alle celle nel cluster di HA di database, fare clic su **Disponibilità del database vCD**.

Proprietà	Descrizione
Nome	Il nome DNS della cella.
Ruolo	Può essere primario o in standby. Un cluster HA di database dell'appliance è composto da una cella primaria e da due celle di standby.
Stato	Può essere in esecuzione, non raggiungibile o non riuscita. Un asterisco (*) indica lo stato della cella primaria.
Seguenti	Il nome della cella primaria con cui la cella di standby viene replicata.

## Operazioni successive

Se una cella di standby non si trova in uno stato di esecuzione, distribuire una nuova cella di standby.

Se la cella primaria non si trova in uno stato di esecuzione, [Ripristino da un errore di database primario in un cluster ad alta disponibilità](#).

## Ripristino da un errore di database primario in un cluster ad alta disponibilità

Se la cella primaria non è eseguita correttamente, per ripristinare il database vCloud Director, è possibile promuovere una delle celle di standby per diventare la nuova cella primaria. Dopo di che, è necessario distribuire una nuova cella di standby.

## Prerequisiti

- La cella primaria si trova nello stato non raggiungibile o non riuscito.
- Le due celle di standby si trovano nello stato in esecuzione.

Vedere [Visualizzazione dello stato delle celle in un cluster ad alta disponibilità del database](#).

## Procedura

- 1 Accedere come **root** all'interfaccia utente di gestione dell'appliance di una cella di standby in esecuzione, `https:// standby_ip_address:5480`.



- 2 Nella colonna **Ruolo** per la cella di standby che si desidera diventi la nuova cella primaria, fare clic su **Promuovi**.

La cella diventa la nuova cella primaria in stato di esecuzione. L'altra cella di standby sta seguendo la cella primaria appena promossa.

- 3 Distribuire una nuova appliance di standby.

#### Operazioni successive

- 1 Rimuovere l'appliance primaria non riuscita dal gruppo di server vCloud Director e dal cluster a disponibilità elevata di repmgr. Vedere [Eliminazione di una cella cloud](#) e [Annullamento della registrazione di una cella primaria non riuscita in un cluster a disponibilità elevata del database](#).
- 2 Se necessario, eliminare l'appliance primaria non riuscita.

## Backup e ripristino del database integrato dell'appliance vCloud Director

È possibile eseguire il backup del database PostgreSQL integrato nell'appliance vCloud Director, che può aiutare a ripristinare l'ambiente vCloud Director dopo un errore.

### Backup del database incorporato dell'appliance vCloud Director

Se l'ambiente è composto da distribuzioni dell'appliance vCloud Director con database PostgreSQL incorporati, è possibile eseguire il backup del database vCloud Director dalla cella primaria. Il file .tgz risultante viene archiviato nel percorso di storage condiviso NFS del servizio di trasferimento.

#### Procedura

- 1 Accedere direttamente o con SSH alla cella primaria come **root**.
- 2 Passare a `/opt/vmware/appliance/bin`.
- 3 Eseguire il comando `create-db-backup`.

#### Risultati

Nello storage condiviso NFS del servizio di trasferimento, nella directory `vcloudapp.nfs_mount.VMware_vCloud_Director/pgdb-backup/`, è possibile visualizzare il file `db-backup-date_time_format.tgz` appena creato. Il file .tgz contiene il file di dump del database e i file `global.properties`, `responses.properties`, `certificates` e `proxycertificates` della cella primaria.

## Ripristino di un ambiente dell'appliance vCloud Director con una configurazione del database ad alta disponibilità

Se è stato eseguito il backup del database PostgreSQL incorporato di un ambiente dell'appliance vCloud Director con una configurazione del database HA, è possibile distribuire un nuovo cluster di appliance e ripristinare il database dell'appliance al suo interno.

Per ripristinare una distribuzione dell'appliance con una configurazione del database non HA, vedere [Ripristino di un ambiente dell'appliance vCloud Director senza configurare un database a disponibilità elevata](#).

Il flusso di lavoro di ripristino include tre fasi principali.

- Copia del file .tar di backup del database integrato dall'archivio NFS condiviso del servizio di trasferimento
- Ripristino del database nelle celle primaria e di standby del database integrato
- Distribuzione di tutte le celle dell'applicazione richieste.

### Prerequisiti

- Verificare di disporre di un file di backup .tar del database PostgreSQL integrato. Vedere [Backup del database incorporato dell'appliance vCloud Director](#).
- Distribuire una cella del database primario e due celle di database di standby. Vedere [Capitolo 6 Distribuzione dell'appliance vCloud Director](#).
- Se si desidera che il nuovo cluster di appliance utilizzi il server NFS dell'ambiente esistente, esportare una nuova directory nel server NFS come nuovo punto condiviso. Impossibile riutilizzare il punto di montaggio esistente.

### Procedura

- 1 Nelle celle primarie e di standby, accedere come **root** ed eseguire il comando per arrestare il servizio vCloud Director.

```
service vmware-vcd stop
```

- 2 Nelle celle primarie e di standby, copiare il file .tar di backup nella cartella /tmp.

Se nella cartella /tmp non è disponibile spazio sufficiente, utilizzare un'altra posizione per archiviare il file .tar.

- 3 Nelle celle primarie e di standby, decomprimere il file di backup in /tmp.

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

Nella cartella `/tmp` è possibile visualizzare i file `global.properties`, `responses.properties`, `certificates`, `proxycertificates` e `truststore` estratti, nonché il file di dump del database denominato `vcloud_date_time_format`.

---

**Nota** Il file `truststore` è disponibile solo per vCloud Director 9.7.0.1 e versioni successive.

---

- 4 Solo nella cella primaria, accedere come **root** alla console ed eseguire i comandi seguenti.
  - a Rilasciare il database `vcloud`.

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

- b Eseguire il comando `pg_restore`.

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

- 5 Nelle celle primarie e di standby, salvare una copia dei file di dati di configurazione, sostituirli e riconfigurare e avviare il servizio vCloud Director.
  - a Eseguire il backup di proprietà, certificati e file `truststore`.

I file `global.properties`, `responses.properties`, `certificates`, `proxycertificates` e `truststore` sono disponibili in `/opt/vmware/vcloud-director/etc/`.

---

**Nota** Il file `truststore` è disponibile solo per vCloud Director 9.7.0.1 e versioni successive.

---

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

- b Copiare e sostituire le proprietà, i certificati e i file `truststore` dai file di backup estratti al [passaggio 3](#).

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

---

**Nota** Il file `truststore` è disponibile solo per vCloud Director 9.7.0.1 e versioni successive.

---

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

- c Eseguire il backup del file dell'archivio chiavi che si trova in `/opt/vmware/vcloud-director/certificates.ks`.

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

- d Eseguire il comando per riconfigurare il servizio vCloud Director.

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

Dove:

- L'opzione `--keystore-password` corrisponde alla password dell'archivio chiavi per i certificati nell'appliance.
- L'opzione `--database-password` corrisponde alla password del database impostata durante la distribuzione dell'appliance.
- L'opzione `--database-host` corrisponde all'indirizzo IP di rete eth1 dell'appliance di database primaria.
- Il valore `--primary-ip` corrisponde all'indirizzo IP di rete eth0 della cella dell'appliance che si sta ripristinando. Questo non è l'indirizzo IP della cella del database primario.
- L'opzione `--console-proxy-ip` corrisponde all'indirizzo IP di rete eth0 dell'appliance che si sta ripristinando.

Per informazioni sulla risoluzione dei problemi, vedere [La riconfigurazione del servizio vCloud Director non riesce durante la migrazione o il ripristino dell'appliance vCloud Director](#).

- e Eseguire il comando per avviare il servizio vCloud Director.

```
service vmware-vcd start
```

È possibile monitorare l'avanzamento dell'avvio della cella in `/opt/vmware/vcloud-director/logs/cell.log`.

- 6 (Facoltativo) Distribuire tutte le celle dell'applicazione aggiuntive. Vedere [Capitolo 6 Distribuzione dell'appliance vCloud Director](#).
- 7 Dopo aver completato il processo di avvio di tutte le celle del gruppo di server, verificare che il ripristino dell'ambiente vCloud Director sia stato eseguito correttamente.
  - a Aprire vCloud Director Web Console utilizzando l'indirizzo IP di rete eth0 di una cella del nuovo gruppo di server, `https://et0_IP_new_cell/cloud`.
  - b Accedere a vCloud Director Web Console con le credenziali dell'**amministratore di sistema** esistenti.
  - c Verificare che le risorse vSphere e cloud siano disponibili nel nuovo ambiente.

- 8 Dopo aver eseguito correttamente la verifica del ripristino del database, utilizzare vCloud Director Web Console per eliminare le celle disconnesse che appartengono all'ambiente vCloud Director precedente.
  - a Nella scheda **Gestisci e monitora**, fare clic su **Celle cloud**.
  - b Fare clic con il pulsante destro del mouse sul nome di una cella e scegliere **Elimina**.

## Ripristino di un ambiente dell'appliance vCloud Director senza configurare un database a disponibilità elevata

Se è stato eseguito il backup del database PostgreSQL incorporato di un ambiente dell'appliance vCloud Director con una configurazione del database non HA, è possibile distribuire un nuovo cluster di appliance e ripristinare il database dell'appliance al suo interno.

Per ripristinare una distribuzione dell'appliance con una configurazione del database HA, vedere [Ripristino di un ambiente dell'appliance vCloud Director con una configurazione del database ad alta disponibilità](#).

Il flusso di lavoro di ripristino include tre fasi principali.

- Copia del file .tar di backup del database integrato dall'archivio NFS condiviso del servizio di trasferimento
- Ripristino del database nella cella primaria del database integrato.
- Distribuzione di tutte le celle dell'applicazione richieste.

### Prerequisiti

- Verificare di disporre di un file di backup .tar del database PostgreSQL integrato. Vedere [Backup del database incorporato dell'appliance vCloud Director](#).
- Distribuire una cella del database primaria. Vedere [Capitolo 6 Distribuzione dell'appliance vCloud Director](#).
- Se si desidera che il nuovo cluster di appliance utilizzi il server NFS dell'ambiente esistente, esportare una nuova directory nel server NFS come nuovo punto condiviso. Impossibile riutilizzare il punto di montaggio esistente.

### Procedura

- 1 Nella cella primaria, accedere come **root** alla console ed eseguire il comando per arrestare il servizio vCloud Director.

```
service vmware-vcd stop
```

- 2 Copiare il file di backup .tar nella cartella /tmp

Se nella cartella /tmp non è disponibile spazio sufficiente, utilizzare un'altra posizione per archiviare il file .tar.

## 3 Decomprimere il file di backup in /tmp.

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

Nella cartella /tmp è possibile visualizzare i file `global.properties`, `responses.properties`, `certificates`, `proxycertificates` e `truststore` estratti, nonché il file di dump del database denominato `vcloud-date_time_format`.

---

**Nota** Il file `truststore` è disponibile solo per vCloud Director 9.7.0.1 e versioni successive.

---

## 4 Eseguire i comandi per rilasciare il database e ripristinarlo nella nuova appliance.

## a Rilasciare il database vcloud.

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

b Eseguire il comando `pg_restore`.

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

## 5 Nella cella primaria, salvare una copia dei file di dati di configurazione, sostituirli, nonché riconfigurare e avviare il servizio vCloud Director.

a Eseguire il backup di proprietà, certificati e file `truststore`.

I file `global.properties`, `responses.properties`, `certificates`, `proxycertificates` e `truststore` sono disponibili in `/opt/vmware/vcloud-director/etc/`.

---

**Nota** Il file `truststore` è disponibile solo per vCloud Director 9.7.0.1 e versioni successive.

---

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

b Copiare e sostituire le proprietà, i certificati e i file `truststore` dai file di backup estratti al [passaggio 3](#).

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

---

**Nota** Il file `truststore` è disponibile solo per vCloud Director 9.7.0.1 e versioni successive.

---

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

- c Eseguire il backup del file dell'archivio chiavi che si trova in `/opt/vmware/vcloud-director/certificates.ks`.

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

- d Eseguire il comando per riconfigurare il servizio vCloud Director.

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

Dove:

- L'opzione `--keystore-password` corrisponde alla password dell'archivio chiavi per i certificati nell'appliance.
- L'opzione `--database-password` corrisponde alla password del database impostata durante la distribuzione dell'appliance.
- L'opzione `--database-host` corrisponde all'indirizzo IP di rete eth1 dell'appliance di database primaria.
- Il valore `--primary-ip` corrisponde all'indirizzo IP di rete eth0 della cella dell'appliance che si sta ripristinando. Questo non è l'indirizzo IP della cella del database primario.
- L'opzione `--console-proxy-ip` corrisponde all'indirizzo IP di rete eth0 dell'appliance che si sta ripristinando.

Per informazioni sulla risoluzione dei problemi, vedere [La riconfigurazione del servizio vCloud Director non riesce durante la migrazione o il ripristino dell'appliance vCloud Director](#).

- e Eseguire il comando per avviare il servizio vCloud Director.

```
service vmware-vcd start
```

È possibile monitorare l'avanzamento dell'avvio della cella in `/opt/vmware/vcloud-director/logs/cell.log`.

- 6 (Facoltativo) Distribuire tutte le celle dell'applicazione aggiuntive. Vedere [Capitolo 6 Distribuzione dell'appliance vCloud Director](#).

- 7 Dopo aver completato il processo di avvio di tutte le celle del gruppo di server, verificare che il ripristino dell'ambiente vCloud Director sia stato eseguito correttamente.
  - a Aprire vCloud Director Web Console utilizzando l'indirizzo IP di rete eth0 di una cella del nuovo gruppo di server, `https://eth0_IP_new_cell/cloud`.
  - b Accedere a vCloud Director Web Console con le credenziali dell'**amministratore di sistema** esistenti.
  - c Verificare che le risorse vSphere e cloud siano disponibili nel nuovo ambiente.
- 8 Dopo aver eseguito correttamente la verifica del ripristino del database, utilizzare vCloud Director Web Console per eliminare le celle disconnesse che appartengono all'ambiente vCloud Director precedente.
  - a Nella scheda **Gestisci e monitora**, fare clic su **Celle cloud**.
  - b Fare clic con il pulsante destro del mouse sul nome di una cella e scegliere **Elimina**.

## Configurazione dell'accesso esterno al database di vCloud Director

È possibile abilitare l'accesso da determinati indirizzi IP esterni al database di vCloud Director incorporato nell'appliance primaria.

Durante una migrazione all'appliance vCloud Director o se si intende utilizzare una soluzione di backup del database di terze parti, è possibile abilitare l'accesso esterno al database di vCloud Director incorporato.

### Procedura

- 1 Accedere direttamente o con SSH alla cella primaria come **root**.
- 2 Passare alla directory del database, `/opt/vmware/appliance/etc/pg_hba.d/`.
- 3 Creare un file di testo contenente le voci per gli indirizzi IP esterni di destinazione simili a:

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

Ad esempio:

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

Le voci vengono aggiunte al file `pg_hba.conf` aggiornato dinamicamente, che controlla l'accesso al database primario nel cluster a disponibilità elevata.



## Abilitazione o disabilitazione dell'accesso SSH all'appliance di vCloud Director

Durante la distribuzione dell'appliance, è possibile lasciare disabilitato o abilitare l'accesso SSH all'appliance. Dopo la distribuzione, è possibile cambiare l'impostazione di accesso SSH.

Il daemon SSH viene eseguito nell'appliance per essere utilizzato dalla funzione HA del database e per gli accessi **root** remoti. È possibile disabilitare l'accesso SSH per l'utente **root**. L'accesso SSH per la funzione HA del database rimane invariato.

### Procedura

- 1 Se si desidera apportare modifiche temporanee alla proprietà OVF, ad esempio a scopo di test, modificare la proprietà in vCloud Director.
  - a Accedere alla console dell'appliance vCloud Director come **root** direttamente o utilizzando un client SSH.
  - b Eseguire lo script per abilitare o disabilitare l'accesso **root** SSH.
    - Per abilitare l'accesso **root** SSH, eseguire lo script `/opt/vmware/appliance/bin/enable_root_login.sh`.
    - Per disabilitare l'accesso **root** SSH, eseguire lo script `/opt/vmware/appliance/bin/disable_root_login.sh`.
- 2 Se si desidera apportare modifiche permanenti alla proprietà OVF, utilizzare l'interfaccia utente di vSphere per impostare il valore della proprietà `vcloudapp.enable_ssh.VMware_vCloud_Director`.

---

**Nota** È necessario spegnere la macchina virtuale per modificare il valore della proprietà in vSphere.

---

- Per abilitare SSH, impostare il valore di `vcloudapp.enable_ssh.VMware_vCloud_Director` su **True**.
- Per disabilitare SSH, impostare il valore di `vcloudapp.enable_ssh.VMware_vCloud_Director` su **False**.

## Modifica delle impostazioni DNS dell'appliance vCloud Director

Dopo la distribuzione, è possibile modificare il server o i server DNS dell'appliance vCloud Director.

---

**Importante** Non è possibile modificare il nome host dell'appliance. È necessario distribuire una nuova appliance con il nome host desiderato.

---

## Procedura

- 1 Se si desidera modificare temporaneamente le impostazioni DNS, ad esempio a scopo di test, modificare le impostazioni DNS in vCloud Director.

- a Accedere alla console dell'appliance vCloud Director come **root** direttamente o utilizzando un client SSH.
- b (Facoltativo) Verificare la configurazione DNS corrente eseguendo il comando seguente:

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

- c Modificare il server o i server DNS.

Per specificare più server DNS, impostare *DNS\_server\_IP* come elenco separato da virgole senza spazi.

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

- d Affinché le modifiche abbiano effetto, riavviare il servizio VAOS.

```
systemctl restart vaos.service
```

- 2 Se si desidera modificare le impostazioni DNS in modo permanente, utilizzare l'interfaccia utente di vSphere per impostare il valore della proprietà *vami.DNS.VMware\_vCloud\_Director* sul nuovo indirizzo IP del server DNS.

Per specificare più server DNS, immettere un elenco separato da virgole senza spazi.

---

**Nota** È necessario spegnere la macchina virtuale per modificare il valore della proprietà in vSphere.

---

## Modifica delle route statiche per le interfacce di rete dell'appliance vCloud Director

Dopo la distribuzione di vCloud Director iniziale, è possibile modificare le route statiche per le interfacce di rete *eth0* e *eth1*.

## Procedura

- 1 Se si desidera modificare temporaneamente il valore della route statica, ad esempio a scopo di test, modificare le route statiche in vCloud Director.

- a Accedere alla console dell'appliance vCloud Director come **root** direttamente o utilizzando un client SSH.
- b (Facoltativo) Verificare la configurazione della route statica corrente.

- Per eth0, eseguire il comando seguente.

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

- Per eth1, eseguire il comando seguente.

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

- c Modificare il valore della route statica.

Le route statiche devono trovarsi in un elenco di specifiche delle route separate da virgole. Ad esempio, per eth0 è necessario eseguire:

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

- Per eth0, eseguire il comando seguente.

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

- Per eth1, eseguire il comando seguente.

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

- d Riavviare il servizio di rete nell'appliance vCloud Director.

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

- 2 Se si desidera modificare il valore della route statica in modo permanente, modificare la proprietà OVF utilizzando l'interfaccia utente di vSphere.

Le route statiche devono trovarsi in un elenco di specifiche delle route separate da virgole.

---

**Nota** È necessario spegnere la macchina virtuale per modificare il valore della proprietà in vSphere.

---

- Utilizzare l'interfaccia utente di vSphere per impostare il valore della proprietà `vcloudnet.routes0.VMware_vCloud_Director` sulla nuova stringa di specifica della route.
- Utilizzare l'interfaccia utente di vSphere per impostare il valore della proprietà `vcloudnet.routes1.VMware_vCloud_Director` sulla nuova stringa di specifica della route.

## Script di configurazione nell'appliance vCloud Director

L'appliance vCloud Director contiene script di configurazione specifici.

Directory	Descrizione
/opt/vmware/appliance/bin/	Gli script di configurazione dell'appliance.
/opt/vmware/appliance/etc/	I file di configurazione dell'appliance.
/opt/vmware/appliance/etc/pg_hba.d/	La directory in cui è possibile aggiungere voci personalizzate al file pg_hba.conf. Vedere <a href="#">Configurazione dell'accesso esterno al database di vCloud Director</a> .

## Modifica delle configurazioni di PostgreSQL nell'appliance di vCloud Director

È possibile modificare le configurazioni di PostgreSQL dell'appliance di vCloud Director utilizzando il comando `ALTER SYSTEM` di PostgreSQL.

Il comando `ALTER SYSTEM` scrive le modifiche delle impostazioni dei parametri nel file `postgresql.auto.conf`, che ha la precedenza sul file `postgresql.conf` durante l'inizializzazione di PostgreSQL. Alcune impostazioni richiedono un riavvio del servizio PostgreSQL, mentre altre vengono configurate dinamicamente e non richiedono un riavvio. Non modificare il file `postgresql.conf` perché le modifiche non vengono mantenute dopo il riavvio.

### Procedura

- 1 Accedere direttamente o tramite un client SSH al sistema operativo dell'appliance primaria come **root**.
- 2 Sostituire l'utente con **postgres**.

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

- 3 Utilizzare il comando `ALTER SYSTEM` di PostgreSQL per modificare un parametro.

```
psql -c "ALTER SYSTEM set parameter='value';"
```

- 4 Ripetere [Passaggio 3](#) per ogni parametro di configurazione che si desidera modificare.
- 5 Se alcuni dei parametri che si desidera modificare richiedono un riavvio del servizio PostgreSQL, riavviare il processo `vpostgres`.

```
systemctl restart vpostgres
```

- 6 Se l'ambiente include nodi di standby, copiare il file `postgresql.auto.conf` nelle appliance di standby e riavviare il servizio PostgreSQL, se necessario.

- a Copiare il file `postgresql.auto.conf` dal nodo primario a un nodo di standby.

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

- b Se per l'applicazione di alcuni dei parametri nel file `postgresql.auto.conf` copiato è necessario il riavvio, riavviare il processo `vpostgres` nel nodo di standby.

```
systemctl restart vpostgres
```

- c Ripetere [6.a](#) e [6.b](#) per ogni nodo di standby.

# Utilizzo di Replication Manager Tool Suite in una configurazione di cluster a disponibilità elevata

## 9

La suite di strumenti open source repmgr fa parte del database PostgreSQL incorporato dell'appliance vCloud Director. È possibile utilizzare repmgr per configurare, monitorare e controllare la replica PostgreSQL e il failover del database nel cluster a disponibilità elevata del database di vCloud Director.

È possibile utilizzare l'interfaccia della riga di comando di repmgr per controllare lo stato e gli eventi di un nodo o di un cluster, per registrare o annullare la registrazione di un nodo, per promuovere un nodo di standby, per scambiare i ruoli di un nodo primario e un nodo di standby oppure per seguire un nuovo nodo primario.

Per ulteriori informazioni sulla configurazione della disponibilità elevata del database di vCloud Director, vedere [Distribuzioni dell'appliance e configurazione della disponibilità elevata del database](#).

Per ulteriori informazioni su repmgr, visitare [repmgr.org](http://repmgr.org).

Questo capitolo include i seguenti argomenti:

- [Verifica dello stato di connettività di un cluster a disponibilità elevata del database](#)
- [Verifica dello stato di replica di un nodo in un cluster a disponibilità elevata del database](#)
- [Verifica dello stato di un cluster a disponibilità elevata del database](#)
- [Rilevamento di un precedente nodo primario che torna online in un cluster a disponibilità elevata](#)
- [Scambio dei ruoli tra cella primaria e cella di standby in un cluster a disponibilità elevata del database](#)
- [Annullamento della registrazione di un nodo di standby non riuscito o irraggiungibile in un cluster a disponibilità elevata del database](#)
- [Annullamento della registrazione di una cella primaria non riuscita in un cluster a disponibilità elevata del database](#)
- [Annullamento della registrazione di una cella di standby in esecuzione in un cluster a disponibilità elevata del database](#)

## Verifica dello stato di connettività di un cluster a disponibilità elevata del database

È possibile utilizzare Replication Manager Tool Suite per controllare la connettività tra i nodi nel cluster a disponibilità elevata del database.

### Procedura

- 1 Accedere o accedere tramite SSH come **root** al sistema operativo di tutte le celle in esecuzione nel cluster.

- 2 Sostituire l'utente con **postgres**.

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

- 3 Controllare la connettività del cluster.

- Il comando `repmgr cluster matrix` esegue il comando `repmgr cluster show` su ciascun nodo del cluster e presenta il risultato come matrice.

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

Nell'esempio seguente, il nodo 1 e il nodo 2 sono attivi e il nodo 3 è inattivo. Ogni riga corrisponde a un server e rappresenta il risultato della verifica di una connessione in uscita da tale server.

Le tre voci nella terza riga sono contrassegnate con un simbolo ?, perché il nodo 3 è inattivo e non sono disponibili informazioni sulle connessioni in uscita.

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	x
node 3	3	?	?	?

- Il comando `repmgr cluster crosscheck` esegue una verifica incrociata delle connessioni tra ciascuna combinazione di nodi e potrebbe fornire una panoramica migliore della connettività del cluster.

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

Nell'esempio seguente, il nodo da cui si esegue il comando `repmgr cluster crosscheck` unisce l'output del sistema della matrice del cluster con l'output degli altri nodi ed esegue una verifica incrociata tra i nodi. In questo caso, tutti i nodi sono attivi, ma il firewall elimina i pacchetti provenienti dal nodo 1 e diretti al nodo 3. Questo è un esempio di partizione di rete asimmetrica, in cui il nodo 1 non può inviare i pacchetti al nodo 3.

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	*
node 3	3	*	*	*

### Operazioni successive

Per determinare lo stato di connettività generale nel cluster a disponibilità elevata del database, eseguire questi comandi su ciascun nodo e confrontare i risultati.

## Verifica dello stato di replica di un nodo in un cluster a disponibilità elevata del database

È possibile utilizzare Replication Manager Tool Suite e il terminale interattivo PostgreSQL per verificare lo stato di replica dei singoli nodi in un cluster a disponibilità elevata del database.

### Procedura

- 1 Accedere o accedere tramite SSH come **root** al sistema operativo di tutti i nodi in esecuzione nel cluster.
- 2 Sostituire l'utente con **postgres**.

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

- 3 Controllare lo stato della replica del nodo.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf node status
```

L'output del sistema fornisce informazioni sul nodo, sulla versione di PostgreSQL e sui dettagli della replica.



- 4 (Facoltativo) Per informazioni più dettagliate, utilizzare il terminale interattivo PostgreSQL per verificare lo stato di replica dei nodi.

Il terminale interattivo PostgreSQL può fornire informazioni sulla possibilità che uno qualsiasi dei record del registro ricevuti dei nodi di standby sia in ritardo rispetto ai registri inviati dal nodo primario.

- a Connettersi al terminale `psql`

```
/opt/vmware/vpostgres/current/bin/psql
```

- b Per espandere la visualizzazione e rendere più semplice la lettura dei risultati delle query, eseguire il comando `set \x`.
- c Eseguire una query sullo stato della replica in base al ruolo del nodo.

Opzione	Azione
Eseguire una query sul nodo primario.	<code>/opt/vmware/vpostgres/current/bin/psql</code>
Eseguire una query su un nodo di standby.	<code>select * from pg_stat_wal_receiver;</code>

## Verifica dello stato di un cluster a disponibilità elevata del database

Per risolvere i problemi relativi al cluster a disponibilità elevata del database, è necessario monitorare lo stato dei nodi e gli eventi nel cluster.

### Procedura

- 1 Accedere o accedere tramite SSH come **root** al sistema operativo di tutte le celle in esecuzione nel cluster.
- 2 Sostituire l'utente con **postgres**.

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

- 3 Controllare lo stato del cluster.

La colonna **Upstream** indica il nodo primario corrente.

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

Nell'output della console vengono visualizzate le informazioni sul cluster. Nell'esempio seguente, il nodo primario nel cluster, il nodo 3, non è raggiungibile.

```

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

```

```

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

```

Nel seguente esempio di output di sistema, node 3 è il nodo primario in un cluster in esecuzione integro.

```

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

```

#### 4 Controllare il registro eventi del cluster.

```

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

```

L'output del sistema mostra gli eventi di creazione, clonazione e registrazione nel cluster.

#### Operazioni successive

Se lo stato del nodo primario è non raggiungibile o non riuscito, è necessario promuovere un nodo di standby.

Se lo stato di un nodo di standby è non raggiungibile o non riuscito, riparare il nodo e avviare il servizio PostgreSQL se non è in esecuzione.

## Rilevamento di un precedente nodo primario che torna online in un cluster a disponibilità elevata

Se un nodo primario nel cluster non riesce e successivamente torna online quando si promuove un nodo di standby come nuovo nodo primario, si verificano imprecisioni nei dati repmgr. È possibile individuare le irregolarità con il comando `repmgr cluster show`.

### Esempio: Esecuzione di `repmgr cluster show` nel nodo primario precedente

Nell'esempio seguente, l'esecuzione del comando `repmgr cluster show` in un nodo primario precedente che torna online comporta il seguente output di sistema.

```

      ID | Name      | Role   | Status           | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Node1 name| standby | !running as primary| Node 3 name| default  | host=host IP address

```

```

user=repmgr dbname=repmgr
Node 2 | Node2 name| standby |      running      | Node 3 name| default | host=host IP address
user=repmgr dbname=repmgr
Node 3 | Node3 name| primary | * running      |           | default | host=host IP address
user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is registered as standby but running as primary

```

Nell'esempio, node 1 è il nodo primario corrente nel cluster.

Quando si esegue il comando `repmgr cluster show`, se si ottiene lo stato `!running as primary` per un nodo di standby significa che un nodo primario precedente è in esecuzione nel cluster. In questo caso, è necessario arrestare il nodo primario precedente e annullarne la registrazione.

## Esempio: Esecuzione di `repmgr cluster show` nel nuovo nodo primario

Nell'esempio seguente, l'esecuzione del comando `repmgr cluster show` nel nuovo nodo primario comporta il seguente output di sistema.

```

ID | Name | Role | Status | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Node1 name| primary | * running |           | default | host=host IP address user=repmgr
dbname=repmgr
Node 2 | Node2 name| standby | running | Node1 name | default | host=host IP address user=repmgr
dbname=repmgr
Node 3 | Node3 name| primary | ! running |           | default | host=host IP address user=repmgr
dbname=repmgr
WARNING: following issues were detected
- node 3(ID: Node 3) is running but the repmgr node record is inactive

```

In questo caso, i dati `repmgr` sono corretti. Indica con precisione che node 1 è in esecuzione e che è il nodo primario corrente. Il messaggio di avviso relativo a node 3, il nodo primario precedente, indica che i dati `repmgr` in tale nodo non sono esatti.

## Esempio: Esecuzione di `repmgr cluster show` dopo la promozione di un nodo di standby, senza l'esecuzione di `standby follow` nei restanti nodi di standby

Nell'esempio seguente, è possibile visualizzare i dati `repmgr` in ciascun nodo in un cluster in cui il nodo primario non è riuscito. Un nodo di standby è stato promosso manualmente utilizzando il comando `repmgr standby promote`, ma senza l'esecuzione di `repmgr standby follow` nei restanti nodi di standby.

Quando si esegue `repmgr cluster show` nel nuovo nodo primario, l'output del sistema rappresenta i dati `repmgr` corretti, ma il nuovo nodo primario, node 2, non è seguito da alcun nodo di standby.

```

ID | Name | Role | Status | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Node1 name| primary | * running |           | default | host=host IP address user=repmgr
dbname=repmgr

```

```

Node 2 |Node2 name| primary | ! running |          | default | host=host IP address user=repmgr
dbname=repmgr
Node 3 |Node3 name| standby |   running |Node 1 name | default | host=host IP address user=repmgr
dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is running but the repmgr node record is inactive

```

Sia node 1, ovvero il nodo primario precedente, sia node 3, ovvero il nodo di standby che segue il nodo primario precedente, forniscono dati repmgr imprecisi.

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	Node1 name	primary	* running		default	host=host IP address user=repmgr dbname=repmgr
Node 2	Node2 name	standby	! running as primary	Node1 name	default	host=host IP address user=repmgr dbname=repmgr
Node 3	Node3 name	standby	running	Node1 name	default	host=host IP address user=repmgr dbname=repmgr

```

WARNING: following issues were detected
- node 2(ID: Node 2) is registered as standby but running as primary

```

## Esempio: Esecuzione di repmgr cluster show in un nodo di standby

L'esecuzione del comando in un nodo di standby che segue il nodo primario corrente comporta un output di sistema con dati di repmgr precisi identici ai dati nel nodo primario corrente.

L'esecuzione del comando in un nodo di standby che segue il nodo primario precedente genera un output di sistema con dati imprecisi repmgr identici ai dati nel nodo primario precedente.

## Voci di registro

Se un nodo primario precedente che non è riuscito torna online dopo aver promosso un nodo di standby come nuovo nodo primario, le seguenti voci vengono visualizzate nel file `update-repmgr-data.log` in tutti i nodi con dati repmgr imprecisi.

```

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

```

## Scambio dei ruoli tra cella primaria e cella di standby in un cluster a disponibilità elevata del database

È possibile utilizzare un comando repmgr per scambiare i ruoli del nodo primario e di uno dei nodi di standby nel cluster a disponibilità elevata del database durante una manutenzione pianificata.

### Prerequisiti

- Attivare la modalità di manutenzione per tutte le celle di vCloud Director che fanno parte del cluster a disponibilità elevata.

- Verificare che tutti i nodi nel cluster siano integri e online.

#### Procedura

- 1 Accedere o accedere tramite SSH come **root** al sistema operativo del nodo di standby che si desidera promuovere.

- 2 Sostituire l'utente con **postgres**.

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

- 3 (Facoltativo) Verificare che i prerequisiti per lo switchover vengano soddisfatti eseguendo il comando con l'opzione **--dry-run**.

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

- 4 Scambiare i ruoli della cella primaria e della cella di standby.

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

#### Risultati

L'ultima riga dell'output della console indica che lo switchover di standby è stato completato correttamente.

#### Operazioni successive

- 1 Eseguire il comando **reconfigure-database** per aggiornare l'indirizzo IP del database in tutte le celle di vCloud Director. Vedere [Aggiornamento degli indirizzi IP del database nelle celle di vCloud Director](#).
- 2 Quando si riconfigurano le celle di vCloud Director nel gruppo di server in modo che puntino al nuovo database primario, disattivare la modalità di manutenzione per tutte le celle di vCloud Director che fanno parte del cluster a disponibilità elevata.

## Annullamento della registrazione di un nodo di standby non riuscito o irraggiungibile in un cluster a disponibilità elevata del database

È possibile utilizzare repmgr in un nodo in esecuzione nel cluster per annullare la registrazione di un nodo di standby non riuscito o irraggiungibile.

---

**Nota** Affinché il nodo primario funzioni normalmente, almeno un nodo di standby deve essere sempre in esecuzione.

---

## Prerequisiti

Per annullare la registrazione di un nodo di standby non in esecuzione, è necessario fornire l'ID del nodo. Per trovare l'indirizzo IP, controllare lo stato del cluster e individuare il nodo. In tale riga, utilizzare il valore dell'host della colonna Stringa di connessione per identificare l'indirizzo IP del nodo. Vedere [Verifica dello stato di un cluster a disponibilità elevata del database](#).

## Procedura

- 1 Accedere o accedere tramite SSH come **root** al sistema operativo di uno dei nodi in esecuzione del cluster.
- 2 Sostituire l'utente con **postgres**.

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

- 3 Annullare la registrazione del nodo non riuscito o non raggiungibile.

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

## Risultati

Se si annulla la registrazione del nodo, le informazioni relative al nodo vengono rimosse dai metadati di repmgr.

# Annullamento della registrazione di una cella primaria non riuscita in un cluster a disponibilità elevata del database

Se il nodo primario nel cluster a disponibilità elevata del database non riesce e si promuove un nuovo nodo primario, è necessario annullare la registrazione del nodo primario non riuscito per rimuoverlo dal cluster ed evitare incoerenze nei dati di stato del cluster.

## Prerequisiti

- Per annullare la registrazione di un nodo primario non in esecuzione, è necessario fornire l'ID del nodo. Per trovare l'indirizzo IP, controllare lo stato del cluster e individuare il nodo. In tale riga, utilizzare il valore dell'host della colonna Stringa di connessione per identificare l'indirizzo IP del nodo. Vedere [Verifica dello stato di un cluster a disponibilità elevata del database](#).
- Verificare che il nodo primario non riuscito sia inattivo e privo di nodi di standby successivi e promuovere un nuovo nodo primario.

## Procedura

- 1 Accedere o accedere tramite SSH come **root** al sistema operativo di tutti i nodi in esecuzione nel cluster.

## 2 Sostituire l'utente con **postgres**.

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

- 3 (Facoltativo) Per verificare che i prerequisiti per annullare la registrazione del nodo siano soddisfatti, eseguire il comando con l'opzione `--dry-run`.

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

- 4 Annullare la registrazione del nodo.

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

### Risultati

L'operazione rimuove il nodo dai metadati di repmgr.

## Annullamento della registrazione di una cella di standby in esecuzione in un cluster a disponibilità elevata del database

Se si desidera utilizzare un nodo in un altro ruolo o rimuoverlo dal cluster a disponibilità elevata, è necessario annullarne la registrazione.

È possibile eseguire questo comando durante il normale funzionamento del sistema.

---

**Nota** Affinché il nodo primario funzioni normalmente, almeno un nodo di standby deve essere sempre in esecuzione.

---

### Prerequisiti

Per annullare la registrazione di un nodo di standby, è necessario fornire l'ID del nodo. Per trovare l'indirizzo IP, controllare lo stato del cluster e individuare il nodo. In tale riga, utilizzare il valore dell'host della colonna Stringa di connessione per identificare l'indirizzo IP del nodo. Vedere [Verifica dello stato di un cluster a disponibilità elevata del database](#).

### Procedura

- 1 Accedere o accedere tramite SSH come **root** al sistema operativo di tutti i nodi in esecuzione nel cluster.
- 2 Sostituire l'utente con **postgres**.

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

- 3 Annullare la registrazione del nodo.

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

## **Risultati**

Se si annulla la registrazione del nodo, il record del nodo di standby viene rimosso dalla tabella dei metadati interna della suite di strumenti repmgr.



# Dopo avere installato vCloud Director o distribuito l'appliance vCloud Director

# 10

Dopo aver creato il gruppo di server vCloud Director, è possibile installare i file Microsoft Sysprep e il database Cassandra. Se si utilizza un database PostgreSQL, è possibile configurare il protocollo SSL e regolare alcuni parametri nel database.

Questo capitolo include i seguenti argomenti:

- [Installazione dei file Microsoft Sysprep nei server](#)
- [Personalizzazione degli endpoint pubblici](#)
- [Installazione e configurazione di un broker AMQP RabbitMQ](#)
- [Installazione e configurazione di un database Cassandra per l'archiviazione dei dati relativi alle metriche cronologiche](#)
- [Esecuzione di configurazioni aggiuntive nel database PostgreSQL esterno](#)

## Installazione dei file Microsoft Sysprep nei server

Se il cloud richiede il supporto della personalizzazione del guest per alcuni sistemi operativi Microsoft obsoleti, è necessario installare i file di Microsoft Sysprep appropriati in ogni membro del gruppo di server.

I file Sysprep sono richiesti soltanto per alcuni sistemi operativi Microsoft obsoleti. Se il cloud in uso non necessita di supportare la personalizzazione guest per tali sistemi operativi, non sarà necessario installare i file Sysprep.

Per installare i file binari Sysprep, copiarli in una posizione specifica nel server. Occorre copiare i file in ciascun membro del gruppo di server.

### Prerequisiti

Verificare di disporre dell'accesso a file binari Sysprep a 32 e 64 bit per Windows 2003 e Windows XP.

### Procedura

- 1 Eseguire il login al server di destinazione come utente **root**.

- 2 Modificare la directory in `$VCLLOUD_HOME/guestcustomization/default/windows`.

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

- 3 Creare una directory denominata `sysprep`.

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

- 4 Per ogni sistema operativo guest che richiede file binari Sysprep, creare una sottodirectory di `$VCLLOUD_HOME/guestcustomization/default/windows/sysprep`.

I nomi delle sottodirectory sono specifici per un sistema operativo guest.

**Tabella 10-1. Assegnazioni di sottodirectory per file Sysprep**

Sistema operativo guest	Sottodirectory da creare in <code>\$VCLLOUD_HOME/guestcustomization/default/windows/sysprep</code>
Windows 2003 (a 32 bit)	svr2003
Windows 2003 (a 64 bit)	svr2003-64
Windows XP (a 32 bit)	xp
Windows XP (a 64 bit)	xp-64

Ad esempio, per creare una sottodirectory per mantenere i file binari Sysprep per Windows XP, utilizzare il seguente comando Linux.

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

- 5 Copiare il file binario Sysprep nella posizione appropriata su ciascun server vCloud Director nel gruppo di server.
- 6 Verificare che i file Sysprep siano leggibili dall'utente `vcld:vcld`.

A tal fine, utilizzare il comando `chown` di Linux.

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

## Risultati

Quando i file Sysprep vengono copiati in tutti i membri del gruppo di server, è possibile confermare la personalizzazione guest nelle macchine virtuali presenti nel cloud in uso. Dopo avere copiato i file Sysprep, non è necessario riavviare vCloud Director.

## Personalizzazione degli endpoint pubblici

Per soddisfare i requisiti del bilanciamento del carico o del proxy, è possibile modificare gli indirizzi Web degli endpoint predefiniti per la console Web di vCloud Director, l'API di vCloud, il portale tenant e il proxy della console.

Se è stata distribuita l'appliance vCloud Director, è necessario configurare l'indirizzo del proxy della console pubblica di vCloud Director, perché l'appliance utilizza un singolo indirizzo IP con la porta personalizzata 8443 per il servizio proxy della console. Vedere il [passaggio 5](#).

## Prerequisiti

Solo l'**amministratore di sistema** può personalizzare gli endpoint pubblici.

## Procedura

**1** Fare clic sulla scheda **Amministrazione** e, nel riquadro a sinistra, fare clic su **Indirizzi pubblici**.

**2** Selezionare **Personalizza endpoint pubblici**.

Se si deseleziona questa casella di controllo, per tutti gli endpoint vengono ripristinati i valori predefiniti, che non sono visualizzati nella pagina.

**3** Per personalizzare l'API REST di vCloud e gli URL di OpenAPI, modificare gli endpoint dell'**API**.

a Immettere un URL di base HTTP personalizzato.

Ad esempio, se si imposta l'URL di base HTTP su **http://vcloud.example.com**, è possibile accedere all'API di vCloud all'indirizzo `http://vcloud.example.com/api` ed è possibile accedere all'OpenAPI di vCloud all'indirizzo `http://vcloud.example.com/cloudapi`.

b Immettere un URL di base dell'API REST HTTPS personalizzato e fare clic su **Sfoglia** per caricare i certificati che stabiliscono la catena di attendibilità per l'endpoint.

Ad esempio, se si imposta l'URL di base dell'API REST HTTPS su **https://vcloud.example.com**, è possibile accedere all'API di vCloud all'indirizzo `https://vcloud.example.com/api` ed è possibile accedere all'OpenAPI di vCloud all'indirizzo `https://vcloud.example.com/cloudapi`.

La catena di certificati deve corrispondere al certificato utilizzato dall'endpoint del servizio, che è il certificato caricato in ogni archivio chiavi di cella di vCloud Director con alias `http` o il certificato VIP del bilanciamento del carico se viene utilizzata una terminazione SSL. La catena di certificati deve includere un certificato di endpoint, certificati intermedi e un certificato root nel formato PEM senza una chiave privata.

**4** Per personalizzare gli URL del portale tenant di vCloud Director, modificare gli endpoint del **portale tenant**.

■ Per configurare il portale tenant di vCloud Director in modo che utilizzi gli stessi endpoint e la catena di certificati specificati nel [Passaggio passaggio 3](#), selezionare **Copia impostazioni URL API**.

■ Per configurare il portale tenant di vCloud Director in modo che utilizzi endpoint e una catena di certificati differenti, eseguire i passaggi seguenti.

a Deselezionare **Copia impostazioni URL API**.

b Immettere un URL di base HTTP personalizzato.

Ad esempio, se si imposta l'URL di base HTTP su **http://vcloud.example.com**, è possibile accedere al portale tenant all'indirizzo **http://vcloud.example.com/tenant/org\_name**.

- c Immettere un URL di base dell'API REST HTTPS personalizzato e fare clic su **Sfoglia** per caricare i certificati che stabiliscono la catena di attendibilità per l'endpoint.

Ad esempio, se si imposta l'URL di base dell'API REST HTTPS su **https://vcloud.example.com**, è possibile accedere al portale tenant all'indirizzo **https://vcloud.example.com/tenant/org\_name**.

La catena di certificati deve corrispondere al certificato utilizzato dall'endpoint del servizio, che è il certificato caricato in ogni archivio chiavi di cella di vCloud Director con alias **http** o il certificato VIP del bilanciamento del carico se viene utilizzata una terminazione SSL. La catena di certificati deve includere un certificato di endpoint, certificati intermedi e un certificato root nel formato PEM senza una chiave privata.

**5** Per personalizzare gli URL di vCloud Director Web Console e l'indirizzo del proxy della console, modificare gli endpoint della **console Web**.

- a Immettere un URL pubblico di vCloud Director personalizzato per le connessioni HTTP.

L'URL deve includere `/cloud`.

Ad esempio, se si imposta l'URL pubblico di vCloud Director su

**`http://vcloud.example.com/cloud`**, è possibile accedere alla vCloud Director Web Console all'indirizzo `http://vcloud.example.com/cloud`.

- b Immettere un URL dell'API REST personalizzato per le connessioni HTTPS e fare clic su **Sfoglia** per caricare i certificati che stabiliscono la catena di attendibilità per l'endpoint.

L'URL deve includere `/cloud`.

Ad esempio, se si imposta l'URL di base su **`https://vcloud.example.com`**, è possibile accedere alla vCloud Director Web Console all'indirizzo `https://vcloud.example.com/cloud`.

La catena di certificati deve corrispondere al certificato utilizzato dall'endpoint del servizio, che è il certificato caricato in ogni archivio chiavi della cella di vCloud Director con alias **HTTP** o il certificato VIP del bilanciamento del carico se viene utilizzata una terminazione SSL. La catena di certificati deve includere un certificato di endpoint, certificati intermedi e un certificato root nel formato PEM senza una chiave privata.

- c Immettere un indirizzo proxy della console pubblica di vCloud Director personalizzato.

Questo indirizzo è il nome di dominio completo del server vCloud Director o del bilanciamento del carico con il numero di porta. La porta predefinita è 443.

---

**Importante** L'appliance vCloud Director utilizza la sua NIC `eth0` con la porta personalizzata 8443 per il servizio proxy della console.

---

La terminazione SSL delle connessioni del proxy della console in un bilanciamento del carico non è supportata. Il certificato del proxy della console viene caricato in ogni archivio chiavi della cella di vCloud Director con alias **consoleproxy**.

Ad esempio, per l'istanza di un'appliance vCloud Director con nome di dominio completo `vcloud.example.com`, immettere **`vcloud.example.com:8443`**.

La console Web di vCloud Director utilizza l'indirizzo del proxy della console quando viene aperta una finestra di console remota in una macchina virtuale.

**6** Per salvare le modifiche, fare clic su **Applica**.

## Installazione e configurazione di un broker AMQP RabbitMQ

AMQP (Advanced Message Queuing Protocol) è uno standard aperto per l'accodamento dei messaggi che supporta servizi di messaggistica flessibili per i sistemi aziendali. vCloud Director utilizza il broker RabbitMQ AMQP per fornire il bus di messaggi utilizzato dai servizi di estensione, dalle estensioni degli oggetti e dalle notifiche.

## Procedura

- 1 Scaricare il server RabbitMQ da <https://www.rabbitmq.com/download.html>.

Per l'elenco delle release RabbitMQ supportate, vedere *Note di rilascio di vCloud Director*.

- 2 Seguire le istruzioni per l'installazione di RabbitMQ e installare RabbitMQ in un host supportato.

L'host del server RabbitMQ deve essere raggiungibile nella rete da ogni cella vCloud Director.

- 3 Durante l'installazione di RabbitMQ, prendere nota dei valori necessari per configurare vCloud Director in modo che funzioni con questa installazione di RabbitMQ.

- Nome di dominio completo dell'host del server RabbitMQ, ad esempio *amqp.esempio.com*.
- Nome utente e password validi per l'autenticazione in RabbitMQ.
- La porta alla quale il broker si mette in ascolto dei messaggi. La porta predefinita è 5672.
- L'host virtuale RabbitMQ. Il valore predefinito è "/".

## Operazioni successive

Per impostazione predefinita, il servizio AMQP di vCloud Director invia messaggi non crittografati. È possibile configurare il servizio AMQP per crittografare questi messaggi utilizzando SSL. È inoltre possibile configurare il servizio per verificare il certificato del broker utilizzando l'archivio affidabilità JCEKS predefinito dell'ambiente di runtime Java nella cella vCloud Director, in genere in `$VCLLOUD_HOME/jre/lib/security/cacerts`.

Per abilitare il protocollo SSL con il servizio AMQP di vCloud Director:

- 1 Nella console Web di vCloud Director, fare clic sulla scheda **Amministrazione** e su **Estendibilità**.
- 2 Fare clic su **Estendibilità** e quindi sulla scheda **Impostazioni**.
- 3 Nella sezione **Impostazioni Broker AMQP**, selezionare **Usa SSL**.
- 4 Selezionare la casella di controllo **Accetta tutti i certificati** o fornire uno dei seguenti:
  - il percorso di un certificato SSL
  - il percorso e la password di un archivio affidabilità JCEKS

## Installazione e configurazione di un database Cassandra per l'archiviazione dei dati relativi alle metriche cronologiche

vCloud Director può raccogliere i valori che forniscono informazioni attuali e cronologiche relative alle prestazioni e all'utilizzo di risorse delle macchine virtuali incluse nel cloud. I dati relativi alle metriche cronologiche vengono archiviati in un cluster Cassandra.

Cassandra è un database open source che può essere utilizzato come archivio di backup di una soluzione scalabile a elevate prestazioni per la raccolta di dati di serie temporali, come le metriche delle macchine virtuali. Se si desidera che vCloud Director supporti il recupero di metriche cronologiche dalle macchine virtuali, è necessario installare e configurare un cluster Cassandra, quindi utilizzare `cell-management-tool` per connettere il cluster a vCloud Director. Per il recupero dei valori attuali non è necessario disporre del software di database facoltativo.

### Prerequisiti

- Assicurarsi che vCloud Director sia installato e in esecuzione, prima di configurare il software del database facoltativo.
- Se non si conosce già Cassandra, consultare il materiale all'indirizzo <http://cassandra.apache.org/>.
- Per l'elenco delle versioni di Cassandra che possono essere utilizzate come database delle metriche, vedere *Note di rilascio di vCloud Director*. È possibile scaricare Cassandra all'indirizzo <http://cassandra.apache.org/download/>.
- Installare e configurare il cluster Cassandra:
  - Il cluster Cassandra deve includere almeno quattro macchine virtuali distribuite in due o più host.
  - Sono necessari due nodi di inizializzazione di Cassandra.
  - Abilitare la codifica da client a nodo di Cassandra. Vedere <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html>.
  - Abilitare l'autenticazione utente di Cassandra. Vedere <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html>.
  - In ogni cluster Cassandra, abilitare Java Native Access (JNA) 3.2.7 o versioni successive.
  - La codifica da nodo a nodo di Cassandra è facoltativa.
  - L'uso del protocollo SSL con Cassandra è facoltativo. Se si decide di non abilitare il protocollo SSL per Cassandra, è necessario impostare il parametro di configurazione `cassandra.use.ssl` su 0 nel file `global.properties` in ogni cella (`$VCLLOUD_HOME/etc/global.properties`)

### Procedura

- 1 Utilizzare l'utilità `cell-management-tool` per configurare una connessione tra vCloud Director e i nodi nel cluster Cassandra.

Nel seguente comando di esempio, *node1-ip*, *node2-ip*, *node3-ip* e *node4-ip* sono gli indirizzi IP dei membri del cluster Cassandra. Viene utilizzata la porta predefinita (9042). I dati relativi alle metriche vengono conservati per 15 giorni.

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --configure --create-schema \ --cluster-nodes node1-
ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P055w0rd' --ttl 15
```

Per informazioni sull'uso dello strumento di gestione delle celle, vedere la *Guida per gli amministratori di vCloud Director*.

- 2 (Facoltativo) Se si sta aggiornando vCloud Director dalla versione 9.1, utilizzare `cell-management-tool` in modo da configurare il database delle metriche per l'archiviazione delle metriche con rollup.

Eseguire un comando simile all'esempio seguente:

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

- 3 Riavviare ciascuna cella di vCloud Director.

## Esecuzione di configurazioni aggiuntive nel database PostgreSQL esterno

Dopo la creazione del gruppo di server di vCloud Director, è possibile configurare il database PostgreSQL esterno per richiedere connessioni SSL dalle celle di vCloud Director e regolare alcuni parametri di database per ottimizzare le prestazioni.

Le connessioni più sicure richiedono un certificato SSL firmato correttamente, che include una catena di attendibilità completa basata su un'autorità di certificazione pubblica conosciuta. In alternativa, è possibile utilizzare un certificato SSL autofirmato o un certificato SSL firmato da un'autorità di certificazione privata, ma è necessario importare il certificato nell'archivio attendibilità di vCloud Director.

Per ottenere prestazioni ottimali per le specifiche e i requisiti di sistema, è possibile modificare le configurazioni del database e i parametri autovacuum nel file di configurazione del database.



## Procedura

### 1 Configurare le connessioni SSL tra vCloud Director e il database PostgreSQL.

- a Se è stato utilizzato un certificato autofirmato o privato per il database PostgreSQL esterno, da ogni cella di vCloud Director eseguire il comando per importare il certificato del database nell'archivio attendibilità di vCloud Director.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#  
  
cell-management-tool import-trusted-certificates --source path_to_self-signed_or_private_cert
```

- b Eseguire il comando per abilitare le connessioni SSL tra vCloud Director e PostgreSQL.

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

È possibile eseguire il comando per tutte le celle nel gruppo di server utilizzando l'opzione `--private-key-path`.

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

Per ulteriori informazioni sull'uso dello strumento di gestione delle celle, vedere *Guida per gli amministratori di vCloud Director*.

### 2 Modificare le configurazioni del database nel file `postgresql.conf` in base alle specifiche del sistema.

Ad esempio, per un sistema con 16 GB di memoria, è possibile utilizzare il frammento seguente.

```
max_connections = 500  
# Set effective cache size to 50% of total memory.  
effective_cache_size = 8GB  
# Set shared buffers to 25% of total memory  
shared_buffers = 4GB
```

### 3 Modificare i parametri autovacuum nel file `postgresql.conf` in base ai propri requisiti.

Per carichi di lavoro di vCloud Director standard, è possibile utilizzare il frammento seguente.

```
autovacuum = on  
track_counts = on  
autovacuum_max_workers = 3  
autovacuum_naptime = 1min  
autovacuum_vacuum_cost_limit = 2400
```

Il sistema imposta un valore `autovacuum_vacuum_scale_factor` personalizzato per l'attività e le tabelle `activity_parameters`.

#### **Operazioni successive**

Se si modifica il file `postgresql.conf`, è necessario riavviare il database.

# Aggiornamento di vCloud Director e applicazione di patch all'appliance di vCloud Director

# 11

È possibile eseguire un aggiornamento orchestrato, aggiornare manualmente vCloud Director a una nuova versione oppure applicare patch alle distribuzioni dell'appliance di vCloud Director.

Se il gruppo di server vCloud Director esistente è composto da installazioni di vCloud Director su Linux, è possibile utilizzare il programma di installazione di vCloud Director per Linux per aggiornare l'ambiente. In alternativa, è possibile migrare l'ambiente all'appliance vCloud Director 9.7. Vedere [Capitolo 12 Migrazione all'appliance vCloud Director](#).

Se il gruppo di server vCloud Director esistente è composto da distribuzioni dell'appliance vCloud Director 9.5, è possibile migrare l'ambiente solo in appliance vCloud Director 9.7. È possibile utilizzare il programma di installazione di vCloud Director per Linux per aggiornare l'ambiente esistente solo come parte del workflow di migrazione. Vedere [Capitolo 12 Migrazione all'appliance vCloud Director](#).

È possibile [Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director](#) o [Aggiornamento manuale di un'installazione di vCloud Director](#). L'aggiornamento orchestrato consente di eseguire un singolo comando che aggiorna tutte le celle nel gruppo di server e il database. Se si esegue l'aggiornamento manuale, si aggiornano in sequenza tutte le celle e il database.

A partire da vCloud Director 9.5:

- I database Oracle non sono supportati. Se l'installazione di vCloud Director esistente utilizza un database Oracle, vedere [Flusso di lavoro per l'aggiornamento di un'installazione di vCloud Director con un database Oracle](#).
- Le operazioni di abilitazione e disabilitazione degli host ESXi non sono supportate. Prima di iniziare l'aggiornamento, è necessario abilitare tutti gli host di ESXi. Per attivare la modalità di manutenzione degli host di ESXi, è possibile utilizzare vSphere Web Client.
- vCloud Director utilizza Java con un supporto LDAP migliorato. Se si utilizza un server LDAPS, per evitare errori di accesso a LDAP, verificare di disporre di un certificato creato correttamente. Per informazioni, vedere *l'argomento relativo alle modifiche di Java 8* all'indirizzo <https://www.java.com>.

Quando si esegue l'aggiornamento di vCloud Director, la nuova versione deve essere compatibile con i seguenti componenti dell'installazione esistente:

- Il software di database correntemente utilizzato per il database di vCloud Director.  
Se l'installazione di vCloud Director esistente utilizza un database Oracle, vedere [Flusso di lavoro per l'aggiornamento di un'installazione di vCloud Director con un database Oracle](#).
- La versione di VMware vSphere® correntemente utilizzata.
- La versione di VMware NSX® correntemente utilizzata.

Per informazioni sui percorsi di aggiornamento e sulla compatibilità di vCloud Director con gli altri prodotti VMware e con database di terze parti, fare riferimento alle *Matrici di interoperabilità dei prodotti VMware* all'indirizzo [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php). Se si intende aggiornare i componenti di NSX o vSphere come parte dell'aggiornamento di vCloud Director, è necessario aggiornarli come descritto in [Capitolo 13 Dopo l'aggiornamento o la migrazione di vCloud Director](#).

Dopo aver aggiornato almeno un server di vCloud Director, è possibile aggiornare il database di vCloud Director. Nel database vengono archiviate le informazioni sullo stato di runtime del server, incluso lo stato di tutti i task di vCloud Director in esecuzione. Per assicurarsi che nel database non rimangano informazioni sui task non valide dopo un aggiornamento, verificare che non vi siano task attivi nei server prima di effettuare l'aggiornamento.

L'aggiornamento preserva anche i seguenti elementi, che non sono archiviati nel database di vCloud Director:

- I file di proprietà locali e globali vengono copiati nella nuova installazione.
- I file di Microsoft Sysprep utilizzati per il supporto della personalizzazione guest vengono copiati nella nuova installazione.

L'aggiornamento richiede un periodo di inattività sufficiente di vCloud Director per aggiornare tutti i server nel gruppo di server e il database. Se si utilizza un programma di bilanciamento del carico, è possibile configurarlo in modo che restituisca un messaggio, ad esempio *Il sistema non è in linea per aggiornamento*.

## Flusso di lavoro per l'aggiornamento di un'installazione di vCloud Director con un database Oracle

Prima di aggiornare un'installazione di vCloud Director che utilizza un database Oracle, è necessario eseguire la migrazione del database a PostgreSQL da vCloud Director versione 9.1.

- 1 Se la versione di vCloud Director corrente è precedente alla 9.1, eseguire l'aggiornamento alla versione 9.1.

Per informazioni sull'aggiornamento di vCloud Director alla versione 9.1, vedere *Guida all'installazione, alla configurazione e all'aggiornamento di vCloud Director 9.1*.

- 2 Quando l'installazione di vCloud Director è relativa alla versione 9.1, eseguire la migrazione del database Oracle a un database PostgreSQL.

Per informazioni sulla migrazione a un database PostgreSQL, vedere il riferimento allo strumento di gestione delle celle nella documentazione di *Guida per gli amministratori di vCloud Director*.

- 3 Aggiornare l'installazione di vCloud Director dalla versione 9.1. È possibile eseguire la procedura [Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director](#) o [Aggiornamento manuale di un'installazione di vCloud Director](#).

## Applicazione di patch alla distribuzione dell'appliance di vCloud Director

È possibile applicare patch all'appliance di vCloud Director per migliorarne la funzionalità o la sicurezza. Vedere [Applicazione di patch alla distribuzione dell'appliance vCloud Director](#). Dopo aver applicato la patch a ogni appliance vCloud Director e aver completato l'aggiornamento del database, è necessario riavviare i servizi vCloud Director nel gruppo di server per riportarlo di nuovo online.

Questo capitolo include i seguenti argomenti:

- [Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director](#)
- [Aggiornamento manuale di un'installazione di vCloud Director](#)
- [Riferimento dell'utilità di aggiornamento del database](#)
- [Applicazione di patch alla distribuzione dell'appliance vCloud Director](#)

## Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director

È possibile aggiornare tutte le celle nel gruppo di server insieme al database condiviso eseguendo il programma di installazione di vCloud Director con l'opzione `--private-key-path`.

È possibile utilizzare il programma di installazione di vCloud Director per Linux per aggiornare un gruppo di server di vCloud Director composto da installazioni di vCloud Director in un sistema operativo Linux supportato. Se il gruppo di server di vCloud Director è costituito da distribuzioni di appliance vCloud Director 9.5, è possibile utilizzare il programma di installazione di vCloud Director per Linux per aggiornare l'ambiente esistente solo come parte del flusso di lavoro di migrazione. Vedere [Capitolo 12 Migrazione all'appliance vCloud Director](#).

vCloud Director for Linux è distribuito come file eseguibile firmato digitalmente con formato del nome `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, dove *v.v.v* rappresenta la versione di prodotto e *nnnnnn* il numero di build. Ad esempio: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Questo eseguibile consente di installare o aggiornare vCloud Director.

Quando si esegue il programma di installazione di vCloud Director con l'opzione `--private-key-path`, è possibile aggiungere altre opzioni di comando dell'utilità `upgrade`, ad esempio `--maintenance-cell`. Per informazioni sulle opzioni dell'utilità `upgrade` del database, vedere [Riferimento dell'utilità di aggiornamento del database](#).

### Prerequisiti

- Verificare che il database vCloud Director, i componenti vSphere e i componenti NSX siano compatibili con la nuova versione di vCloud Director.

---

**Importante** Se l'installazione di vCloud Director esistente utilizza un database Oracle, verificare di aver effettuato la migrazione a un database PostgreSQL da vCloud Director versione 9.1. Vedere [Flusso di lavoro per l'aggiornamento di un'installazione di vCloud Director con un database Oracle](#).

---

- Assicurarsi di disporre delle credenziali di utente con privilegi avanzati per il server di destinazione
- Se si desidera che il programma di installazione verifichi la firma digitale del file di installazione, scaricare e installare la chiave pubblica VMware nel server di destinazione. Se la firma digitale del file di installazione è stata già verificata, non è necessario verificarla di nuovo durante l'installazione. Vedere [Download e installazione della chiave pubblica VMware](#).
- Assicurarsi di disporre di una chiave di licenza valida per utilizzare la versione del software vCloud Director a cui si desidera effettuare l'aggiornamento.
- Verificare che tutte le celle consentano le connessioni SSH da parte dell'utente con privilegi avanzati senza alcuna password. Per eseguire una verifica è possibile eseguire il seguente comando di Linux:

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

Nell'esempio seguente l'identità dell'utente viene impostata su `vcloud`, quindi viene stabilita una connessione SSH alla cella in `cell-ip` come `root`, ma la password dell'utente `root` non viene fornita. Se la chiave privata in `private-key-path` nella cella locale è leggibile dall'utente `vcloud.vcloud` e la chiave pubblica corrispondente è presente nel file `authorized-keys` per l'utente `root` in `cell-ip`, il comando viene eseguito correttamente.

---

**Nota** Il programma di installazione di vCloud Director crea l'utente `vcloud`, il gruppo `vcloud` e l'account `vcloud.vcloud` per consentire di utilizzarli come identità con cui vengono eseguiti i processi di vCloud Director. L'utente `vcloud` non dispone di password.

---

- Verificare che tutti gli host di ESXi siano abilitati. A partire da vCloud Director 9.5, gli host di ESXi disabilitati non sono supportati.
- Verificare che tutti i server nel gruppo di server possano accedere allo storage del server di trasferimento condiviso. Vedere [Preparazione dello storage del server di trasferimento](#).

- Se l'installazione di vCloud Director utilizza un server LDAPS, per evitare errori di accesso LDAP dopo l'aggiornamento, verificare di disporre di un certificato creato adeguatamente per Java 8 Update 181. Per informazioni, vedere l'*argomento relativo alle modifiche di Java 8* all'indirizzo <https://www.java.com>.

## Procedura

- 1 Eseguire il login al server di destinazione come utente **root**.

- 2 Scaricare il file di installazione nel server di destinazione.

Se il software è stato acquistato su supporto multimediale, copiare il file di installazione in una posizione accessibile dal server di destinazione.

- 3 Verificare che il checksum del download corrisponda a quello pubblicato nella pagina di download.

I valori per entrambi i checksum MD5 e SHA1 vengono pubblicati nella pagina di download. Utilizzare lo strumento appropriato per verificare che il checksum del file di installazione scaricato corrisponda a quello visualizzato nella pagina di download. Un comando Linux nel seguente formato visualizza il checksum per *file-installazione*.

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

Il comando restituisce il checksum del file di installazione che deve corrispondere al checksum MD5 della pagina di download.

- 4 Verificare che il file di installazione sia eseguibile.

Tale file richiede l'autorizzazione per l'esecuzione. Per verificare se tale autorizzazione è disponibile, aprire una console, una shell o una finestra del terminale ed eseguire il comando Linux riportato di seguito, dove *file-di-installazione* è il percorso completo del file di installazione di vCloud Director.

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

- 5 In una console, shell o finestra del terminale, eseguire il file di installazione con l'opzione `--private-key-path` e il percorso completo della chiave privata della cella di destinazione.

È possibile aggiungere altre opzioni di comando dell'utilità `upgrade` del database.

```
./installation-file --private-key-path /vcloud/.ssh/id_rsa
```

---

**Nota** Non è possibile eseguire il file di installazione da una directory il cui percorso includa caratteri spazio incorporati.

---

Il programma di installazione rileva una versione precedente di vCloud Director e richiede di confermare l'aggiornamento.

Se il programma di installazione rileva una versione di vCloud Director che corrisponde o è successiva alla versione del file di installazione, viene visualizzato un messaggio di errore e il programma di installazione si chiude.

- 6 Immettere **y** e premere INVIO per confermare l'aggiornamento.

#### Risultati

Il programma di installazione avvia il seguente flusso di lavoro di aggiornamento di più celle.

- 1 Verifica che l'host della cella corrente soddisfi tutti i requisiti.
- 2 Apre il pacchetto RPM di vCloud Director.
- 3 Aggiorna il software di vCloud Director nella cella corrente.
- 4 Aggiorna il database di vCloud Director.
- 5 Aggiorna il software di vCloud Director in tutte le celle rimanenti, quindi riavvia i servizi di vCloud Director nella cella.
- 6 Riavvia i servizi di vCloud Director nella cella corrente.

#### Operazioni successive

Avviare i servizi di vCloud Director in tutte le celle nel gruppo di server.

È ora possibile [Aggiornamento di ciascun NSX Manager associato a un sistema vCenter Server collegato](#), quindi [Aggiornamento dei sistemi vCenter Server, degli host ESXi e degli NSX Edge](#).

## Aggiornamento manuale di un'installazione di vCloud Director

È possibile aggiornare una singola cella eseguendo il programma di installazione di vCloud Director senza opzioni di comando. Prima di riavviare una cella aggiornata, è necessario aggiornare lo schema del database. È possibile aggiornare lo schema del database dopo aver aggiornato almeno una cella nel gruppo di server.

È possibile utilizzare il programma di installazione di vCloud Director per Linux per aggiornare un gruppo di server di vCloud Director composto da installazioni di vCloud Director in un sistema operativo Linux supportato. Se il gruppo di server di vCloud Director è costituito da distribuzioni di appliance vCloud Director 9.5, è possibile utilizzare il programma di installazione di vCloud Director per Linux per aggiornare l'ambiente esistente solo come parte del flusso di lavoro di migrazione. Vedere [Capitolo 12 Migrazione all'appliance vCloud Director](#).

Per un'installazione di vCloud Director in più celle, anziché aggiornare manualmente ogni cella e il database in sequenza, è possibile [Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director](#).



## Prerequisiti

- Verificare che il database vCloud Director, i componenti vSphere e i componenti NSX siano compatibili con la nuova versione di vCloud Director.

---

**Importante** Se l'installazione di vCloud Director esistente utilizza un database Oracle, verificare di aver effettuato la migrazione a un database PostgreSQL da vCloud Director versione 9.1. Vedere [Flusso di lavoro per l'aggiornamento di un'installazione di vCloud Director con un database Oracle](#).

---

- Verificare di disporre delle credenziali di utente con privilegi avanzati per i server nel gruppo di server vCloud Director.
- Se si desidera che il programma di installazione verifichi la firma digitale del file di installazione, scaricare e installare la chiave pubblica VMware nel server di destinazione. Se la firma digitale del file di installazione è stata già verificata, non è necessario verificarla di nuovo durante l'installazione. Vedere [Download e installazione della chiave pubblica VMware](#).
- Assicursi di disporre di una chiave di licenza valida per utilizzare la versione del software vCloud Director a cui si desidera effettuare l'aggiornamento.
- Verificare che tutti gli host di ESXi siano abilitati. A partire da vCloud Director 9.5, gli host di ESXi disabilitati non sono supportati.

## Procedura

### 1 [Aggiornamento di una cella di vCloud Director](#)

Il programma di installazione di vCloud Director verifica che il server di destinazione soddisfi tutti i requisiti preliminari di aggiornamento ed esegue l'aggiornamento del software vCloud Director sul server.

### 2 [Esecuzione dell'aggiornamento del database vCloud Director](#)

Da un server vCloud Director aggiornato, è possibile eseguire uno strumento che effettui l'aggiornamento del database vCloud Director. Riavviare il server vCloud Director aggiornato solo dopo aver aggiornato il database condiviso.

## Operazioni successive

Dopo aver aggiornato tutti i server di vCloud Director nel gruppo di server e il database, è possibile avviare i servizi di vCloud Director in tutte le celle.

È possibile [Aggiornamento di ciascun NSX Manager associato a un sistema vCenter Server collegato](#), quindi è possibile [Aggiornamento dei sistemi vCenter Server, degli host ESXi e degli NSX Edge](#).

## Aggiornamento di una cella di vCloud Director

Il programma di installazione di vCloud Director verifica che il server di destinazione soddisfi tutti i requisiti preliminari di aggiornamento ed esegue l'aggiornamento del software vCloud Director sul server.

vCloud Director for Linux è distribuito come file eseguibile firmato digitalmente con formato del nome `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, dove *v.v.v* rappresenta la versione di prodotto e *nnnnnn* il numero di build. Ad esempio: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Questo eseguibile consente di installare o aggiornare vCloud Director.

Per un'installazione di vCloud Director in più celle, è necessario eseguire il programma di installazione di vCloud Director in ogni membro del gruppo di server vCloud Director.

### Procedura

- 1 Eseguire il login al server di destinazione come utente **root**.

- 2 Scaricare il file di installazione nel server di destinazione.

Se il software è stato acquistato su supporto multimediale, copiare il file di installazione in una posizione accessibile dal server di destinazione.

- 3 Verificare che il checksum del download corrisponda a quello pubblicato nella pagina di download.

I valori per entrambi i checksum MD5 e SHA1 vengono pubblicati nella pagina di download. Utilizzare lo strumento appropriato per verificare che il checksum del file di installazione scaricato corrisponda a quello visualizzato nella pagina di download. Un comando Linux nel seguente formato visualizza il checksum per *file-installazione*.

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

Il comando restituisce il checksum del file di installazione che deve corrispondere al checksum MD5 della pagina di download.

- 4 Verificare che il file di installazione sia eseguibile.

Tale file richiede l'autorizzazione per l'esecuzione. Per verificare se tale autorizzazione è disponibile, aprire una console, una shell o una finestra del terminale ed eseguire il comando Linux riportato di seguito, dove *file-di-installazione* è il percorso completo del file di installazione di vCloud Director.

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

- 5 Eseguire il file di installazione.

Per eseguire il file di installazione, immetterne il percorso completo, ad esempio:

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

Il file include uno script di installazione e un pacchetto RPM incorporato.

---

**Nota** Non è possibile eseguire il file di installazione da una directory il cui percorso includa caratteri spazio incorporati.

---

Se il programma di installazione rileva una versione di vCloud Director che corrisponde o è successiva alla versione del file di installazione, viene visualizzato un messaggio di errore e il programma di installazione si chiude.

Se il programma di installazione rileva una versione precedente di vCloud Director, viene richiesto di confermare l'aggiornamento.

## 6 Immettere **y** e premere INVIO per confermare l'aggiornamento.

Il programma di installazione avvia il flusso di lavoro di aggiornamento seguente.

- a Verifica che l'host soddisfi tutti i requisiti.
- b Apre il pacchetto RPM di vCloud Director.
- c Una volta terminati tutti i processi di vCloud Director attivi nella cella, arresta i servizi di vCloud Director nel server e aggiorna il software di vCloud Director installato.

Se la chiave pubblica di VMware non è installata nel server di destinazione, il programma di installazione visualizza un avviso nel formato seguente:

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

Quando si modifica il file `global.properties` esistente nel server di destinazione, il programma di installazione visualizza un avviso nel formato seguente:

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-director/etc/global.properties.rpmnew
```

**Nota** Se il file `global.properties` esistente è stato precedentemente aggiornato, è possibile recuperare le modifiche da `global.properties.rpmnew`.

## 7 (Facoltativo) Eseguire l'aggiornamento delle proprietà di registrazione.

Al termine di un aggiornamento, nel file `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` vengono scritte nuove proprietà di registrazione.

Opzione	Azione
<b>Se le proprietà di registrazione esistenti non sono state modificate</b>	Copiare questo file in <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> .
<b>Se le proprietà di registrazione sono state modificate</b>	Per mantenere le modifiche, unire <code>/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew</code> al file <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> esistente.

## Risultati

Al termine dell'aggiornamento di vCloud Director, il programma di installazione visualizza un messaggio con le informazioni sulla posizione dei file di configurazione precedenti. Il programma di installazione richiede quindi l'esecuzione dello strumento di aggiornamento del database.

## Operazioni successive

Se non è ancora stato aggiornato, è possibile aggiornare il database di vCloud Director.

Ripetere questa procedura per ogni cella di vCloud Director nel gruppo di server.

---

**Importante** Non avviare i servizi di vCloud Director finché non si esegue l'aggiornamento di tutte le celle nel gruppo di server e del database.

---

## Esecuzione dell'aggiornamento del database vCloud Director

Da un server vCloud Director aggiornato, è possibile eseguire uno strumento che effettui l'aggiornamento del database vCloud Director. Riavviare il server vCloud Director aggiornato solo dopo aver aggiornato il database condiviso.

Le informazioni su tutti i task in esecuzione e completati di recente vengono archiviate nel database vCloud Director. Poiché l'aggiornamento di un database invalida queste informazioni sulle attività, l'utilità di aggiornamento del database verifica che non vi siano attività in esecuzione quando il processo di aggiornamento inizia.

Tutte le celle in un gruppo di server vCloud Director condividono lo stesso database. Indipendentemente dal numero di celle che si sta aggiornando, è necessario aggiornare il database una sola volta. Dopo l'aggiornamento del database, le celle di vCloud Director che non vengono aggiornate non possono connettersi al database. È necessario aggiornare tutte le celle in modo che siano connesse al database aggiornato.

### Prerequisiti

- Eseguire il backup del database esistente, utilizzando le procedure consigliate dal fornitore del software di database.
- Verificare che tutte le celle di vCloud Director nel gruppo di server siano arrestate. Le celle aggiornate vengono arrestate durante il processo di aggiornamento. Se sono presenti server vCloud Director non ancora aggiornati, è possibile utilizzare lo strumento di gestione delle celle per disattivare e arrestare i relativi servizi. Per informazioni su come gestire una cella utilizzando lo strumento di gestione delle celle, vedere *Guida per gli amministratori di vCloud Director*.
- Se l'installazione di vCloud Director utilizza un database Oracle, eseguire la migrazione a un database PostgreSQL. Per informazioni sulla migrazione a un database PostgreSQL, vedere il riferimento allo strumento di gestione delle celle in *Guida per gli amministratori di vCloud Director*.
- Esaminare il [Riferimento dell'utilità di aggiornamento del database](#). Le opzioni e gli argomenti non sono obbligatori.

## Procedura

- 1 Eseguire l'utilità `upgrade` del database con o senza opzioni.

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

Se l'utilità di aggiornamento del database rileva una versione non compatibile di NSX Manager, viene visualizzato un messaggio di avviso e l'aggiornamento viene annullato.

- 2 Alla richiesta, immettere **y** e premere INVIO per confermare l'aggiornamento del database.
- 3 Alla richiesta, immettere **y** e premere INVIO per confermare di aver eseguito il backup del database.

Se è stata utilizzata l'opzione `--backup-completed`, l'utilità ignora questa richiesta.

- 4 Se l'utilità rileva una cella attiva, alla richiesta di continuare immettere **n** per uscire dalla shell, verificare che non vi siano celle in esecuzione e riprovare l'aggiornamento dal [Passaggio 1](#).

## Risultati

Viene eseguito lo strumento di aggiornamento dei database che mostra messaggi sullo stato di avanzamento. Al termine dell'aggiornamento, viene richiesto di avviare il servizio vCloud Director nel server corrente.

## Operazioni successive

Immettere **y** e premere INVIO o avviare il servizio in un secondo momento eseguendo il comando `service vmware-vcd start`.

È possibile avviare i servizi dei server vCloud Director aggiornati.

È possibile aggiornare gli altri membri vCloud Director del gruppo di server e avviarne i servizi. Vedere [Aggiornamento di una cella di vCloud Director](#).

## Riferimento dell'utilità di aggiornamento del database

Quando si esegue l'utilità `upgrade`, le informazioni di configurazione nella riga di comando vengono fornite come opzioni e argomenti.

Tabella 11-1. Opzioni e argomenti dell'utilità di aggiornamento del database

Opzione	Argomento	Descrizione
--backup-completed	Nessuno	Specifica che è stato completato un backup di vCloud Director. Quando si include questa opzione, l'utilità di aggiornamento non mostra la richiesta di effettuare il backup del database.
--ceip-user	Nome utente dell'account del servizio CEIP.	Se nell'organizzazione System è già presente questo nome utente, l'aggiornamento non riuscirà. Predefinito: phone-home-system-account
--enable-ceip	Scegliere tra: ■ true ■ false	Specifica se l'installazione partecipa al programma di miglioramento dell'esperienza utente CEIP (Customer Experience Improvement Program) VMware. L'impostazione predefinita è true se non viene specificato alcun valore e se non si imposta il valore false nella configurazione corrente. Ulteriori informazioni sui dati raccolti tramite il programma CEIP e le finalità per le quali vengono utilizzati da VMware sono riportate nel centro di affidabilità e controllo all'indirizzo <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> . È possibile utilizzare lo strumento di gestione delle celle per attivare o disattivare la partecipazione al programma CEIP VMware per questo prodotto in qualsiasi momento. <i>Guida per gli amministratori di vCloud Director</i>

Tabella 11-1. Opzioni e argomenti dell'utilità di aggiornamento del database (continua)

Opzione	Argomento	Descrizione
--installer-path	Percorso completo del file di installazione di vCloud Director. Il file di installazione e la directory in cui è memorizzato devono essere leggibili dall'utente vcloud.vcloud.	<p>Questo prodotto partecipa al programma CEIP (Customer Experience Improvement Program) di VMware. I dettagli sui dati raccolti tramite il programma CEIP e le finalità per le quali vengono utilizzati da VMware sono riportati nel centro di affidabilità e controllo all'indirizzo <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a>. È possibile utilizzare lo strumento di gestione delle celle per attivare o disattivare la partecipazione al programma CEIP VMware per questo prodotto in qualsiasi momento. Vedere "Guida di riferimento allo strumento di gestione delle celle" nella <i>Guida per gli amministratori di vCloud Director</i>.</p> <p>Richiede l'opzione --private-key-path .</p>
--maintenance-cell	Indirizzo IP	<p>Indirizzo IP di una cella utilizzato dall'utilità di aggiornamento per l'esecuzione in modalità di manutenzione durante l'aggiornamento. Questa cella passa in modalità di manutenzione prima della disattivazione delle altre celle e resta in modalità di manutenzione mentre le altre celle vengono aggiornate. Dopo che le altre celle sono state aggiornate e almeno una di esse riavviata, questa cella viene disattivata e aggiornata. Richiede l'opzione --private-key-path .</p>
--multisite-user	Nome utente per l'account di sistema multisito.	<p>Questo account viene utilizzato dalla funzionalità multisito di vCloud Director. Se nell'organizzazione System è già presente questo nome utente, l'aggiornamento non riuscirà. Predefinito: multisite-system-account</p>

Tabella 11-1. Opzioni e argomenti dell'utilità di aggiornamento del database (continua)

Opzione	Argomento	Descrizione
<code>--private-key-path</code>	Percorso completo	Percorso completo della chiave privata della cella. Quando si utilizza questa opzione, tutte le celle del gruppo di server vengono disattivate in modo normale, aggiornate e riavviate dopo aver aggiornato il database. Vedere <a href="#">Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director</a> per ulteriori informazioni su questo flusso di lavoro di aggiornamento.
<code>--unattended-upgrade</code>	Nessuno	Specifica l'esecuzione di un aggiornamento automatico.

Se si utilizza l'opzione `--private-key-path`, è necessario configurare tutte le celle in modo da consentire connessioni ssh da parte del superuser senza alcuna password. È possibile utilizzare una riga di comando Linux come quella seguente per verificare questa condizione. Nell'esempio seguente l'identità dell'utente viene impostata su `vcld`, quindi viene stabilita una connessione ssh alla cella in `cell-ip` come `root`, ma la password dell'utente `root` non viene fornita.

```
sudo -u vcld ssh -i private-key-path root@cell-ip
```

Se la chiave privata in *private-key-path* nella cella locale è leggibile dall'utente `vcld.vcld` e la chiave pubblica corrispondente è stata aggiunta al file `authorized-keys` per l'utente `root` in *cell-ip*, il comando viene eseguito correttamente.

**Nota** Il programma di installazione di vCloud Director crea l'utente `vcld`, il gruppo `vcld` e l'account `vcld.vcld` per consentire di utilizzarli come identità con cui vengono eseguiti i processi di vCloud Director. L'utente `vcld` non dispone di password.

## Applicazione di patch alla distribuzione dell'appliance vCloud Director

È possibile aggiornare l'appliance vCloud Director con le patch che possono essere correlate alla funzionalità del prodotto e ai miglioramenti della sicurezza.

Durante l'applicazione delle patch alla distribuzione dell'appliance vCloud Director, il servizio vCloud Director smette di funzionare e può verificarsi un po' di tempo di inattività. Il tempo di inattività dipende dal tempo necessario per applicare la patch a ogni appliance vCloud Director e per eseguire lo script di aggiornamento del database vCloud Director. Il numero di celle funzionanti nel gruppo di server vCloud Director si riduce finché non si arresta il servizio vCloud Director nell'ultima appliance vCloud Director. Un bilanciamento del carico configurato correttamente davanti agli endpoint HTTP di vCloud Director dovrebbe interrompere il routing del traffico verso le celle arrestate.



Dopo aver applicato la patch a ogni appliance vCloud Director e aver completato l'aggiornamento del database, è necessario riavviare i servizi vCloud Director nel gruppo di server per riportarlo di nuovo online.

#### Procedura

- 1 In un browser Web, accedere all'interfaccia utente di gestione dell'appliance di un'istanza dell'appliance vCloud Director per identificare l'appliance primaria, `https://appliance_ip_address:5480`.

Prendere nota del nome dell'appliance primaria. Quando si esegue l'aggiornamento del database, è necessario utilizzare il nome dell'appliance primaria.

- 2 Scaricare il pacchetto di aggiornamento in un'appliance.

vCloud Director è distribuito come file eseguibile con il nome del modulo `VMware_vCloud_Director_v.v.v.v-nnnnnnnn_update.tar.gz`, dove *v.v.v.v* rappresenta la versione di prodotto e *nnnnnnnn* il numero di build. Ad esempio, `VMware_vCloud_Director_9.7.0.4248-13560441_update.tar.gz`.

- 3 Creare la directory `local-update-package` in cui estrarre il pacchetto di aggiornamento.

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

- 4 Estrarre il pacchetto di aggiornamento nella directory appena creata.

```
tar -zxf VMware_vCloud_Director_v.v.v.v-nnnnnnnn_update.tar.gz \
-C /tmp/local-update-package
```

- 5 Impostare la directory `local-update-package` come repository di aggiornamento.

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

- 6 Controllare la disponibilità degli aggiornamenti per verificare che il repository sia stato stabilito correttamente.

```
vamcli update --check
```

La versione della patch viene visualizzata come **Aggiornamento disponibile**.

- 7 Arrestare vCloud Director eseguendo il comando seguente:

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

- 8 Dall'appliance primaria, eseguire il backup del database incorporato dell'appliance vCloud Director.

---

**Nota** Se si esegue l'aggiornamento da vCloud Director 9.7.0.1 a una versione successiva, eseguire manualmente il backup del file truststore che si trova in `/opt/vmware/vcloud-director/etc/truststore`.

---

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

- 9 Applicare la patch disponibile.

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

- 10 Ripetere i passaggi da [Passaggio 2](#) a [Passaggio 7](#) e [Passaggio 9](#) in ogni appliance.
- 11 Da qualsiasi appliance, eseguire lo script di aggiornamento del database vCloud Director.

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

- 12 Avviare i servizi vCloud Director in ogni appliance.

```
service vmware-vcd start
```

# Migrazione all'appliance vCloud Director

# 12

A partire dalla versione 9.7, l'appliance vCloud Director include un database PostgreSQL incorporato con funzionalità a disponibilità elevata. È possibile eseguire la migrazione dell'ambiente vCloud Director esistente di una versione precedente a un ambiente vCloud Director costituito da distribuzioni dell'appliance vCloud Director 9.7.

È possibile eseguire la migrazione di un ambiente vCloud Director costituito da installazioni di vCloud Director su distribuzioni di appliance Linux o vCloud Director. È possibile eseguire la migrazione di un ambiente vCloud Director che utilizza un database Microsoft SQL esterno o un database PostgreSQL esterno.

Se l'ambiente vCloud Director utilizza un database Oracle esterno, prima di effettuare la migrazione all'appliance vCloud Director, è necessario eseguire la migrazione del database a PostgreSQL da vCloud Director versione 9.1. Per informazioni sul workflow per l'aggiornamento di un'installazione di vCloud Director con un database Oracle, vedere [Capitolo 11 Aggiornamento di vCloud Director e applicazione di patch all'appliance di vCloud Director](#).

Questo capitolo include i seguenti argomenti:

- [Migrazione di vCloud Director con un database Microsoft SQL esterno all'appliance vCloud Director](#)
- [Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director](#)

## Migrazione di vCloud Director con un database Microsoft SQL esterno all'appliance vCloud Director

Se l'ambiente vCloud Director corrente di una versione precedente utilizza un database Microsoft SQL esterno, è possibile eseguire la migrazione a un nuovo ambiente vCloud Director costituito da distribuzioni dell'appliance vCloud Director 9.7. L'ambiente vCloud Director corrente può essere costituito da installazioni di vCloud Director in Linux o da distribuzioni dell'appliance vCloud Director. Il nuovo ambiente vCloud Director può utilizzare i database PostgreSQL integrati dell'appliance in modalità a disponibilità elevata.

Il flusso di lavoro di migrazione include quattro fasi principali.

- Creazione del nuovo gruppo di server di vCloud Director mediante la distribuzione di una o più istanze dell'appliance vCloud Director 9.7

- Aggiornamento dell'ambiente vCloud Director esistente
- Migrazione del database esterno nel database integrato
- Copia dei dati del servizio di trasferimento condiviso e dei dati dei certificati

## Procedura

- 1 Aggiornare l'ambiente vCloud Director corrente alla versione 9.7 e aggiornare lo schema del database di origine.

Vedere [Capitolo 11 Aggiornamento di vCloud Director e applicazione di patch all'appliance di vCloud Director](#).

- 2 Verificare che il riavvio dell'origine della migrazione vCloud Director abbia esito positivo.
- 3 Se si desidera che il nuovo ambiente vCloud Director utilizzi gli indirizzi IP dell'ambiente esistente, sostituire gli indirizzi IP delle celle esistenti con indirizzi IP temporanei.
- 4 Se si desidera che il nuovo ambiente vCloud Director utilizzi il server NFS dell'ambiente esistente, creare ed esportare una nuova directory in questo server NFS come nuovo punto di montaggio NFS condiviso.

Non è possibile riutilizzare il punto di montaggio esistente perché gli ID utente e gruppo (UID/GID) degli utenti nel vecchio NFS potrebbero non coincidere con gli ID utente e gruppo nel nuovo NFS.

- 5 Creare il nuovo gruppo di server distribuendo una o più istanze dell'appliance vCloud Director 9.7.
  - Se si desidera utilizzare la funzionalità a disponibilità elevata (HA) del database, distribuire una cella primaria e due celle di standby e, facoltativamente, una o più celle dell'applicazione vCD.
  - Se si sostituiscono gli indirizzi IP delle celle esistenti con indirizzi IP temporanei, è possibile utilizzare gli indirizzi IP originali per le nuove celle.
  - Se si esporta un nuovo percorso nel server NFS esistente, è possibile utilizzare questo nuovo punto di montaggio condiviso per il nuovo ambiente.

Vedere [Capitolo 6 Distribuzione dell'appliance vCloud Director](#).

- 6 In ogni cella esistente e in ogni cella appena distribuita, eseguire il comando per arrestare il servizio vCloud Director.

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

- 7 Scegliere una delle celle esistenti come origine della migrazione.

L'origine della migrazione deve avere accesso all'indirizzo IP di rete eth1 della cella primaria appena distribuita.

- 8 Nella nuova cella primaria, abilitare l'accesso al database integrato dall'origine della migrazione.

Vedere [Configurazione dell'accesso esterno al database di vCloud Director](#).

- 9 Nell'origine della migrazione, eseguire lo strumento di gestione delle celle per eseguire la migrazione del database esterno al database integrato nella nuova cella primaria.

Il database integrato utilizza l'indirizzo IP di rete eth1 dell'appliance.

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

Per informazioni sull'uso dello strumento di gestione delle celle, vedere la *Guida per gli amministratori di vCloud Director*.

- 10 In ciascuna cella appena distribuita, eseguire il backup e sostituire i dati di configurazione e riconfigurare e avviare il servizio vCloud Director.

- a Eseguire il backup delle proprietà e dei file dei certificati e copiare e sostituire questi file dall'origine della migrazione.

I file `global.properties`, `responses.properties`, `certificates` e `proxycertificates` sono disponibili in `/opt/vmware/vcloud-director/etc/`.

---

**Importante** Se si esegue la migrazione a vCloud Director versione 9.7.0.1 o successiva, è inoltre necessario eseguire il backup, la copia e la sostituzione del file `truststore` dall'origine della migrazione, insieme agli altri file.

---

- b Eseguire il backup del file dell'archivio chiavi che si trova in `/opt/vmware/vcloud-director/certificates.ks`.

Non copiare e sostituire con il file di archivio chiavi dall'origine della migrazione.

- c Eseguire il comando per riconfigurare il servizio vCloud Director.

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

Dove:

- Il valore `--keystore-password` corrisponde alla password **root** iniziale di questa appliance.
- Il valore `--database-password` corrisponde alla password del database impostata durante la distribuzione dell'appliance.
- Il valore `--database-host` corrisponde all'indirizzo IP di rete eth1 dell'appliance primaria.
- Il valore `--keystore` è il percorso del file `certificates.ks` di cui è stato eseguito il backup nel passaggio [10.b](#).

- Il valore `--primary-ip` corrisponde all'indirizzo IP di rete `eth0` dell'appliance.
- Il valore `--console-proxy-ip` corrisponde all'indirizzo IP di rete `eth0` dell'appliance.

Per informazioni sulla risoluzione dei problemi, vedere [La riconfigurazione del servizio vCloud Director non riesce durante la migrazione o il ripristino dell'appliance vCloud Director](#).

- d Eseguire il comando per avviare il servizio vCloud Director.

```
service vmware-vcd start
```

È possibile monitorare l'avanzamento dell'avvio della cella in `/opt/vmware/vcloud-director/logs/cell.log`.

- 11 Dopo aver completato il processo di avvio di tutte le celle del nuovo gruppo di server, verificare che la migrazione dell'ambiente vCloud Director sia stata eseguita correttamente.
  - a Aprire vCloud Director Web Console utilizzando l'indirizzo IP di rete `eth0` di una cella del nuovo gruppo di server, `https://eth0_IP_new_cell/cloud`.
  - b Accedere a vCloud Director Web Console con le credenziali dell'**amministratore di sistema** esistenti.
  - c Verificare che le risorse vSphere e cloud siano disponibili nel nuovo ambiente.
- 12 Dopo aver verificato correttamente la migrazione di vCloud Director, utilizzare vCloud Director Web Console per eliminare le celle disconnesse che appartengono al vecchio ambiente vCloud Director.
  - a Nella scheda **Gestisci e monitora**, fare clic su **Celle cloud**.
  - b Fare clic con il pulsante destro del mouse sul nome di una cella e scegliere **Elimina**.

È possibile distribuire l'appliance vCloud Director per aggiungere membri al gruppo di server dell'ambiente migrato.

## Operazioni successive

Il nuovo ambiente dell'appliance vCloud Director migrato utilizza certificati autofirmati. Per utilizzare i certificati firmati correttamente dall'ambiente precedente in ogni cella del nuovo ambiente eseguire i passaggi seguenti:

- 1 Copiare e sostituire il file dell'archivio chiavi dalla cella precedente in `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.
- 2 Eseguire il comando dello strumento di gestione delle celle per sostituire i certificati.

Assicurarsi che `vcloud.vcloud` sia il proprietario di questo file.

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

### 3 Riavviare il servizio vCloud Director.

```
service vmware-vcd restart
```

Se si aggiungono nuovi membri a questo gruppo di server, le nuove celle dell'appliance vengono distribuite con questi certificati firmati correttamente.

## Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director

Se l'ambiente vCloud Director corrente di una versione precedente utilizza un database PostgreSQL esterno, è possibile eseguire la migrazione a un nuovo ambiente vCloud Director costituito da distribuzioni dell'appliance vCloud Director 9.7. L'ambiente vCloud Director corrente può essere costituito da installazioni di vCloud Director in Linux o da distribuzioni dell'appliance vCloud Director. Il nuovo ambiente vCloud Director può utilizzare i database PostgreSQL integrati dell'appliance in modalità a disponibilità elevata.

Il flusso di lavoro di migrazione include quattro fasi principali.

- Aggiornamento dell'ambiente vCloud Director esistente
- Creazione del nuovo gruppo di server di vCloud Director mediante la distribuzione di una o più istanze dell'appliance vCloud Director 9.7
- Migrazione del database esterno nel database integrato
- Copia dei dati del servizio di trasferimento condiviso e dei dati dei certificati

### Procedura

- 1 Se la versione del database PostgreSQL esterno corrente è 9.x, aggiornarlo alla versione 10.
- 2 Aggiornare l'ambiente vCloud Director corrente alla versione 9.7.

Vedere [Capitolo 11 Aggiornamento di vCloud Director e applicazione di patch all'appliance di vCloud Director](#).

- 3 Verificare che il riavvio dell'origine della migrazione vCloud Director abbia esito positivo.
- 4 In ogni cella dell'ambiente vCloud Director aggiornato, eseguire il comando per arrestare il servizio vCloud Director.

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

- 5 Nel database PostgreSQL esterno, eseguire il backup del database corrente.

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

Se nella cartella /tmp non è disponibile spazio sufficiente, utilizzare un'altra posizione per archiviare il file di dump.

- 6 Se il proprietario del database e il nome del database sono diversi da vcloud, prendere nota del nome utente e del nome del database.

È necessario creare questo utente nel nuovo ambiente e rinominare il database al passaggio 13.

- 7 Se si desidera che il nuovo ambiente vCloud Director utilizzi gli indirizzi IP dell'ambiente esistente, è necessario copiare le proprietà e i file dei certificati in una posizione nel database PostgreSQL esterno e disattivare le celle.

- a Copiare i file `global.properties`, `responses.properties`, `certificates` e `proxycertificates` da `/opt/vmware/vcloud-director/etc/` a `/tmp` o in qualsiasi posizione preferita nel database PostgreSQL esterno.

- b Disattivare le celle nell'ambiente esistente.

- 8 Se si desidera che il nuovo ambiente vCloud Director utilizzi il server NFS dell'ambiente esistente, creare ed esportare una nuova directory in questo server NFS come nuovo punto di montaggio NFS condiviso.

Non è possibile riutilizzare il punto di montaggio esistente perché gli ID utente e gruppo (UID/GID) degli utenti nel vecchio NFS potrebbero non coincidere con gli ID utente e gruppo nel nuovo NFS.

- 9 Creare il nuovo gruppo di server distribuendo una o più istanze dell'appliance vCloud Director 9.7.

- Se si desidera utilizzare la funzionalità a disponibilità elevata (HA) del database, distribuire una cella primaria e due celle di standby e, facoltativamente, una o più celle dell'applicazione vCD.
- Se si disattivano le celle nell'ambiente esistente, è possibile utilizzare gli indirizzi IP originali per le nuove celle.
- Se si esporta un nuovo percorso nel server NFS esistente, è possibile utilizzare questo nuovo punto di montaggio condiviso per il nuovo ambiente.

Vedere [Capitolo 6 Distribuzione dell'appliance vCloud Director](#).

- 10 In ogni cella appena distribuita, eseguire il comando per arrestare il servizio vCloud Director.

```
service vmware-vcd stop
```

- 11 Copiare il file di dump dalla cartella `/tmp` nel database PostgreSQL esterno alla cartella `/tmp` nella cella primaria del nuovo ambiente.

Vedere il passaggio 5.

- 12 Modificare le autorizzazioni nel file di dump.

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



- 13 Accedere come **root** alla console della cella primaria appena distribuita e trasferire il database vCloud Director dal database esterno al database integrato.

- a Passare all'utente postgres, connettersi al terminale del database psql ed eseguire l'istruzione per eliminare il database vcloud.

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

- b Se il proprietario del database esterno esistente è diverso da vcloud, creare un utente con il nome annotato nel passaggio 6.

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

- c Eseguire il comando pg\_restore.

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

- d Se il nome del database esterno esistente è diverso da vcloud, sostituirlo con vcloud utilizzando il nome annotato nel passaggio 6.

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

- e Se il proprietario del database dell'ambiente vCloud Director esistente è diverso da vcloud, sostituirlo con vcloud e riassegnare le tabelle a vcloud.

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

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -d vcloud -c 'REASSIGN OWNED BY  
<db_owner_external_pg> TO vcloud;'
```

- 14 In ciascuna cella appena distribuita, eseguire il backup e sostituire i dati di configurazione e riconfigurare e avviare il servizio vCloud Director.

- a Eseguire il backup delle proprietà e dei file dei certificati e copiare e sostituire questi file dalla posizione nel database PostgreSQL esterno dell'origine della migrazione in cui sono stati copiati i file nel passaggio 7a.

I file `global.properties`, `responses.properties`, `certificates` e `proxycertificates` sono disponibili in `/opt/vmware/vcloud-director/etc/`.

---

**Importante** Se si esegue la migrazione a vCloud Director versione 9.7.0.1 o successiva, è inoltre necessario eseguire il backup, la copia e la sostituzione del file `truststore` dall'origine della migrazione, insieme agli altri file.

---

- b Eseguire il backup del file dell'archivio chiavi che si trova in `/opt/vmware/vcloud-director/certificates.ks`.

Non copiare e sostituire con il file di archivio chiavi dall'origine della migrazione.

- c Eseguire il comando per riconfigurare il servizio vCloud Director.

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

Dove:

- Il valore `--keystore-password` corrisponde alla password **root** iniziale di questa appliance.
- Il valore `--database-password` corrisponde alla password del database impostata durante la distribuzione dell'appliance.
- Il valore `--database-host` corrisponde all'indirizzo IP di rete eth1 dell'appliance primaria.
- Il valore `--primary-ip` corrisponde all'indirizzo IP di rete eth0 dell'appliance.
- Il valore `--console-proxy-ip` corrisponde all'indirizzo IP di rete eth0 dell'appliance.
- Il valore `--console-proxy-port` corrisponde alla porta del proxy della console dell'appliance 8443.

Per informazioni sulla risoluzione dei problemi, vedere [La riconfigurazione del servizio vCloud Director non riesce durante la migrazione o il ripristino dell'appliance vCloud Director](#).

- d Eseguire il comando per avviare il servizio vCloud Director.

```
service vmware-vcd start
```

È possibile monitorare l'avanzamento dell'avvio della cella in `/opt/vmware/vcloud-director/logs/cell.log`.

- 15 Dopo aver completato il processo di avvio di tutte le celle del nuovo gruppo di server, verificare che la migrazione dell'ambiente vCloud Director sia stata eseguita correttamente.
  - a Aprire vCloud Director Web Console utilizzando l'indirizzo IP di rete eth0 di una cella del nuovo gruppo di server, `https://et0_IP_new_cell/cloud`.
  - b Accedere a vCloud Director Web Console con le credenziali dell'**amministratore di sistema** esistenti.
  - c Verificare che le risorse vSphere e cloud siano disponibili nel nuovo ambiente.
- 16 Dopo aver verificato correttamente la migrazione di vCloud Director, utilizzare vCloud Director Web Console per eliminare le celle disconnesse che appartengono al vecchio ambiente vCloud Director.
  - a Nella scheda **Gestisci e monitora**, fare clic su **Celle cloud**.

- b Fare clic con il pulsante destro del mouse sul nome di una cella e scegliere **Elimina**.

È possibile distribuire l'appliance vCloud Director per aggiungere membri al gruppo di server dell'ambiente migrato.

## Operazioni successive

Il nuovo ambiente dell'appliance vCloud Director migrato utilizza certificati autofirmati. Per utilizzare i certificati firmati correttamente dall'ambiente precedente in ogni cella del nuovo ambiente eseguire i passaggi seguenti:

- 1 Copiare e sostituire il file dell'archivio chiavi dalla cella precedente in `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.
- 2 Eseguire il comando dello strumento di gestione delle celle per sostituire i certificati.

Assicurarsi che `vcloud.vcloud` sia il proprietario di questo file.

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

- 3 Riavviare il servizio vCloud Director.

```
service vmware-vcd restart
```

Se si aggiungono nuovi membri a questo gruppo di server, le nuove celle dell'appliance vengono distribuite con questi certificati firmati correttamente.

# Dopo l'aggiornamento o la migrazione di vCloud Director

# 13

Dopo avere aggiornato o migrato tutti i server vCloud Director e il database condiviso, è possibile aggiornare le istanze di NSX Manager che forniscono i servizi di rete al cloud. Dopo questa operazione, è possibile aggiornare gli host ESXi e le istanze di vCenter Server che sono registrate nell'installazione di vCloud Director.

**Importante** A partire dalla versione 9.7, vCloud Director supporta solo gateway edge avanzati. È necessario convertire un gateway edge non avanzato preesistente in un gateway avanzato. Vedere <https://kb.vmware.com/kb/66767>.

Questo capitolo include i seguenti argomenti:

- [Aggiornamento di ciascun NSX Manager associato a un sistema vCenter Server collegato](#)
- [Aggiornamento dei sistemi vCenter Server, degli host ESXi e degli NSX Edge](#)
- [Nuovi diritti in questa versione](#)

## Aggiornamento di ciascun NSX Manager associato a un sistema vCenter Server collegato

Prima di aggiornare un vCenter Server e gli host ESXi registrati in vCloud Director, è necessario aggiornare ciascuna istanza di NSX Manager associata a vCenter Server.

L'aggiornamento di NSX Manager interrompe l'accesso alle funzioni amministrative di NSX, ma non interrompe i servizi di rete. È possibile aggiornare NSX Manager prima o dopo l'aggiornamento di vCloud Director, indipendentemente dal fatto che vi siano celle di vCloud Director in esecuzione.

Per informazioni sull'aggiornamento di NSX, consultare la documentazione di NSX per vSphere all'indirizzo <https://docs.vmware.com>.

### Procedura

- 1 Aggiornare l'istanza di NSX Manager associata a ogni vCenter Server registrato nell'installazione di vCloud Director in uso.
- 2 Dopo aver eseguito l'aggiornamento di tutte le istanze di NSX Manager, è possibile aggiornare i sistemi vCenter Server e gli host ESXi registrati.

# Aggiornamento dei sistemi vCenter Server, degli host ESXi e degli NSX Edge

Dopo aver aggiornato vCloud Director e NSX Manager, è necessario aggiornare i sistemi vCenter Server e gli host ESXi registrati in vCloud Director. Dopo l'aggiornamento di tutti i sistemi vCenter Server e host ESXi collegati, è possibile aggiornare gli NSX Edge.

## Prerequisiti

Assicurarsi di aver già eseguito l'aggiornamento di tutte le istanze di NSX Manager associate ai sistemi vCenter Server collegati al cloud. Vedere [Aggiornamento di ciascun NSX Manager associato a un sistema vCenter Server collegato](#).

## Procedura

- 1 Disabilitare l'istanza di vCenter Server.
  - a Nella console Web di vCloud Director, fare clic sulla scheda **Gestisci e monitora** e su **vCenter** nel riquadro sinistro.
  - b Fare clic con il pulsante destro del mouse sul nome dell'istanza di vCenter Server di destinazione e scegliere **Disabilita**.
  - c Fare clic su **Sì**.
- 2 Aggiornare il sistema vCenter Server.

Per informazioni, vedere *Aggiornamento di vCenter Server*.
- 3 Verificare tutti gli URL pubblici e le catene di certificati di vCloud Director.
  - a Nella console Web di vCloud Director, fare clic sulla scheda **Amministrazione** e, nel riquadro sinistro, fare clic su **Indirizzi pubblici**.
  - b Verificare tutti gli indirizzi pubblici.
- 4 Aggiornare la registrazione di vCenter Server in vCloud Director.
  - a Nella console Web di vCloud Director, fare clic sulla scheda **Gestisci e monitora** e su **vCenter** nel riquadro sinistro.
  - b Fare clic con il pulsante destro del mouse sul nome dell'istanza di vCenter Server di destinazione e scegliere **Aggiorna**.
  - c Fare clic su **Sì**.

- 5 Eseguire l'aggiornamento di ciascun host ESXi supportato dal sistema vCenter Server aggiornato.

Vedere *Aggiornamento di VMware ESXi*.

---

**Importante** Per assicurarsi di disporre di capacità host aggiornata sufficiente per il supporto delle macchine virtuali nel Cloud, eseguire l'aggiornamento degli host in piccoli batch. In questo modo è possibile completare in tempo gli aggiornamenti dell'agente host per consentire la migrazione delle macchine virtuali di nuovo nell'host aggiornato.

---

- a Utilizzare il sistema vCenter Server per attivare la modalità di manutenzione dell'host e consentire a tutte le macchine virtuali su tale host di eseguire la migrazione a un altro host.
  - b Aggiornare l'host.
  - c Utilizzare il sistema vCenter Server per riconnettere l'host.
  - d Utilizzare il sistema vCenter Server per disattivare la modalità di manutenzione dell'host.
- 6 (Facoltativo) Eseguire l'aggiornamento delle istanze di NSX Edge gestite dall'istanza di NSX Manager associata al sistema vCenter Server aggiornato.

Le istanze di NSX Edge aggiornate consentono di migliorare le prestazioni e l'integrazione. È possibile utilizzare NSX Manager o vCloud Director per aggiornare le istanze di NSX Edge.

- Per informazioni sull'utilizzo di NSX Manager per l'aggiornamento di NSX Edge, consultare la documentazione di NSX per vSphere all'indirizzo <https://docs.vmware.com>.
- Per aggiornare le istanze di NSX Edge tramite vCloud Director, è necessario intervenire sull'oggetto di rete di vCloud Director supportato da Edge:
  - Quando si utilizza la console Web di vCloud Director o l'API di vCloud per reimpostare una rete servita da un gateway edge, l'aggiornamento appropriato di tale gateway edge viene eseguito automaticamente.
  - La redistribuzione di un gateway edge comporta l'aggiornamento dell'appliance di NSX Edge associata.
  - La reimpostazione di una rete di vApp effettuata dall'interno del contesto della vApp comporta l'aggiornamento dell'appliance di NSX Edge associata a tale rete. Per utilizzare la console Web di vCloud Director per reimpostare la rete di vApp dall'interno del contesto di una vApp, passare alla scheda **Rete** della vApp, visualizzare i relativi dettagli di rete, fare clic con il pulsante destro del mouse sulla rete di vApp e selezionare **Reimposta rete**.

Per ulteriori informazioni sulle modalità di redistribuzione dei gateway edge e sulla reimpostazione delle reti di vApp, vedere la guida online della console Web di vCloud Director oppure la *guida alla programmazione dell'API di vCloud*.

## Operazioni successive

Ripetere questa procedura per gli altri sistemi vCenter Server registrati nell'installazione di vCloud Director.

## Nuovi diritti in questa versione

vCloud Director 9.7 include nuovi diritti, che possono essere aggiunti a tutti i ruoli globali esistenti che sono stati pubblicati nei tenant.

Diritto	Descrizione	Ruolo predefinito
<b>SDDC: Visualizza SDDC</b>	Consente di visualizzare tutti gli SDDCs pubblicati nell'organizzazione.  L' <b>amministratore di sistema</b> può visualizzare tutti gli SDDC.	<b>Amministratore di sistema e Amministratore organizzazione</b>
<b>SDDC: Gestisci SDDC</b>	Consente di aggiungere, rimuovere e modificare SDDC.	<b>Amministratore di sistema</b>
<b>SDDC: Gestisci proxy SDDC</b>	Consente di aggiungere, rimuovere, abilitare e disabilitare i proxy SDDC.	<b>Amministratore di sistema</b>
<b>Applicazioni di servizio: Visualizza applicazioni di servizio</b>	Consente di visualizzare l'elenco delle applicazioni di servizio registrate.  Utilizzato per gli account VMC.	<b>Amministratore di sistema</b>
<b>Applicazioni di servizio: Registra VMC SDDC</b>	Consente di creare, visualizzare, modificare e rimuovere le applicazioni di servizio.  Utilizzato per gli account VMC.	<b>Amministratore di sistema</b>
<b>Applicazioni di servizio: Gestisci applicazioni di servizio</b>	Consente di registrare le applicazioni di servizio.  Utilizzato per gli account VMC.	<b>Amministratore di sistema</b>
<b>Cluster edge: Visualizza cluster edge</b>	Consente di visualizzare un elenco di cluster edge e di recuperare un singolo cluster edge.	<b>Amministratore di sistema e Amministratore organizzazione</b>
<b>Cluster edge: Gestisci cluster edge</b>	Consente di creare, modificare e rimuovere i cluster edge.	<b>Amministratore di sistema e Amministratore organizzazione</b>
<b>vApp: Modifica criterio di calcolo della macchina virtuale</b>	Consente agli utenti di modificare il criterio di calcolo di una macchina virtuale.	<b>Amministratore di sistema , Amministratore organizzazione, Autore catalogo e Autore vApp</b>
<b>Gateway: Importa gateway edge</b>	Consente di importare un router di livello 1 come gateway edge.	<b>Amministratore di sistema e Amministratore organizzazione</b>

Per informazioni sulla gestione di diritti e ruoli, vedere *Guida del portale di amministrazione del provider di servizi di vCloud Director*.

# Risoluzione dei problemi relativi all'appliance vCloud Director

# 14

Se la distribuzione dell'appliance vCloud Director non riesce o se l'appliance non funziona correttamente, è possibile esaminare i file di registro dell'appliance per determinare la causa del problema.

Il supporto tecnico di VMware richiede di routine informazioni diagnostiche nella gestione di richieste di supporto. È possibile utilizzare lo script `vmware-vcd-support` per raccogliere informazioni sul registro host e registri di vCloud Director. Per ulteriori informazioni sulla raccolta di informazioni diagnostiche per vCloud Director, vedere <https://kb.vmware.com/s/article/1026312>. Quando si esegue lo script `vmware-vcd-support`, i registri possono includere informazioni sulle celle disattivate o sostituite con stato FAIL. Vedere <https://kb.vmware.com/s/article/71349>.

Questo capitolo include i seguenti argomenti:

- [Esame dei file di registro nell'appliance vCloud Director](#)
- [La cella di vCloud Director non viene avviata dopo la distribuzione dell'appliance](#)
- [La riconfigurazione del servizio vCloud Director non riesce durante la migrazione o il ripristino dell'appliance vCloud Director](#)
- [Utilizzo dei file di registro per risolvere i problemi relativi agli aggiornamenti e alle patch di vCloud Director](#)
- [Il controllo della disponibilità degli aggiornamenti di vCloud Director non riesce](#)
- [L'installazione dell'aggiornamento più recente di vCloud Director non riesce](#)

## Esame dei file di registro nell'appliance vCloud Director

Dopo aver distribuito l'appliance vCloud Director, è possibile esaminare i registri di firstboot e database per individuare gli errori e gli avvisi.

### Procedura

- 1 Accedere direttamente o con SSH alla console dell'appliance vCloud Director come **root**.
- 2 Passare a `/opt/vmware/var/log`.
- 3 Esaminare i file di registro.
  - Il file `firstboot` contiene informazioni di registro relative al primo avvio dell'appliance.



- La directory `/opt/VMware/var/log/VCD/` contiene i registri relativi alla configurazione della suite di strumenti di Replication Manager (repmgr) e alla sincronizzazione della riconfigurazione e dell'appliance.
- La directory `/opt/VMware/var/log/VCD/PG/` contiene i registri relativi al backup del database dell'appliance incorporata.
- Il file `/opt/vmware/etc/vami/ovfEnv.xml` contiene i parametri OVF della distribuzione.

## La cella di vCloud Director non viene avviata dopo la distribuzione dell'appliance

L'appliance vCloud Director è stata distribuita correttamente, ma i servizi vCloud Director potrebbero non avviarsi.

### Problema

Il servizio `vmware-vcd` è inattivo dopo la distribuzione dell'appliance.

### Causa

Se è stata distribuita una cella primaria, i servizi vCloud Director potrebbero non avviarsi a causa di uno storage del servizio di trasferimento condiviso NFS già popolato. Prima di distribuire l'appliance primaria, lo storage del servizio di trasferimento condiviso non deve contenere un file `responses.properties` o una directory `appliance-nodes`.

Se è stata distribuita una cella di applicazione in modalità standby o vCD, i servizi vCloud Director potrebbero non avviarsi a causa di un file `responses.properties` mancante nello storage di trasferimento condiviso NFS. Prima di distribuire un'appliance di applicazioni di standby o vCD, lo storage del servizio di trasferimento condiviso deve contenere il file `responses.properties`.

### Soluzione

- 1 Accedere direttamente o con SSH alla console dell'appliance vCloud Director come **root**.
- 2 Esaminare il file di registro `/opt/vmware/var/log/vcd/setupvcd.log` per i messaggi di errore relativi allo storage NFS.
- 3 Preparare lo storage NFS per il tipo di appliance.
- 4 Ridistribuire la cella.

## La riconfigurazione del servizio vCloud Director non riesce durante la migrazione o il ripristino dell'appliance vCloud Director

Quando si esegue la migrazione o il ripristino dell'appliance vCloud Director, è possibile che l'esecuzione del comando `configure` non riesca.

**Problema**

Durante la procedura per la migrazione o il ripristino di vCloud Director in un nuovo ambiente dell'appliance vCloud Director, eseguire il comando `configure` per riconfigurare il servizio vCloud Director in ogni nuova cella. Il comando `configure` potrebbe non riuscire con il messaggio di errore `sun.security.validator.ValidatorException: convalida percorso PKIX non riuscita: java.security.cert.CertPathValidatorException: controllo della firma non riuscito`.

**Soluzione**

- 1 Nella cella di destinazione, eseguire il comando.

```
sed -i '/vcd_ova.crt/ s/$/ --force /' /opt/vmware/appliance/bin/appliance-sync.sh
```

- 2 Attendere 1 minuto e rieseguire il comando `configure`.

## Utilizzo dei file di registro per risolvere i problemi relativi agli aggiornamenti e alle patch di vCloud Director

Quando si applicano le patch all'appliance vCloud Director, è possibile esaminare i file di registro per controllare eventuali errori e avvisi.

**Problema**

Se il comando `vamicli` restituisce un errore, è possibile utilizzare i file di registro per risolverlo.

**Soluzione**

- 1 Accedere direttamente o tramite SSH alla console dell'appliance vCloud Director come **root**.
- 2 Passare al file di registro appropriato.
  - Se `vamicli update --check` non riesce, passare a `/opt/vmware/var/log/vami/vami.log`.
  - Se `vamicli update --install latest` non riesce, passare a `/opt/vmware/var/log/vami/updatecli.log`.
- 3 Esaminare il file di registro.

## Il controllo della disponibilità degli aggiornamenti di vCloud Director non riesce

Quando si controlla la disponibilità degli aggiornamenti dell'appliance vCloud Director, è possibile che l'esecuzione del comando `vamicli update --check` non riesca.

### Problema

Durante la procedura di applicazione di una patch all'appliance vCloud Director, si esegue il comando `vamicli update --check` per verificare la disponibilità di aggiornamenti. Il comando `vamicli update --check` potrebbe non riuscire con Errore: errore durante il download del manifesto. Contattare il fornitore.

### Causa

Il percorso della directory di aggiornamento del repository non è corretto.

### Soluzione

- 1 Eseguire il comando `vamicli` con il percorso corretto.

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

- 2 Eseguire di nuovo il comando per verificare la disponibilità di aggiornamenti.

```
vamicli update --check
```

## L'installazione dell'aggiornamento più recente di vCloud Director non riesce

Quando si esegue l'installazione degli aggiornamenti più recenti dell'appliance vCloud Director, è possibile che l'esecuzione del comando `vamicli update --install latest` non riesca.

### Problema

Durante la procedura di applicazione di una patch all'appliance vCloud Director, eseguire il comando `vamicli update --install latest` per applicare la patch più recente disponibile. Il comando `vamicli update --install latest` potrebbe non riuscire con Errore: errore durante l'esecuzione dell'installazione del pacchetto

### Causa

L'errore si verifica quando il server NFS non è accessibile.

### Soluzione

- 1 Verificare che il server NFS montato in `/opt/vmware/vcloud-director/data/transfer` sia accessibile.
- 2 Eseguire di nuovo il comando per applicare la patch disponibile.

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

# Disinstallazione del software vCloud Director

# 15

Utilizzare il comando `rpm` di Linux per disinstallare il software vCloud Director da un singolo server.

## Procedura

- 1 Eseguire il login al server di destinazione come utente **root**.
- 2 Smontare lo storage del servizio di trasferimento, generalmente montato nel percorso `/opt/vmware/vcloud-director/data/transfer`.
- 3 Aprire una finestra della console, della shell o del terminale ed eseguire il comando `rpm` di Linux.

```
rpm -e vmware-phonehome vmware-vcloud-director vmware-vcloud-director-rhel
```

Qualora altri pacchetti installati dipendano da quello di `vmware-vcloud-director`, il sistema richiede di disinstallarli prima di procedere con la disinstallazione di vCloud Director.