

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

19 SET 2019

VMware Cloud Director 10.0

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

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

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

- 1** Panoramica delle operazioni di installazione, configurazione e aggiornamento di vCloud Director 8
 - Architettura di vCloud Director 8
 - Pianificazione della configurazione 10
- 2** Requisiti hardware e software di vCloud Director 11
 - Requisiti di configurazione di rete per vCloud Director 12
 - Requisiti di sicurezza della rete 13
- 3** Prima dell'installazione di vCloud Director o della distribuzione dell'appliance vCloud Director 16
 - Configurazione di un database PostgreSQL esterno per vCloud Director su Linux 16
 - Preparazione dello storage del server di trasferimento 18
 - Installazione e configurazione di un broker AMQP RabbitMQ 20
 - Download e installazione della chiave pubblica VMware 21
 - Installazione e configurazione di NSX Data Center for vSphere per vCloud Director 22
 - Installazione e configurazione di NSX-T Data Center per vCloud Director 23
- 4** Creazione e gestione di certificati SSL per vCloud Director in Linux 25
 - Prima di creare certificati SSL per vCloud Director in Linux 25
 - Creazione di certificati SSL autofirmati per vCloud Director in Linux 26
 - Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione per vCloud Director in Linux 27
 - Creazione di un archivio chiavi del certificato SSL firmato da un'autorità di certificazione con chiavi private importate per vCloud Director in Linux 31
- 5** Installazione di vCloud Director in Linux 33
 - Installazione di vCloud Director nel primo membro di un gruppo di server 34
 - Configurazione delle connessioni di rete e database 36
 - Riferimento alla configurazione interattiva 38
 - Riferimenti per la configurazione automatica 39
 - Protezione e riutilizzo del file di risposta 43
 - Installazione di vCloud Director in un membro aggiuntivo di un gruppo di server 44
- 6** Distribuzione dell'appliance vCloud Director 47
 - Distribuzioni dell'appliance e configurazione della disponibilità elevata del database 49

Prerequisiti per la distribuzione dell'appliance di vCloud Director	52
Distribuzione dell'appliance vCloud Director tramite vSphere Client	53
Linee guida per il dimensionamento dell'appliance vCloud Director	54
Avviamento della distribuzione dell'appliance vCloud Director	59
Personalizzazione dell'appliance di vCloud Director e completamento della distribuzione	61
Distribuzione dell'appliance vCloud Director tramite VMware OVF Tool	63
7 Creazione e gestione di certificati SSL dell'appliance vCloud Director	71
Distribuzione dell'appliance vCloud Director con certificati con caratteri jolly firmati per la comunicazione HTTPS e proxy console	71
Creazione e importazione di certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director	73
Importazione di chiavi private e certificati SSL firmati dall'autorità di certificazione nell'appliance di vCloud Director	77
Sostituzione di un certificato autofirmato dell'interfaccia utente di gestione dell'appliance vCloud Director e di un database PostgreSQL incorporato	79
Rinnovo dei certificati dell'appliance vCloud Director	80
8 Configurazione dell'appliance vCloud Director	82
Visualizzazione dello stato delle celle in un cluster ad alta disponibilità del database	82
Ripristino da un errore di database primario in un cluster ad alta disponibilità	83
Ripristino da un errore di cella di standby in un cluster a disponibilità elevata	84
Backup e ripristino del database integrato dell'appliance vCloud Director	85
Backup del database incorporato dell'appliance vCloud Director	85
Ripristino di un ambiente dell'appliance vCloud Director con una configurazione del database ad alta disponibilità	86
Configurazione dell'accesso esterno al database di vCloud Director	89
Abilitazione o disabilitazione dell'accesso SSH all'appliance di vCloud Director	89
Modifica delle impostazioni DNS dell'appliance vCloud Director	90
Modifica delle route statiche per le interfacce di rete dell'appliance vCloud Director	91
Script di configurazione nell'appliance vCloud Director	92
Aumento della capacità del database PostgreSQL incorporato in un'appliance vCloud Director	93
Modifica delle configurazioni di PostgreSQL nell'appliance di vCloud Director	94
9 Utilizzo di Replication Manager Tool Suite in una configurazione di cluster a disponibilità elevata	96
Verifica dello stato di connettività di un cluster a disponibilità elevata del database	97
Verifica dello stato di replica di un nodo in un cluster a disponibilità elevata del database	98
Verifica dello stato di un cluster a disponibilità elevata del database	99
Rilevamento di un precedente nodo primario che torna online in un cluster a disponibilità elevata	100
Scambio dei ruoli tra cella primaria e cella di standby in un cluster a disponibilità elevata del database	102

Annullamento della registrazione di un nodo di standby non riuscito o irraggiungibile in un cluster a disponibilità elevata del database 103

Annullamento della registrazione di una cella primaria non riuscita in un cluster a disponibilità elevata del database 104

Annullamento della registrazione di una cella di standby in esecuzione in un cluster a disponibilità elevata del database 105

10 Guida di riferimento allo strumento di gestione delle celle 107

Configurazione di un'installazione di vCloud Director 111

Abilitazione di vCloud Director Web Console 113

Disabilitazione dell'accesso del provider di servizi all'endpoint API legacy 115

Gestione di una cella 116

Gestione delle applicazioni della cella 117

Aggiornamento delle proprietà di connessione del database 119

Rilevamento e riparazione dei dati danneggiati dello scheduler 122

Generazione di certificati autofirmati per gli endpoint proxy della console e HTTP 123

Sostituzione di certificati per gli endpoint proxy della console e HTTP 124

Importazione di certificati SSL da servizi esterni 126

Gestione dell'elenco di crittografia SSL consentita 127

Gestione dell'elenco dei protocolli SSL consentiti 129

Configurazione della raccolta di metriche 131

Configurazione di un database delle metriche Cassandra 134

Recupero della password dell'amministratore di sistema 136

Aggiornamento dello stato di errore di un task 137

Configurazione della gestione dei messaggi di controllo 138

Configurazione dei modelli e-mail 139

Individuazione di macchine virtuali orfane 141

Attivazione o disattivazione della partecipazione al programma CEIP VMware 143

Aggiornamento delle impostazioni di configurazione dell'applicazione 144

Configurazione della limitazione della sincronizzazione del catalogo 144

Risoluzione dei problemi relativi all'accesso non riuscito all'interfaccia utente di vCloud Director 146

Debug dell'individuazione delle macchine virtuali vCenter 147

Rigenerazione degli indirizzi MAC per reti estese multisito 148

Aggiornamento degli indirizzi IP del database nelle celle di vCloud Director 151

11 Dopo avere installato vCloud Director o distribuito l'appliance vCloud Director 153

Installazione dei file Microsoft Sysprep nei server 153

Modifica del fuso orario dell'appliance di vCloud Director 155

Personalizzazione degli indirizzi pubblici 155

Installazione e configurazione di un database Cassandra per l'archiviazione dei dati relativi alle metriche cronologiche 157

	Esecuzione di configurazioni aggiuntive nel database PostgreSQL esterno	158
12	Eseguire l'aggiornamento di vCloud Director	160
	Aggiornamento dell'appliance vCloud Director	164
	Rollback di un'appliance di vCloud Director quando un aggiornamento non riesce	167
	Aggiornamento dell'appliance vCloud Director mediante il repository di aggiornamento di VMware	168
	Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director	170
	Aggiornamento manuale di un'installazione di vCloud Director	173
	Aggiornamento di una cella di vCloud Director	174
	Esecuzione dell'aggiornamento del database vCloud Director	176
	Riferimento dell'utilità di aggiornamento del database	178
13	Migrazione all'appliance vCloud Director	181
	Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director	181
14	Dopo l'aggiornamento o la migrazione di vCloud Director	187
	Aggiornamento di ciascun NSX Manager associato a un sistema vCenter Server collegato	187
	Aggiornamento dei sistemi vCenter Server, degli host ESXi e degli NSX Edge	188
15	Visualizzazione dei registri di vCloud Director	191
16	Risoluzione dei problemi relativi all'appliance vCloud Director	193
	Esame dei file di registro nell'appliance vCloud Director	193
	La cella di vCloud Director non viene avviata dopo la distribuzione dell'appliance	194
	La riconfigurazione del servizio vCloud Director non riesce durante la migrazione o il ripristino dell'appliance vCloud Director	194
	Utilizzo dei file di registro per risolvere i problemi relativi agli aggiornamenti e alle patch di vCloud Director	195
	Il controllo della disponibilità degli aggiornamenti di vCloud Director non riesce	195
	L'installazione dell'aggiornamento più recente di vCloud Director non riesce	196
17	Disinstallazione del software vCloud Director	197

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[®] for Service Providers e sulla sua configurazione per l'utilizzo con VMware vSphere[®], VMware NSX[®] for vSphere[®] e VMware NSX-T[™] 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.

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

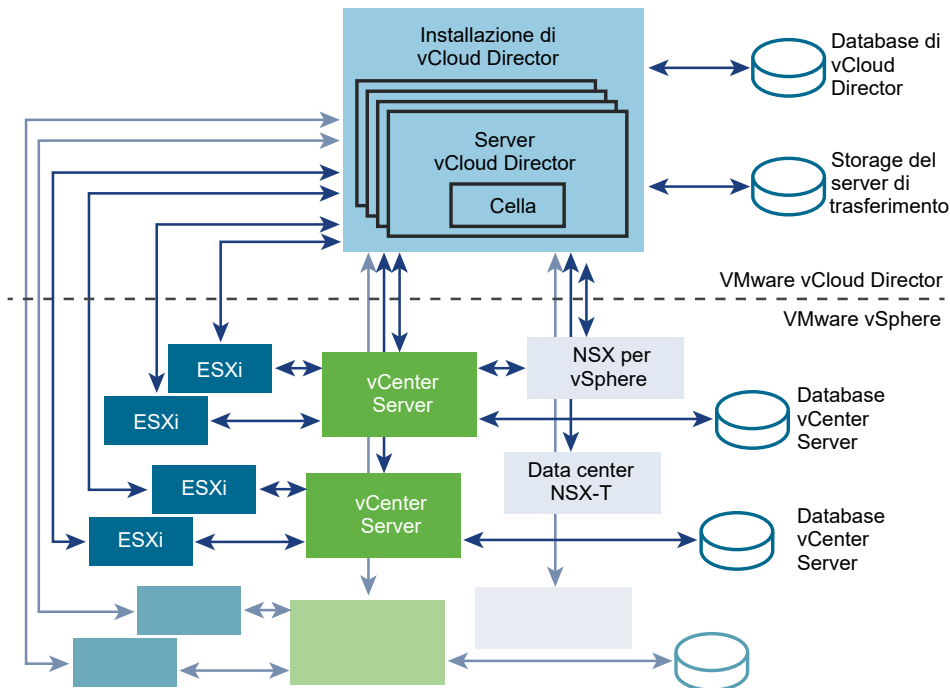
Un gruppo di server vCloud Director è costituito da uno o più server vCloud Director installati su Linux o distribuzioni dell'appliance di vCloud Director. Su ogni server del gruppo viene eseguita una raccolta di servizi denominata cella vCloud Director. Tutte le celle condividono un singolo database 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[®] e agli host VMware ESXi[™] 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 o NSX-T Manager.

Per informazioni sull'aggiunta di vSphere e delle risorse di rete, vedere *Guida del portale di amministrazione del provider di servizi 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 [Configurazione di un database PostgreSQL esterno per vCloud Director su Linux](#).

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.

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 10.0* 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 10.0*.

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 da Service Provider Admin Portal. 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.

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

Porta	Protocollo	Commenti
5432	TCP	Porta di database PostgreSQL predefinita
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:

- [Configurazione di un database PostgreSQL esterno per vCloud Director su Linux](#)
- [Preparazione dello storage del server di trasferimento](#)
- [Installazione e configurazione di un broker AMQP RabbitMQ](#)
- [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](#)

Configurazione di un database PostgreSQL esterno per vCloud Director su Linux

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'istanza del database PostgreSQL e creare l'account utente del database di vCloud Director.

I database PostgreSQL hanno requisiti di configurazione specifici quando vengono utilizzati con vCloud Director.

È necessario creare uno schema di database dedicato separato per vCloud Director da utilizzare. vCloud Director non può infatti condividere uno schema di database con altri prodotti VMware.

vCloud Director supporta connessioni SSL solo al 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](#).

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

Prerequisiti

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

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](#).

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.

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 Dal menu principale () del vCloud Director Service Provider Admin Portal, selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Impostazioni**, fare clic su **Estendibilità**.
- 3 Fare clic su **Estendibilità**, quindi fare clic su **Modifica** per la sezione **Broker AMQP**.
- 4 Attivare l'opzione **Usa SSL**.
- 5 Attivare l'opzione **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

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 per 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. 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 12 Eseguire l'aggiornamento 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.

Importante Per configurare gli oggetti e gli strumenti di NSX-T Data Center, utilizzare l'interfaccia utente semplificata dei criteri e le API dei criteri corrispondenti all'interfaccia utente semplificata. Per ulteriori informazioni, vedere la panoramica di NSX-T Manager in *Guida all'amministrazione di NSX-T Data Center*.

Per le informazioni più aggiornate sulla compatibilità tra vCloud Director e gli altri prodotti VMware, vedere le [Matrici di interoperabilità dei prodotti VMware](#).

Per informazioni sui requisiti di rete, vedere [Requisiti di configurazione di rete per vCloud Director](#).

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 12 Eseguire l'aggiornamento di vCloud Director](#).

Prerequisiti

Acquisire familiarità con NSX-T Data Center.

Procedura

- 1 Distribuire e configurare le appliance virtuali di NSX-T Manager.

Per ulteriori informazioni sulla distribuzione di NSX-T Manager, vedere *Guida all'installazione di NSX-T Data Center*.

- 2 Creare le zone di trasporto in base ai requisiti di rete.

Per ulteriori informazioni sulla creazione delle zone di trasporto, vedere *Guida all'installazione di NSX-T Data Center*.

Nota

- 3 Distribuire e configurare i nodi edge e un cluster edge.

Per ulteriori informazioni sulla creazione di NSX Edge, vedere *Guida all'installazione di NSX-T Data Center*.

- 4 Configurare i nodi di trasporto dell'host ESXi.

Per ulteriori informazioni sulla configurazione di un nodo di trasporto dell'host gestito, vedere *Guida all'installazione di NSX-T Data Center*.

- 5 Creare un gateway di livello 0.

Per ulteriori informazioni sulla creazione di un livello 0, vedere *Guida all'amministrazione di NSX-T Data Center*.

Operazioni successive

Dopo aver installato vCloud Director, è possibile:

- 1 Registrare l'istanza di NSX-T Manager nel cloud.

Per informazioni sulla registrazione di un'istanza di NSX-T Manager, vedere *Guida del portale di amministrazione del provider di servizi di vCloud Director*.

- 2 Creare un pool di reti supportato da una zona di trasporto NSX-T Data Center

Per ulteriori informazioni sulla creazione di un pool di reti supportato da una zona di trasporto NSX-T Data Center, vedere *Guida del portale di amministrazione del provider di servizi di vCloud Director*.

- 3 Importare il gateway di livello 0 come rete esterna.

Per ulteriori informazioni sull'aggiunta di una rete esterna supportata da un router logico NSX-T Data Center di livello 0, vedere *Guida del portale di amministrazione del provider di servizi di vCloud Director*.

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 HTTP](#).
- 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 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 12 Eseguire l'aggiornamento 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 [Configurazione di un database PostgreSQL esterno per vCloud Director su Linux](#). 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.

Operazioni successive

Utilizzare il comando di impostazione del sistema dello strumento di gestione delle celle per inizializzare il database del gruppo di server con un account di amministratore di sistema e le informazioni correlate. Vedere [Configurazione di un'installazione 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 file-installazione
```

- 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'utilizzo dello strumento di gestione delle celle, vedere [Capitolo 10 Guida di riferimento allo strumento di gestione delle celle](#).

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/configure options -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. Nota 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 Prima di creare certificati SSL per vCloud Director in Linux .
Password della chiave privata per il certificato SSL HTTP	Vedere Prima di creare certificati SSL per vCloud Director in Linux .
Password della chiave privata per il certificato SSL proxy della console	Vedere Prima di creare certificati SSL per vCloud Director in Linux .

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"> ■ Per ignorare, premere INVIO. ■ Per abilitare, immettere l'indirizzo IP o il nome host di syslog.
Se è abilitata la registrazione di controllo remoto, porta UDP dell'host syslog	L'impostazione predefinita è 514.
Nome host o indirizzo IP del server di database	Server che esegue il database.
Porta del database	L'impostazione predefinita è 5432.
Nome database	L'impostazione predefinita è vcloud.
Nome utente del database	Vedere Configurazione di un database PostgreSQL esterno per vCloud Director su Linux .
Password database	Vedere Configurazione di un database PostgreSQL esterno per vCloud Director su Linux .
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 http://www.vmware.com/trustvmware/ceip.html. 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 Capitolo 10 Guida di riferimento allo strumento di gestione delle celle.</p> <p>Per partecipare al programma, immettere y.</p> <p>Se non si desidera partecipare al programma CEIP di VMware, immettere n.</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>	È possibile configurare il database PostgreSQL in modo che richieda una connessione SSL firmata correttamente da vCloud Director. Se si desidera configurare il database PostgreSQL per utilizzare un certificato autofirmato o privato, vedere Esecuzione di configurazioni aggiuntive nel database PostgreSQL esterno .
<code>--database-host (-dbhost)</code>	Indirizzo IP o nome di dominio completo dell'host database di vCloud Director	Vedere Configurazione di un database PostgreSQL esterno per vCloud Director su Linux .
<code>--database-name (-dbname)</code>	Il nome del servizio di database	Vedere Configurazione di un database PostgreSQL esterno per vCloud Director su Linux .
<code>--database-password (-dbpassword)</code>	Password per l'utente del database. Può essere nulla.	Vedere Configurazione di un database PostgreSQL esterno per vCloud Director su Linux .
<code>--database-port (-dbport)</code>	Numero di porta utilizzato dal servizio di database sull'host database	Vedere Configurazione di un database PostgreSQL esterno per vCloud Director su Linux .

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

Opzione	Argomento	Descrizione
<code>--database-type (-dbtype)</code>	Il tipo di database. Il tipo supportato è postgres.	Facoltativa. Il tipo di database sarà impostato come predefinito su postgres. Vedere Configurazione di un database PostgreSQL esterno per vCloud Director su Linux .
<code>--database-user (-dbuser)</code>	Il nome utente dell'utente del database.	Vedere Configurazione di un database PostgreSQL esterno per vCloud Director su Linux .
<code>--enable-ceip</code>	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 http://www.vmware.com/trustvmware/ceip.html . 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 Capitolo 10 Guida di riferimento allo strumento di gestione delle celle .
<code>--uuid (-g)</code>	Nessuno	Genera un nuovo identificatore univoco per la cella
<code>--primary-ip (-ip)</code>	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> .
<code>--primary-port-http</code>	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
<code>--primary-port-https</code>	Numero intero compreso nell'intervallo 0-65535	Numero della porta da utilizzare per le connessioni HTTPS (protette) al servizio interfaccia Web di vCloud Director
<code>--keystore (-k)</code>	Percorso dell'archivio chiavi Java contenente i certificati SSL e le chiavi private	Il nome del percorso deve essere completo. Ad esempio, <i>/opt/keystore/certificates.ks</i> .

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

Opzione	Argomento	Descrizione
<code>--syslog-host (-loghost)</code>	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 <code>syslog</code> , oltre che al database di vCloud Director.
<code>--syslog-port (-logport)</code>	Numero intero compreso nell'intervallo 0-65535	La porta sulla quale il processo <code>syslog</code> monitora il server specificato. Se non diversamente specificato, il valore predefinito è 514.
<code>--response-file (-r)</code>	Percorso del file di risposta	Il nome del percorso deve essere completo. Se non diversamente specificato, il valore predefinito è <code>/opt/vmware/vcloud-director/etc/responses.properties</code> . Tutte le informazioni fornite quando si esegue la configurazione vengono salvate in questo file. Importante 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.
<code>--unattended-installation (-unattended)</code>	Nessuno	Specifica l'installazione automatica.
<code>--keystore-password (-w)</code>	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 postgres -dbhost 10.150.10.78 -dbname postgresql-db-name -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 postgres -dbhost 10.150.10.78 -dbname postgresql-db-name \
-dbuser vcloud -dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true --unattended
```

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 file-installazione
```

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 utilizzando lo strumento di gestione delle celle con il sottocomando `system-setup`. Vedere [Configurazione di un'installazione 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. Distribuire l'appliance vCloud Director tramite vSphere Client (HTML5) 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.

Nota Le reti eth0 e eth1 devono trovarsi in subnet separate.

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

Dopo la creazione dell'appliance vCloud Director, è possibile utilizzare le funzionalità di rete di vSphere per aggiungere una nuova scheda interfaccia di rete (NIC). Vedere l'argomento sull'[aggiunta di una scheda di rete a una macchina virtuale](#) nella guida *Amministrazione delle macchine virtuali vSphere*.

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

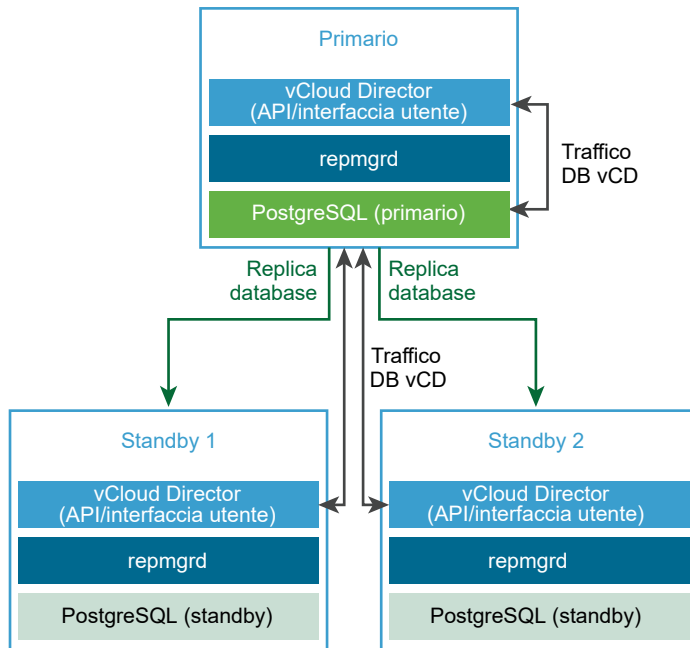
Distribuzioni dell'appliance e configurazione della disponibilità elevata del database

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 tramite 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** al vCloud Director Service Provider Admin Portal all'indirizzo `https://primary_eth0_ip_address/provider`.
- 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.

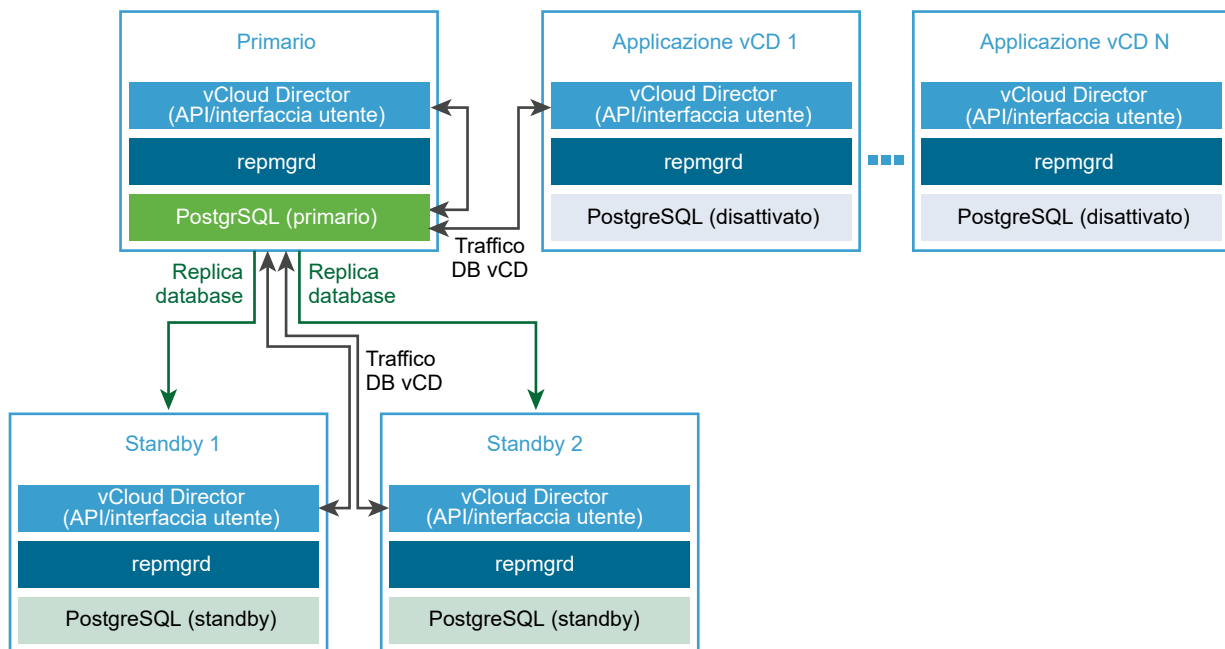
Nota Dopo la distribuzione iniziale dell'appliance di standby, Replication Manager inizia a sincronizzare il proprio database con il database dell'appliance primaria. Durante questo periodo, il database di vCloud Director e quindi l'interfaccia utente di vCloud Director non sono disponibili.

- 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 vCloud Director.

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



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

Nota È possibile distribuire un cluster di vCloud Director con una cella primaria e nessuna cella di standby o dell'applicazione. VMware non fornisce supporto per le distribuzioni con una cella singola in un ambiente di produzione perché rappresentano una singola origine di errore dal punto di vista del database. Le distribuzioni con una cella singola non ricevono il supporto per i problemi relativi alle prestazioni o alla stabilità.

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.

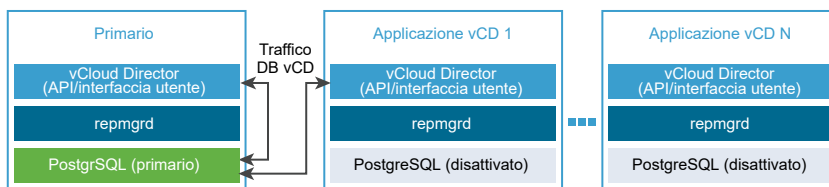
La cella primaria è il primo membro del gruppo di server di vCloud Director. Il database incorporato è configurato come database di vCloud Director. Il nome del database è `vcld` e l'utente del database è `vcld`.

- 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** al vCloud Director Service Provider Admin Portal all'indirizzo `https://primary_eth0_ip_address/provider`.
 - 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 tramite 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 tramite vSphere Client

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

Quando si aggiungono appliance aggiuntive o sostitutive a un cluster di database, la vCPU e la RAM devono corrispondere a quelle delle celle primarie e di standby esistenti nel cluster.

La versione OVA della cella di standby appena distribuita deve essere identica a quella delle appliance esistenti nel cluster. Per visualizzare la versione delle appliance in esecuzione, vedere Informazioni nell'interfaccia utente di gestione dell'appliance. L'appliance viene distribuita con un nome nel formato VMware Cloud 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 Cloud Director-10.0.0.0-9229800_OVA10.ova.

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 Linee guida per il dimensionamento dell'appliance vCloud Director

In base alle proprie esigenze, è possibile avere configurazioni diverse del gruppo di server basato sull'appliance vCloud Director e dimensioni diverse delle istanze della virtual appliance vCloud Director.

2 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).

3 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 indirizzi pubblici](#).
- Per aggiungere membri al gruppo di server vCloud Director, ripetere la procedura.
- Per immettere la chiave di licenza, accedere al vCloud Director Service Provider Admin Portal.
- 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](#).

Linee guida per il dimensionamento dell'appliance vCloud Director

In base alle proprie esigenze, è possibile avere configurazioni diverse del gruppo di server basato sull'appliance vCloud Director e dimensioni diverse delle istanze della virtual appliance vCloud Director.

Panoramica

Per assicurarsi che il cluster possa supportare un failover automatico in caso di errore della cella primaria, la distribuzione minima di vCloud Director deve essere costituita da una cella primaria e da due celle di standby. L'ambiente rimane disponibile in qualsiasi scenario di errore in cui una delle celle passa offline per un motivo qualsiasi. Se si verifica un errore della cella di standby, finché non si ridistribuisce la cella in cui si è verificato l'errore, il cluster è completamente funzionante con qualche peggioramento delle prestazioni. Vedere [Distribuzioni dell'appliance e configurazione della disponibilità elevata del database](#).

L'appliance vCloud Director ha quattro dimensioni che è possibile selezionare durante la distribuzione: Piccola, Media, Grande e Molto grande (VVD). La dimensione dell'appliance Piccola è adatta per la valutazione di laboratorio e questo documento non fornisce istruzioni sulla configurazione di questo tipo di appliance. La tabella delle opzioni di dimensionamento fornisce le specifiche per le opzioni rimanenti e i casi d'uso più adatti per un ambiente di produzione. La configurazione Molto grande corrisponde al profilo di scalabilità [VMware Validated Designs \(VVD\) for Cloud Providers](#).

Per creare dimensioni personalizzate più grandi, gli **amministratori di sistema** possono modificare le dimensioni delle celle distribuite.

La configurazione minima consigliata per le distribuzioni di produzione è una distribuzione di tre nodi di appliance virtuali di dimensioni medie.

Nota È possibile distribuire un cluster di vCloud Director con una cella primaria e nessuna cella di standby o dell'applicazione. VMware non fornisce supporto per le distribuzioni con una cella singola in un ambiente di produzione perché rappresentano una singola origine di errore dal punto di vista del database. Le distribuzioni con una cella singola non ricevono il supporto per i problemi relativi alle prestazioni o alla stabilità.

Opzioni di dimensionamento dell'appliance vCloud Director

È possibile utilizzare le linee guida seguenti per stimare le dimensioni dell'appliance per il proprio ambiente.

	Media	Grande	Molto grande (VVD)
Casi d'uso consigliati	Ambienti di produzione piccoli o di laboratorio	Ambiente di produzione	Produzione con integrazioni API e monitoraggio
Distribuzione di vRealize Operations Management Pack nell'ambiente di vCloud Director	No	No	Sì
Abilitazione delle metriche delle macchine virtuali Cassandra in vCloud Director	No	No	Sì
Numero approssimato di utenti o client che accedono all'API contemporaneamente per un periodo di picco di 30 minuti.	< 50	< 100	< 100
Macchine virtuali gestite	5000	5000	15000

Definizioni di configurazione

Nota Per impostazione predefinita, le appliance `primary-large` e `standby-large` di vCloud Director 9.7 e versioni successive non dispongono delle 16 vCPU necessarie per una configurazione di cluster a disponibilità elevata di grandi dimensioni. Se si desidera disporre di una configurazione dell'appliance di vCloud Director di grandi dimensioni, dopo la distribuzione è necessario impostare manualmente le vCPU della cella primaria e di standby su 16.

	Media	Grande	Molto grande (VVD)
Configurazione cluster HA	1 cella primaria + 2 celle di standby	1 cella primaria + 2 celle di standby + 1 cella dell'applicazione	1 cella primaria + 2 celle di standby + 2 celle dell'applicazione
Cella primaria o di standby vCPU	8	16	24

	Media	Grande	Molto grande (VVD)
Cella dell'applicazione vCPU	N/D	8	8
Cella primaria o di standby RAM	16 GB	24 GB	32 GB
Cella dell'applicazione RAM	N/D	8	8
Rapporto tra vCPU e core fisici	1:1	1:1	1:1
Personalizzazione di PostgreSQL nelle celle primarie e di standby	shared_buffers = '3GB'; effective_cache_size = '9GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '8';	shared_buffers = '5GB'; effective_cache_size = '15GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '16';	shared_buffers = '7GB'; effective_cache_size = '21GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '24';

Come stabilire se le dimensioni del sistema sono insufficienti

In una cella vCloud Director, l'uso della CPU o della memoria aumenta fino a raggiungere un livello elevato, ovvero quasi vicino alla capacità massima. La cella di vCloud Director potrebbe inoltre perdere la connessione al database.

Come stabilire se il numero di celle del sistema è insufficiente

Nei file `vcloud-container-debug.log` e `cell-runtime.log` di tutte le celle di vCloud Director sono presenti voci simili a `rg.apache.apache.tomcat.jdbc.pool.PoolExcatetedException: [pool-jetty-XXXXX] Timeout: Pool empty. Unable to fetch a connection in 20 seconds, none available`. La cella di vCloud Director potrebbe inoltre perdere la connessione al database.

Nota In base alla configurazione della connessione del database predefinita, tutte le configurazioni sono limitate a un massimo di 6 celle di tipo primario, standby e applicazione.

Come personalizzare il dimensionamento dell'appliance

Per personalizzare il dimensionamento dell'appliance di vCloud Director con una delle configurazioni personalizzate, dopo aver eseguito lo strumento di distribuzione dell'appliance di vCloud Director, è necessario eseguire questa procedura in tutte le celle.

- 1 Verificare di disporre del numero di celle necessario per la configurazione selezionata.
- 2 Modificare la memoria e la vCPU di tutte le celle in modo che corrisponda alla configurazione supportata desiderata.

Importante La quantità di RAM e vCPU deve essere la stessa per tutte le celle primarie e di standby.

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

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

- 5 Aggiornare il file di configurazione postgresql.auto.conf eseguendo i comandi seguenti.

Tipo di configurazione	Descrizione
Media	<pre>psql -c "ALTER SYSTEM set shared_buffers = '3GB';" psql -c "ALTER SYSTEM set effective_cache_size = '9GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '8';"</pre>
Grande	<pre>psql -c "ALTER SYSTEM set shared_buffers = '5GB';" psql -c "ALTER SYSTEM set effective_cache_size = '15GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '16';"</pre>
Molto grande	<pre>psql -c "ALTER SYSTEM set shared_buffers = '7GB';" psql -c "ALTER SYSTEM set effective_cache_size = '21GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '24';"</pre>

- 6 Tornare all'utente **root** eseguendo il comando exit.
- 7 Riavviare il processo vpostgres.

```
systemctl restart vpostgres
```

- 8 Impostare di nuovo l'utente su **postgres**.

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

- 9 Per ogni nodo di standby, copiare il file `postgresql.auto.conf` nel nodo e riavviare il processo `vpostgres`.

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

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

- b Riavviare il processo `vpostgres`.

```
systemctl restart vpostgres
```

Per personalizzare il dimensionamento dell'appliance vCloud Director con una configurazione personalizzata, dopo aver eseguito lo strumento di distribuzione dell'appliance vCloud Director, è necessario eseguire questa procedura in tutte le celle.

- 1 Accedere direttamente o tramite un client SSH al sistema operativo dell'appliance primaria come **root**.
- 2 Per visualizzare e annotare le informazioni sulla vCPU, eseguire il comando seguente.

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

- 3 Per visualizzare e annotare le informazioni sulla RAM, eseguire il comando seguente.

La RAM indicata di seguito è in KB ed è necessario convertirla in GB dividendola per 1024000.

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

- 4 Calcolare il valore `shared_buffers` in modo che corrisponda a un quarto della RAM totale meno 4 GB.

$shared_buffers = 0,25 * (RAM\ totale - 4\ GB)$

- 5 Calcolare il valore `effective_cache_size` in modo che corrisponda a tre quarti della RAM totale meno 4 GB.

$effective_cache_size = 0,75 * (RAM\ totale - 4\ GB)$

- 6 Calcolare il valore `max_worker_processes` che è il numero di vCPU.

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

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

- 8 Aggiornare il file di configurazione `postgresql.auto.conf` eseguendo i comandi seguenti e sostituendo i valori calcolati.

```
psql -c "ALTER SYSTEM set shared_buffers = 'shared_buffers value';"
psql -c "ALTER SYSTEM set effective_cache_size = 'effective_cache_size value';"
psql -c "ALTER SYSTEM set work_mem = '8MB';"
psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"
psql -c "ALTER SYSTEM set max_worker_processes= 'max_worker_processes value';"
```

9 Tornare all'utente **root** eseguendo il comando `exit`.

10 Riavviare il processo `vpostgres`.

```
systemctl restart vpostgres
```

11 Impostare di nuovo l'utente su **postgres**.

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

12 Per ogni nodo di standby, copiare il file `postgresql.auto.conf` nel nodo e riavviare il processo `vpostgres`.

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

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

b Riavviare il processo `vpostgres`.

```
systemctl restart vpostgres
```

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
Primaria-piccola	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.
Primaria-grande	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.
Standby-piccola	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.
Standby-grande	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.
Applicazione cella vCD	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.

Importante Le due reti di destinazione devono essere diverse.

- 10 Nei menu a discesa **Impostazioni allocazione IP**, selezionare l'allocazione IP **Statica - Manuale** e quindi il 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
Server NTP	Nome host o indirizzo IP del server NTP da utilizzare.
Password root iniziale	<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>Importante 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>Nota La procedura guidata di distribuzione OVF non convalida la password root iniziale rispetto ai criteri della password.</p> <hr/>
Scadenza password root al primo accesso	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
Abilita SSH	Disabilitata per impostazione predefinita.
Montaggio NFS per il percorso del trasferimento file	Vedere Preparazione dello storage del server di trasferimento .

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
Password DB "vcloud" per l'utente "vcloud"	La password dell'utente del database vcloud .
Nome utente amministratore	Nome utente per l'account dell' amministratore di sistema . Impostazione predefinita: administrator.
Nome completo amministratore	Nome completo dell' amministratore di sistema . Impostazione predefinita: vCD Admin.
Password utente amministratore	Password dell'account dell' amministratore di sistema .
E-mail amministratore	Indirizzo e-mail dell' amministratore di sistema .
Nome sistema	Nome della cartella di vCenter Server da creare per questa installazione di vCloud Director. Impostazione predefinita: vcd1.
ID installazione	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**.

Se si desidera raggiungere gli host tramite una route del gateway non predefinito, potrebbe essere necessario specificare route statiche. 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, 172.16.200.253**.

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

Impostazione	Descrizione
Gateway predefinito	Indirizzo IP del gateway predefinito per l'appliance.
Nome dominio	Dominio di ricerca DNS, ad esempio <i>mydomain.com</i> .
Percorso di ricerca dominio	Elenco di nomi di dominio separati da virgole o da spazi per la ricerca del nome host dell'appliance, ad esempio <i>subdomain.example.com</i> . Nota Il nome di dominio immesso nella casella di testo Nome dominio è il primo elemento nell'elenco dei percorsi di ricerca del dominio.
Server nome di dominio	Indirizzo IP del server dei nomi di dominio per l'appliance.
Indirizzo IP di rete eth0	Indirizzo IP dell'interfaccia eth0.
Network mask eth0	La maschera di rete o il prefisso per l'interfaccia eth0.
Indirizzo IP di rete eth1	Indirizzo IP dell'interfaccia eth1.
Network mask eth1	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.
- [Modifica del fuso orario dell'appliance di vCloud Director](#)

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*.

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

Quando si aggiungono appliance aggiuntive o sostitutive a un cluster di database, la vCPU e la RAM devono corrispondere a quelle delle celle primarie e di standby esistenti nel cluster.

La versione OVA della cella di standby appena distribuita deve essere identica a quella delle appliance esistenti nel cluster. Per visualizzare la versione delle appliance in esecuzione, vedere Informazioni nell'interfaccia utente di gestione dell'appliance. L'appliance viene distribuita con un nome nel formato VMware Cloud 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 Cloud Director-10.2.0.0-9229800_OVA10.ova.

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

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

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

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. Importante Deve essere diversa dalla rete di destinazione di eth1.

Opzione	Valore	Descrizione
<code>--net:"eth1 Network"</code>	<code>portgroup_on_vc_for_eth1</code>	La rete di destinazione per la rete eth1 dell'appliance. Importante Deve essere diversa dalla rete di destinazione di eth0.
<code>--name</code>	<code>vm_name_on_vc</code>	Il nome della macchina virtuale per l'appliance.
<code>--diskMode</code>	<code>thin</code> o <code>thick</code>	Il formato del disco per i dischi virtuali e i file di configurazione delle macchine virtuali.
<code>--prop:"vami.ip0.VMware_vCloud_Director"</code>	<code>eth0_ip_address</code>	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.
<code>--prop:"vami.ip1.VMware_vCloud_Director"</code>	<code>eth1_ip_address</code>	Indirizzo IP di eth1. Utilizzato per accedere ai servizi interni, incluso il servizio del database PostgreSQL incorporato.
<code>--prop:"vami.DNS.VMware_vCloud_Director"</code>	<code>dns_ip_address</code>	Indirizzo IP del server dei nomi di dominio per l'appliance.
<code>--prop:"vami.domain.VMware_vCloud_Director"</code>	<code>domain_name</code>	Dominio di ricerca DNS. Viene visualizzato come primo elemento nel percorso di ricerca.
<code>--prop:"vami.gateway.VMware_vCloud_Director"</code>	<code>gateway_ip_address</code>	Indirizzo IP del gateway predefinito per l'appliance.
<code>--prop:"vami.netmask0.VMware_vCloud_Director"</code>	<code>netmask</code>	La maschera di rete o il prefisso per l'interfaccia eth0.
<code>--prop:"vami.netmask1.VMware_vCloud_Director"</code>	<code>netmask</code>	La maschera di rete o il prefisso per l'interfaccia eth1.
<code>--prop:"vami.searchpath.VMware_vCloud_Director"</code>	<code>list_of_domain_names</code>	Il percorso di ricerca del dominio dell'appliance. Un elenco di nomi di dominio separati da una virgola o da uno spazio.
<code>--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"</code>	<code>true</code> o <code>false</code>	Abilita o disabilita l'accesso root SSH all'appliance.
<code>--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"</code>	<code>true</code> o <code>false</code>	Determina se continuare o meno a utilizzare la password iniziale dopo il primo accesso.
<code>--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"</code>	<code>ip_address:nfs_mount_path</code>	L'indirizzo IP e il percorso di esportazione del server NFS esterno. Utilizzato solo per una cella primaria.
<code>--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"</code>	<code>ntp_server_ip_address</code>	L'indirizzo IP del server temporale.

Opzione	Valore	Descrizione
<code>--prop:"vcloudapp.varoot-password.VMware_vCloud_Director_password"</code>	<code>vcloudapp.varoot-password</code>	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. Importante 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.
<code>--prop:"vcloudconf.db_pwd.VMware_vCloud_Director_password"</code>	<code>vcloudconf.db_pwd</code>	La password del database dell'utente vcloud . Utilizzata solo per una cella primaria.
<code>--prop:"vcloudwiz.admin_email.VMware_vCloud_Director_email_address"</code>	<code>vcloudwiz.admin_email</code>	Indirizzo e-mail dell'account dell' amministratore di sistema . Utilizzato solo per una cella primaria.
<code>--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director_firstname"</code>	<code>vcloudwiz.admin_fname</code>	Il nome dell'account dell' amministratore di sistema . Utilizzato solo per una cella primaria.
<code>--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director_password"</code>	<code>vcloudwiz.admin_pwd</code>	Password dell'account dell' amministratore di sistema . Utilizzata solo per una cella primaria.
<code>--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director_username"</code>	<code>vcloudwiz.admin_uname</code>	Nome utente per l'account dell' amministratore di sistema . Utilizzato solo per una cella primaria.
<code>--prop:"vcloudwiz.inst_id.VMware_vCloud_Director_inst_id"</code>	<code>vcloudwiz.inst_id</code>	L'ID di installazione di vCloud Director. Utilizzato solo per una cella primaria.
<code>--prop:"vcloudconf.sys_name.VMware_vCloud_Director_system_name"</code>	<code>vcloudconf.sys_name</code>	Nome della cartella di vCenter Server da creare per questa installazione di vCloud Director.
<code>--prop:"vcloudnet.routes0.VMware_vCloud_Director_ip_address1 cidr, ip_address2, ..."</code>	<code>vcloudnet.routes0</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 un indirizzo IP del gateway e, facoltativamente, da una specifica di rete CIDR (Classless Inter-Domain Routing) (prefisso/bit). Ad esempio, 172.16.100.253 172.16.100/19, 172.16.200.253 .

Opzione	Valore	Descrizione
<code>--prop:"vcloudnet.routes1.VMware_vCloud_Director"</code>	<code>ip_address1 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 un indirizzo IP del gateway e, facoltativamente, da una specifica di rete CIDR (Classless Inter-Domain Routing) (prefisso/bit). Ad esempio, 172.16.100.253 172.16.100/19, 172.16.200.253.

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"> ■ primary-small 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. ■ primary-large 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. ■ standby-small 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. ■ standby-large 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. ■ cell distribuisce l'appliance con 8 GB di RAM e 2 vCPU come membro successivo in un gruppo

Opzione	Valore	Descrizione
		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.
		<p>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.</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

Importante Prima di eseguire il comando VMware OVF Tool, sostituire le password di `vcloudapp.varoot-passwordVMware_vCloud_Director`, `vcloudconf.db_pwdVMware_vCloud_Director` e `vcloudconf.admin_pwd.VMware_vCloud_Director` con password sicure proprie.

```
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"="place-secure-password-here" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-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

Importante Prima di eseguire il comando VMware OVF Tool, sostituire la password di vcloudapp.varoot-password.VMware_vCloud_Director con una password sicura propria.

```
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.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
--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 vcloud.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

8

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](#)
- [Ripristino da un errore di cella di standby in un cluster a disponibilità elevata](#)
- [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](#)
- [Aumento della capacità del database PostgreSQL incorporato in un'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.

È possibile usare questo flusso di lavoro per riutilizzare gli indirizzi IP e il nome host della cella primaria con errore quando si distribuisce la nuova cella di standby.

Prerequisiti

- Verificare che la cella primaria abbia stato non raggiungibile o non riuscito.
- Verificare che le due celle di standby abbiano stato in esecuzione.

- Familiarizzare con la procedura di rimozione di un'appliance con errore dal gruppo di server di vCloud Director e dal cluster a disponibilità elevata repmgr. Vedere [Annullamento della registrazione di una cella primaria non riuscita in un cluster a disponibilità elevata del database](#).

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

Procedura

- 1 Se possibile, utilizzare lo strumento di gestione delle celle per arrestare il processo di vCloud Director. Dalla cella primaria con errore, eseguire il comando seguente.

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

- 2 Spegnerla macchina virtuale primaria in errore.
- 3 Accedere come **root** all'interfaccia utente di gestione dell'appliance di una cella di standby in esecuzione, `https:// standby_ip_address:5480`.
- 4 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.

- 5 Rimuovere l'appliance primaria con errore dal gruppo di server vCloud Director e dal cluster a disponibilità elevata repmgr.
- 6 Se si desidera riutilizzare l'indirizzo IP e il nome host della cella primaria con errore, assicurarsi che l'appliance primaria con errore resti spenta oppure eliminarla.
- 7 Distribuire una nuova appliance di standby. È possibile [Avviamento della distribuzione dell'appliance vCloud Director](#) oppure [Distribuzione dell'appliance vCloud Director tramite VMware OVF Tool](#).

Dopo la distribuzione della nuova appliance di standby, lo stato di integrità del cluster deve essere Integro.

Ripristino da un errore di cella di standby in un cluster a disponibilità elevata

Se una cella di standby non viene eseguita correttamente, è possibile eseguire il ripristino distribuendo una nuova cella di standby.

Se lo stato di una delle celle di standby è `Unreachable` o `Failed`, è possibile distribuire una nuova cella. Per visualizzare lo stato delle celle nel cluster, vedere [Visualizzazione dello stato delle celle in un cluster ad alta disponibilità del database](#).

È possibile utilizzare questo flusso di lavoro per riutilizzare gli indirizzi IP e il nome host della cella di standby in errore quando si distribuisce una nuova cella di standby.

- 1 Se possibile, utilizzare lo strumento di gestione celle per arrestare il processo di vCloud Director. Dalla cella di standby in errore, eseguire il comando seguente.

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

- 2 Spegnerla macchina virtuale di standby in errore.
- 3 Rimuovere l'appliance primaria con errore dal gruppo di server di vCloud Director e dal cluster a disponibilità elevata repmgr. Vedere [Annullamento della registrazione di un nodo di standby non riuscito o irraggiungibile in un cluster a disponibilità elevata del database](#).
- 4 Se si desidera riutilizzare l'indirizzo IP e il nome DNS della cella di standby in errore, è necessario assicurarsi che la cella di standby in errore resti spenta o eliminarla.
- 5 Distribuire una nuova appliance di standby. È possibile [Avviamento della distribuzione dell'appliance vCloud Director](#) oppure [Distribuzione dell'appliance vCloud Director tramite VMware OVF Tool](#).

Dopo la distribuzione della nuova cella di standby, lo stato di integrità del cluster deve essere Integro.

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,

i file `global.properties`, `responses.properties`, `certificates`, `proxycertificates` e i file `truststore` 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.

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 Service Provider Admin Portal utilizzando l'indirizzo IP di rete eth0 di una cella del nuovo gruppo di server, `https://et0_IP_new_cell/provider`.
 - b Accedere a Service Provider Admin Portal 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 Service Provider Admin Portal per eliminare le celle disconnesse che appartengono all'ambiente vCloud Director precedente.
 - a Dal menu principale () , selezionare **Risorse cloud**
 - b Nel riquadro a sinistra fare clic su **Celle cloud**.

- c Selezionare una cella inattiva e fare clic su **Annulla registrazione**.

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 <code>pg_hba.conf</code> . Vedere Configurazione dell'accesso esterno al database di vCloud Director .

Aumento della capacità del database PostgreSQL incorporato in un'appliance vCloud Director

Se non si dispone di spazio sufficiente sul disco del database PostgreSQL di un'appliance vCloud Director, è possibile aumentare la capacità del database PostgreSQL incorporato.

Il database PostgreSQL si trova sul disco rigido 3. Ha una dimensione predefinita di 80 GB. La procedura può essere eseguita mentre le appliance sono operative.

Importante Prima di aumentare la capacità dell'appliance primaria, è necessario aumentare la capacità di tutte le appliance di standby esistenti.

Prerequisiti

- Se l'ambiente vCloud Director dispone di nodi di standby, identificare i nodi di standby e il nodo primario e avviare la procedura da un nodo di standby. Per ulteriori informazioni sull'identificazione dei ruoli dei nodi, vedere [Verifica dello stato di un cluster a disponibilità elevata del database](#).
- Se l'ambiente vCloud Director è costituito solo da un nodo primario, eseguire la procedura sul nodo primario.

Procedura

- 1 Accedere a vSphere Client per aumentare la capacità del disco rigido 3 alle dimensioni desiderate.

Le dimensioni del disco del database PostgreSQL su ciascuna appliance di standby deve essere grande quanto il disco del database PostgreSQL nell'appliance primaria.

- a Selezionare la macchina virtuale dell'appliance che si desidera modificare.
- b Selezionare **Azioni > Modifica impostazioni**.
- c Aumentare le dimensioni del **Disco rigido 3** e fare clic su **OK**.

Lo stato di avanzamento dell'attività di riconfigurazione viene visualizzato nel riquadro **Task recenti**.

- 2 Aumentare la dimensione logica del volume utilizzato dal database.

- a Accedere alla console dell'appliance vCloud Director come **root** direttamente o utilizzando un client SSH.
- b Per applicare la modifica di ridimensionamento del disco rigido al sistema operativo, eseguire il comando seguente.

```
echo 1 > /sys/class/scsi_device/2\:0\:2\:0/device/rescan
```

- c Per consentire che sia riconosciuto lo spazio corretto al livello del volume fisico, eseguire il comando seguente.

```
pvresize /dev/sdc
```

- d (Facoltativo) Confermare le nuove dimensioni del volume fisico eseguendo il comando seguente.

```
pvdiskdisplay
```

- e Ridimensionare il volume logico eseguendo il comando seguente.

```
lvresize /dev/database_vg/vpostgres /dev/sdc
```

- f (Facoltativo) Confermare le nuove dimensioni del volume logico eseguendo il comando seguente.

```
lvdisplay
```

3 Aumentare le dimensioni del file system in modo che utilizzi l'intero volume logico.

- a Per utilizzare lo spazio aggiuntivo, eseguire il comando seguente.

```
resize2fs /dev/database_vg/vpostgres
```

- b (Facoltativo) Per assicurarsi che il file system abbia utilizzato lo spazio aggiuntivo, eseguire `df -h`.

Lo spazio aggiuntivo è disponibile per il sistema operativo. L'output di sistema è simile a: `/dev/mapper/database_vg-vpostgres 157G 75G 82G 48%/var/vmware/vpostgres`

- 4 Se l'ambiente in uso non è costituito da una sola appliance primaria e dispone di altri nodi di standby, ripetere le operazioni indicate dal passaggio 1 al passaggio 3 su tutti gli altri nodi di standby che dispongono di un database e quindi ripetere dal passaggio 1 al passaggio 3 sul nodo primario.

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.

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.

Guida di riferimento allo strumento di gestione delle celle

10

Lo strumento di gestione delle celle è una utility della riga di comando che è possibile utilizzare per gestire un database o una cella di vCloud Director. Per la maggior parte delle operazioni è necessario disporre delle credenziali di utente con privilegi avanzati o amministratore di sistema.

Lo strumento di gestione delle celle viene installato in `/opt/vmware/vcloud-director/bin/`. È possibile utilizzarlo per eseguire un singolo comando oppure come shell interattiva.

Elenco dei comandi disponibili

La seguente riga di comando consente di elencare i comandi per la gestione delle celle.

```
./cell-management-tool -h
```

Utilizzo della modalità shell

È possibile eseguire lo strumento di gestione delle celle come shell interattiva richiamandolo senza argomenti, come mostrato qui.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool
Cell Management Tool v8.14.0.4146350 Type "help" for available subcommands. cmt>
```

In modalità shell, è possibile digitare qualsiasi comando dello strumento di gestione delle celle al prompt `cmt>`, come mostrato in questo esempio.

```
cmt>cell -h
usage: cell [options] -a,--application-states display the state of each application on the cell
[DEPRECATED - use the cell-application command instead] -h,--help print this message -i,--pid <arg>
the process id of the cell [REQUIRED if username is not specified] -m,--maintenance <arg> gracefully
enter maintenance mode on the cell -p,--password <arg> administrator password [OPTIONAL] -q,--quiesce
<arg> quiesce activity on the cell -s,--shutdown gracefully shutdown the cell -t,--status display
activity on the cell -tt,--status-verbose display a verbose description of activity on the cell -u,--
username <arg> administrator username [REQUIRED if pid is not specified] Note: You will be prompted
for administrator password if not entered in command line. cmt>
```

Al termine dell'esecuzione, il comando ritorna al prompt `cmt>`. Per chiudere la modalità shell, digitare **exit** al prompt `cmt>`.

Esempio: Guida all'uso dello strumento di gestione delle celle

In questo esempio viene eseguito un singolo comando non interattivo che elenca i comandi disponibili dello strumento di gestione della shell.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
usage: cell-management-tool -h,--help print this message Available commands: cell - Manipulates the
Cell and core components certificates - Reconfigures the SSL certificates for the cell . . . For
command specific help: cell-management-tool <commandName> -h
```

■ Configurazione di un'installazione di vCloud Director

Utilizzare il comando `system-setup` dello strumento di gestione delle celle per inizializzare il database del gruppo di server con un account di amministratore di sistema e le informazioni correlate.

■ Abilitazione di vCloud Director Web Console

In vCloud Director 10.0, vCloud Director Web Console (l'interfaccia utente basata su Flex) è obsoleta e disabilitata per impostazione predefinita, e l'URL di Web Console reindirizza alle pagine di destinazione HTML5 corrispondenti per i provider di servizi e i tenant. Per abilitare Web Console, è possibile utilizzare lo strumento di gestione delle celle.

■ Disabilitazione dell'accesso del provider di servizi all'endpoint API legacy

A partire da vCloud Director 10.0, è possibile utilizzare gli endpoint di accesso OpenAPI separati di vCloud Director per l'accesso di provider di servizi e tenant a vCloud Director.

■ Gestione di una cella

Grazie al sottocomando `cell` dello strumento di gestione delle celle, è possibile sospendere lo scheduler dei task in modo che non sia possibile avviare nuovi task, visualizzare lo stato dei task attivi, controllare la modalità di manutenzione della cella o chiudere la cella normalmente.

■ Gestione delle applicazioni della cella

Utilizzare il comando `cell-application` dello strumento di gestione delle celle per controllare il set di applicazioni eseguite dalla cella all'avvio.

■ Aggiornamento delle proprietà di connessione del database

È possibile aggiornare le proprietà di connessione per il database di vCloud Director utilizzando il sottocomando `reconfigure-database` dello strumento di gestione delle celle.

■ Rilevamento e riparazione dei dati danneggiati dello scheduler

vCloud Director utilizza lo scheduler di processi Quartz per coordinare le operazioni asincrone (processi) in esecuzione nel sistema. Se il database dello scheduler Quartz si danneggia, potrebbe non essere possibile riuscire a disattivare il sistema. Utilizzare il comando `fix-scheduler-data` dello strumento di gestione delle celle per analizzare il database alla ricerca di eventuali dati danneggiati dello scheduler e ripararli secondo necessità.

- **Generazione di certificati autofirmati per gli endpoint proxy della console e HTTP**

Utilizzare il comando `generate-certs` dello strumento di gestione delle celle per generare certificati SSL autofirmati per gli endpoint proxy della console e HTTP.

- **Sostituzione di certificati per gli endpoint proxy della console e HTTP**

Utilizzare il comando `certificates` dello strumento di gestione delle celle per sostituire i certificati SSL per gli endpoint proxy della console e HTTP.

- **Importazione di certificati SSL da servizi esterni**

Utilizzare il comando `import-trusted-certificates` dello strumento di gestione delle celle per importare certificati da utilizzare per stabilire connessioni protette a servizi esterni come AMQP e il database vCloud Director.

- **Gestione dell'elenco di crittografia SSL consentita**

Utilizzare il comando `ciphers` dello strumento di gestione delle celle per configurare il set di pacchetti di crittografia messo a disposizione dalla cella, da utilizzare durante il processo di handshake SSL.

- **Gestione dell'elenco dei protocolli SSL consentiti**

Utilizzare il comando `ssl-protocols` dello strumento di gestione delle celle per configurare il set di protocolli SSL messo a disposizione dalla cella per l'utilizzo durante il processo di handshake SSL.

- **Configurazione della raccolta di metriche**

Utilizzare il comando `configure-metrics` dello strumento di gestione delle celle per configurare il set di metriche da raccogliere.

- **Configurazione di un database delle metriche Cassandra**

Utilizzare il comando `cassandra` dello strumento di gestione delle celle per connettere la cella a un database delle metriche facoltativo.

- **Recupero della password dell'amministratore di sistema**

Se si conoscono il nome utente e la password del database di vCloud Director, è possibile usare il comando `recover-password` dello strumento di gestione delle celle per recuperare la password dell'amministratore di sistema di vCloud Director.

- **Aggiornamento dello stato di errore di un task**

Utilizzare il comando `fail-tasks` dello strumento di gestione delle celle per aggiornare lo stato di completamento associato ai task che erano in esecuzione quando la cella è stata deliberatamente chiusa. Non è possibile utilizzare il comando `fail-tasks` se tutte le celle non sono state chiuse.

- **Configurazione della gestione dei messaggi di controllo**

Utilizzare il comando `configure-audit-syslog` dello strumento di gestione delle celle per configurare la modalità di registrazione dei messaggi di controllo da parte del sistema.

- [Configurazione dei modelli e-mail](#)

Utilizzare il comando `manage-email` dello strumento di gestione delle celle per gestire i modelli utilizzati dal sistema durante la creazione degli avvisi e-mail.

- [Individuazione di macchine virtuali orfane](#)

Utilizzare il comando `find-orphan-vm` dello strumento di gestione delle celle per trovare riferimenti a macchine virtuali presenti nel database di vCenter ma non nel database di vCloud Director.

- [Attivazione o disattivazione della partecipazione al programma CEIP VMware](#)

Per partecipare o uscire dal programma CEIP di VMware, è possibile utilizzare il sottocomando `configure-ceip` dello strumento di gestione delle celle.

- [Aggiornamento delle impostazioni di configurazione dell'applicazione](#)

Con il sottocomando `manage-config` dello strumento di gestione delle celle è possibile aggiornare le diverse impostazioni di configurazione dell'applicazione, come le attività di limitazione del catalogo.

- [Configurazione della limitazione della sincronizzazione del catalogo](#)

Quando si dispone di numerosi elementi del catalogo pubblicati o sottoscritti da altre organizzazioni, per evitare il sovraccarico del sistema durante le sincronizzazioni del catalogo è possibile configurare la limitazione della sincronizzazione del catalogo. È possibile utilizzare il sottocomando `manage-config` dello strumento di gestione delle celle per configurare la limitazione della sincronizzazione del catalogo limitando il numero di elementi della libreria che possono essere sincronizzati contemporaneamente.

- [Risoluzione dei problemi relativi all'accesso non riuscito all'interfaccia utente di vCloud Director](#)

Per visualizzare e aggiornare le voci DNS e gli indirizzi IP validi per le celle di vCloud Director nell'ambiente di vCloud Director, è possibile utilizzare il sottocomando `manage-config` dello strumento di gestione delle celle.

- [Debug dell'individuazione delle macchine virtuali vCenter](#)

Utilizzando il sottocomando `debug-auto-import` dello strumento di gestione delle celle, è possibile cercare di scoprire il motivo per cui il meccanismo di individuazione delle vApp ignora una o più macchine virtuali vCenter.

- [Rigenerazione degli indirizzi MAC per reti estese multisito](#)

Se si associano due siti di vCloud Director configurati con lo stesso ID di installazione, possono verificarsi conflitti di indirizzi MAC nelle reti estese di questi siti. Per evitare tali conflitti, è necessario rigenerare gli indirizzi MAC in uno dei siti in base a un valore di inizializzazione personalizzato diverso dall'ID di installazione.

- [Aggiornamento degli indirizzi IP del database nelle celle di vCloud Director](#)

È possibile utilizzare lo strumento di gestione delle celle per aggiornare gli indirizzi IP delle celle di vCloud Director in un cluster a elevata disponibilità del database.

Configurazione di un'installazione di vCloud Director

Utilizzare il comando `system-setup` dello strumento di gestione delle celle per inizializzare il database del gruppo di server con un account di amministratore di sistema e le informazioni correlate.

Dopo aver configurato tutti i server del gruppo di server vCloud Director e averli connessi al database, è possibile creare l'account iniziale di amministratore di sistema e inizializzare il database vCloud Director con le informazioni correlate mediante una riga di comando con la seguente struttura:

```
cell-management-tool system-setup options
```

Non è possibile eseguire questo comando su un sistema già configurato. È necessario specificare tutte le opzioni tranne `--unattended` e `--password`.

Tabella 10-1. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `system-setup`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--email</code>	L'indirizzo e-mail dell'amministratore di sistema che si sta creando.	L'indirizzo e-mail dell'amministratore di sistema è archiviato nel database di vCloud Director.
<code>--full-name</code>	Il nome completo dell'amministratore di sistema che si sta creando.	Il nome completo dell'amministratore di sistema è archiviato nel database di vCloud Director.
<code>--installation-id</code>	Un numero intero compreso nell'intervallo da 1 a 63	L'ID installazione per questa installazione di vCloud Director. Il sistema utilizza l'ID installazione durante la generazione degli indirizzi MAC per le schede NIC virtuali.

Nota Se si prevede di creare reti estese in installazioni di vCloud Director in una distribuzione multisito, è consigliabile impostare un ID di installazione univoco per ogni installazione di vCloud Director.

Tabella 10-1. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando system-setup (continua)

Opzione	Argomento	Descrizione
<code>--password</code>	La password dell'amministratore di sistema che si sta creando. Necessaria quando si utilizza l'opzione <code>--unattended</code> . Se non si utilizza l'opzione <code>--unattended</code> e non si fornisce la riga di comando, il comando richiede la password.	L'amministratore di sistema fornisce questa password durante l'autenticazione in vCloud Director.
<code>--serial-number</code>	Il numero di serie (chiave di licenza) per questa installazione.	Facoltativo. Deve essere un numero di serie valido di vCloud Director.
<code>--system-name</code>	Il nome da utilizzare per la cartella vCenter Server di vCloud Director.	Questa installazione di vCloud Director è rappresentata da una cartella con questo nome in ciascun vCenter Server con cui è effettuata la registrazione.
<code>--unattended</code>	Nessuno	Facoltativo. Il comando non richiede ulteriori input quando viene richiamato con questa opzione.
<code>--user</code>	Il nome utente dell'amministratore di sistema che si sta creando.	L'amministratore di sistema fornisce questo nome utente durante l'autenticazione a vCloud Director.

Esempio: Specifica delle impostazioni di sistema di vCloud Director

Un comando come questo specifica tutte le impostazioni di sistema per una nuova installazione di vCloud Director. Poiché `--unattended` e `--password` non sono specificati, il comando richiede di fornire e confermare la password creata per l'amministratore di sistema.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool system-setup \ --user admin --full-name "VCD System Administrator" --email vcd-admin@example.com --system-name VCD --installation-id 2
```

Please enter the new password for user admin (password must have more than 6 characters):

Re-enter the password to confirm:

```
Username: admin
Full name: VCD System Administrator
Email: vcd-admin@example.com
System name: VCD
Installation ID: 2
```



```
Are you sure you want to use these parameters? [Y/n]:y
Creating admin user.
Setting system details.
Completing system setup.
System setup is complete.
```

Abilitazione di vCloud Director Web Console

In vCloud Director 10.0, vCloud Director Web Console (l'interfaccia utente basata su Flex) è obsoleta e disabilitata per impostazione predefinita, e l'URL di Web Console reindirizza alle pagine di destinazione HTML5 corrispondenti per i provider di servizi e i tenant. Per abilitare Web Console, è possibile utilizzare lo strumento di gestione delle celle.

Procedura

- 1 Effettuare l'accesso normalmente o tramite SSH come utente **root** nel sistema operativo di qualsiasi cella di vCloud Director.
- 2 Abilitare Web Console utilizzando lo strumento di gestione delle celle.
 - Per abilitare Web Console per tutti gli utenti, eseguire il comando seguente.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n flex.ui.enabled -v true
```

- Per abilitare Web Console solo per gli amministratori di sistema, eseguire il comando seguente.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n flex.ui.enabled -v sys-admin-only
```

Tabella 10-2. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `manage-config`

Opzione	Argomento	Descrizione
<code>--name (-n)</code>	<code>flex.ui.enabled</code>	Il contrassegno per abilitare o disabilitare Web Console.
<code>--value (-v)</code>	<code>false</code> (valore predefinito)	<p>L'argomento <code>false</code> disabilita Web Console. Questo è il comportamento predefinito.</p> <ul style="list-style-type: none"> ■ <code>base_cell_URL/</code> - Nessun reindirizzamento, ricarica la pagina di accesso. ■ <code>base_cell_URL/cloud</code> - Reindirizza a <code>/provider</code>. ■ <code>base_cell_URL/cloud/login.jsp</code> - Reindirizza a <code>/provider</code>. ■ <code>base_cell_URL/cloud/org/organization_name</code> - Reindirizza a <code>/tenant/organization_name</code>.

Tabella 10-2. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `manage-config` (continua)

Opzione	Argomento	Descrizione
	<code>true</code>	<p>L'argomento <code>true</code> abilita Web Console.</p> <ul style="list-style-type: none"> ■ <code>base_cell_URL/</code> - Nessun reindirizzamento, ricarica la pagina di accesso. ■ <code>base_cell_URL/cloud</code> - Nessun reindirizzamento. ■ <code>base_cell_URL/cloud/login.jsp</code> - Nessun reindirizzamento. ■ <code>base_cell_URL/cloud/org/organization_name</code> - Nessun reindirizzamento.
	<code>sys-admin-only</code>	<p>L'argomento <code>sys-admin-only</code> abilita Web Console per gli amministratori di sistema.</p> <ul style="list-style-type: none"> ■ <code>base_cell_URL/</code> - Nessun reindirizzamento, ricarica la pagina di accesso. ■ <code>base_cell_URL/cloud</code> - Nessun reindirizzamento. ■ <code>base_cell_URL/cloud/login.jsp</code> - Nessun reindirizzamento. ■ <code>base_cell_URL/cloud/org/organization_name</code> - Reindirizza a <code>/tenant/organization_name</code>.

3 Riavviare la cella di vCloud Director per fare in modo che le modifiche vengano applicate.

```
service vmware-vcd restart
```

Operazioni successive

- Per accedere a vCloud Director Web Console, passare a `https://hostname.domain.tld/cloud` e accedere come amministratore di sistema oppure passare a `https://vcloud.example.com/cloud/org/myOrg` per accedere all'organizzazione. Per ulteriori informazioni su vCloud Director Web Console, vedere la *Guida per gli amministratori di vCloud Director versione 9.7* e la *Guida per gli utenti di vCloud Director versione 9.7*.
- Per disabilitare vCloud Director Web Console e tornare al comportamento predefinito, eseguire il comando seguente:

```
cell-management-tool manage-config -n flex.ui.enabled -v false
```

Disabilitazione dell'accesso del provider di servizi all'endpoint API legacy

A partire da vCloud Director 10.0, è possibile utilizzare gli endpoint di accesso OpenAPI separati di vCloud Director per l'accesso di provider di servizi e tenant a vCloud Director.

vCloud Director 10.0 introduce due nuovi endpoint OpenAPI che possono essere utilizzati per aumentare la sicurezza limitando l'accesso a vCloud Director.

- `/cloudapi/1.0.0/sessions/provider`: endpoint OpenAPI per l'accesso del provider di servizi. I tenant non possono accedere a vCloud Director utilizzando questo endpoint.
- `/cloudapi/1.0.0/sessions/`: endpoint OpenAPI per l'accesso del tenant. I provider di servizi non possono accedere a vCloud Director utilizzando questo endpoint.

Per impostazione predefinita, gli amministratori del provider e gli utenti dell'organizzazione accedono a vCloud Director utilizzando l'endpoint API `/api/sessions`.

Utilizzando il sottocomando `manage-config` dello strumento di gestione delle celle, è possibile disabilitare l'accesso del provider di servizi all'endpoint API `/api/sessions` e, di conseguenza, limitare l'accesso del provider al nuovo endpoint OpenAPI `/cloudapi/1.0.0/sessions/provider`, accessibile solo ai provider di servizi.

Procedura

- 1 Effettuare l'accesso normalmente o tramite SSH come utente **root** nel sistema operativo di qualsiasi cella di vCloud Director.
- 2 Per bloccare l'accesso del provider all'endpoint API `/api/sessions`, utilizzare lo strumento di gestione delle celle ed eseguire il comando seguente:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n  
vcloud.api.legacy.nonprovideronly -v true
```

Risultati

L'endpoint API `/api/sessions` non è più accessibile ai provider di servizi. I provider di servizi possono utilizzare il nuovo endpoint OpenAPI `/cloudapi/1.0.0/sessions/provider` per accedere a vCloud Director. I tenant possono accedere a vCloud Director utilizzando sia l'endpoint API `/api/sessions` sia il nuovo endpoint OpenAPI `/cloudapi/1.0.0/sessions/`.

Operazioni successive

Per abilitare l'accesso del provider all'endpoint API `/api/sessions`, eseguire il comando seguente:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n  
vcloud.api.legacy.nonprovideronly -v false
```

Gestione di una cella

Grazie al sottocomando `cell` dello strumento di gestione delle celle, è possibile sospendere lo scheduler dei task in modo che non sia possibile avviare nuovi task, visualizzare lo stato dei task attivi, controllare la modalità di manutenzione della cella o chiudere la cella normalmente.

Per gestire una cella, usare una riga di comando con la seguente struttura:

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

dove *sysadmin-username* e *sysadmin-password* sono il nome utente e la password dell'**amministratore di sistema**.

Nota Per motivi di sicurezza, è possibile omettere la password. In questo caso, il comando richiede di immettere la password senza visualizzarla nella schermata.

Anziché fornire le credenziali dell'**amministratore di sistema**, è possibile utilizzare l'opzione `--pid` e fornire l'ID del processo della cella. Per individuare tale ID, specificare un comando simile al seguente:

```
cat /var/run/vmware-vcd-cell.pid
```

Tabella 10-3. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `cell`

Opzione	Argomento	Descrizione
<code>--help</code> (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--pid</code> (-i)	ID del processo della cella	È possibile utilizzare questa opzione anziché <code>--username</code> .
<code>--maintenance</code> (-m)	true o false	Imposta la modalità di manutenzione per la cella. L'argomento <code>true</code> disattiva l'attività nella cella e inserisce la cella in modalità di manutenzione. L'argomento <code>false</code> rilascia la cella dalla modalità di manutenzione.
<code>--password</code> (-p)	Password dell' amministratore di sistema di vCloud Director	Facoltativa se viene utilizzata l'opzione <code>--username</code> . Se si omette questa opzione, il comando richiede di immettere la password senza visualizzarla nella schermata.
<code>--quiesce</code> (-q)	true o false	Disattiva la cella. L'argomento <code>true</code> sospende lo scheduler. L'argomento <code>false</code> riavvia lo scheduler.

Tabella 10-3. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando cell (continua)

Opzione	Argomento	Descrizione
<code>--shutdown</code> (-s)	Nessuno	Esegue la chiusura normale dei servizi di vCloud Director nel server.
<code>--status</code> (-t)	Nessuno	Mostra informazioni sul numero di task in esecuzione sulla cella e sullo stato della cella.
<code>--status-verbose</code> (-tt)	Nessuno	Mostra informazioni dettagliate sui task in esecuzione sulla cella e sullo stato della cella.
<code>--username</code> (-u)	Nome utente dell' amministratore di sistema di vCloud Director.	È possibile utilizzare questa opzione anziché <code>-pid</code> .

Gestione delle applicazioni della cella

Utilizzare il comando `cell-application` dello strumento di gestione delle celle per controllare il set di applicazioni eseguite dalla cella all'avvio.

Un vCloud Director esegue alcune applicazioni che forniscono i servizi richiesti dai client vCloud Director. Per impostazione predefinita, la cella avvia un sottoinsieme di queste applicazioni. In genere, per supportare un'installazione di vCloud Director sono necessari tutti i membri di tale sottoinsieme.

Per visualizzare o modificare l'elenco di applicazioni eseguite all'avvio della cella, utilizzare una riga di comando con il formato seguente:

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

sysadmin-username

Il nome utente di un amministratore di sistema vCloud Director.

sysadmin-password

La password di un amministratore di sistema vCloud Director. È necessario specificare la password se contiene caratteri speciali.

Nota È possibile fornire la password dell'amministratore di sistema di vCloud Director nella riga di comando `cell-management-tool`, ma è più sicuro ometterla. In questo caso, `cell-management-tool` richiederà l'immissione di una password, che non verrà visualizzata nella schermata durante la digitazione.

Anziché fornire le credenziali dell'amministratore di sistema, è possibile utilizzare l'opzione `--pid` e fornire l'ID del processo della cella. Per individuare tale ID, specificare un comando simile al seguente:

```
cat /var/run/vmware-vcd-cell.pid
```

command

Un sottocomando `cell-application`.

Tabella 10-4. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `cell-application`

Comando	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--application-states</code>	Nessuno	Elenco delle applicazioni della cella con il relativo stato corrente.
<code>--disable</code>	ID applicazione	Impedisce l'esecuzione dell'applicazione della cella all'avvio della cella.
<code>--enable</code>	ID applicazione	Consente l'esecuzione dell'applicazione della cella all'avvio della cella.
<code>--pid (-i)</code>	ID del processo della cella	È possibile utilizzare questa opzione anziché <code>-u</code> o <code>-u</code> e <code>-p</code> .
<code>--list</code>	Nessuno	Elenco di tutte le applicazioni della cella in cui viene anche indicato se vengono avviate all'avvio della cella.
<code>--password (-p)</code>	Password dell'amministratore di vCloud Director	Facoltativo. Il comando richiederà la password se non viene fornita nella riga di comando.
<code>--set</code>	Elenco degli ID delle applicazioni separati da punto e virgola.	Specifica il set di applicazioni della cella avviate all'avvio della cella. Questo comando sovrascrive il set esistente di applicazioni della cella avviate all'avvio della cella. Utilizzare <code>--enable</code> o <code>--disable</code> per modificare lo stato di avvio di una singola applicazione.
<code>--username (-u)</code>	Nome utente dell'amministratore di vCloud Director.	Obbligatorio se non si specifica <code>--pid</code>

Esempio: Elenco delle applicazioni della cella con il relativo stato di avvio

La riga di comando `cell-management-tool` che segue richiede le credenziali dell'amministratore di sistema e restituisce l'elenco delle applicazioni della cella con il relativo stato di avvio.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell-
application --list
Please enter the administrator password:
```

name	id	enabled	description
Networking	com.vmware.vc...	true	Exposes NSX api endpoints directly from vCD.
Console Proxy	com.vmware.vc...	true	Proxies VM console data connection...
Cloud Proxy	com.vmware.vc...	true	Proxies TCP connections from a tenant site.
Compute Service Broker	com.vmware.vc...	true	Allows registering with a service control...
Maintenance Application	com.vmware.vc...	false	Indicates to users the cell is undergo ...
Core Cell Application	com.vmware.vc...	true	Main cell application, Flex UI and REST API.

Aggiornamento delle proprietà di connessione del database

È possibile aggiornare le proprietà di connessione per il database di vCloud Director utilizzando il sottocomando `reconfigure-database` dello strumento di gestione delle celle.

Durante l'installazione di vCloud Director o il processo di distribuzione dell'appliance vCloud Director, è possibile configurare le proprietà del tipo di database e delle connessioni al database. Consultare [Capitolo 5 Installazione di vCloud Director in Linux](#) e [Capitolo 6 Distribuzione dell'appliance vCloud Director](#).

Dopo aver configurato il database di vCloud Director, è possibile aggiornare le connessioni del database utilizzando il sottocomando `reconfigure-database`. È possibile spostare il database di vCloud Director esistente in un nuovo host, modificare il nome utente e la password del database oppure abilitare una connessione SSL per un database PostgreSQL.

```
cell-management-tool reconfigure-database options
```

Importante Le modifiche apportate mediante il comando `reconfigure-database` vengono scritte nel file di configurazione globale `global.properties` e nel file di risposta `responses.properties` della cella. Prima di eseguire il comando, verificare che il file di risposta sia presente su `/opt/vmware/vcloud-director/etc/responses.properties` e che sia scrivibile. Per informazioni sulla protezione e il riutilizzo del file di risposta, vedere [Capitolo 5 Installazione di vCloud Director in Linux](#).

Se non si utilizza l'opzione `--pid`, è necessario riavviare la cella per applicare le modifiche.

Tabella 10-5. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `reconfigure-database`

Opzione	Argomento	Descrizione
<code>--help</code> (-h)	Nessuno	Fornisce un riepilogo delle opzioni disponibili in questa categoria.
<code>--database-host</code> (-dbhost)	Indirizzo IP o nome di dominio completo dell'host database di vCloud Director	Aggiorna il valore della proprietà <code>database.jdbcUrl</code> . Importante Il comando convalida solo il formato del valore.
<code>--database-instance</code> (-dbinstance)	Istanza del database SQL Server.	Facoltativa. Utilizzata se il tipo di database è <code>sqlserver</code> . Importante Se si include questa opzione, è necessario fornire lo stesso valore specificato originariamente durante la configurazione del database.
<code>--database-name</code> (-dbname)	Il nome del servizio di database.	Aggiorna il valore della proprietà <code>database.jdbcUrl</code> .
<code>--database-password</code> (-dbpassword)	Password per l'utente del database.	Aggiorna il valore della proprietà <code>database.password</code> . La password fornita viene crittografata prima di essere archiviata come valore della proprietà.
<code>--database-port</code> (-dbport)	Numero di porta utilizzato dal servizio di database sull'host database.	Aggiorna il valore della proprietà <code>database.jdbcUrl</code> . Importante Il comando convalida solo il formato del valore.
<code>--database-type</code> (-dbtype)	Il tipo di database. Uno tra: ■ <code>sqlserver</code> ■ <code>postgres</code>	Aggiorna il valore della proprietà <code>database.jdbcUrl</code> .
<code>--database-user</code> (-dbuser)	Il nome utente dell'utente del database.	Aggiorna il valore della proprietà <code>database.user</code> .
<code>--database-ssl</code>	true o false	Utilizzata se il tipo di database è <code>postgres</code> . Configura il database PostgreSQL in modo che richieda una connessione SSL da vCloud Director.

Tabella 10-5. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `reconfigure-database` (continua)

Opzione	Argomento	Descrizione
<code>--pid</code> (<code>-i</code>)	ID del processo della cella.	Facoltativa. Esegue una riconfigurazione a caldo in una cella vCloud Director in esecuzione. Non richiede un riavvio della cella. Se viene utilizzata con <code>--private-key-path</code> , è possibile eseguire immediatamente il comando in celle locali e remote.
<code>--private-key-path</code>	Nome del percorso per la chiave privata della cella.	Facoltativa. Chiude tutte le celle nel gruppo di server in modo ordinato, aggiorna le relative proprietà del database e procede al riavvio. Importante Tutte le celle devono consentire connessioni SSH da parte del superuser senza alcuna password.
<code>--remote-sudo-user</code>	Nome utente con diritti di sudo.	Utilizzata con l'opzione <code>--private-key-path</code> quando l'utente remoto è diverso da root . Per l'appliance, è possibile utilizzare questa opzione per l'utente postgres , ad esempio <code>--remote-sudo-user=postgres</code> .

Quando si utilizzano le opzioni `--database-host` e `--database-port`, il comando convalida il formato degli argomenti, ma non verifica la combinazione di host e porta per l'accessibilità di rete o la presenza di un database in esecuzione del tipo specificato.

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. Per una verifica è, ad esempio, possibile eseguire il seguente comando 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.

Esempio: modifica del nome utente e della password del database di vCloud Director.

Per modificare il nome utente e la password del database di vCloud Director, lasciando tutte le altre proprietà di connessione come erano originariamente configurate, è possibile eseguire il comando seguente:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \ -dbuser vcd-dba -dbpassword P@55w0rd
```

Esempio: Aggiornamento dell'indirizzo IP del database di vCloud Director mediante riconfigurazione a caldo in tutte le celle

Se si è un utente non root con diritti sudo, per cambiare immediatamente l'indirizzo IP del database di vCloud Director in tutte le celle, è possibile eseguire il comando seguente:

```
[sudo@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \ --dbhost db_ip_address -i $(service vmware-vcd pid cell) --private-key-path=path_to_private-key \ --remote-sudo-user=non-root-user
```

Rilevamento e riparazione dei dati danneggiati dello scheduler

vCloud Director utilizza lo scheduler di processi Quartz per coordinare le operazioni asincrone (processi) in esecuzione nel sistema. Se il database dello scheduler Quartz si danneggia, potrebbe non essere possibile riuscire a disattivare il sistema. Utilizzare il comando `fix-scheduler-data` dello strumento di gestione delle celle per analizzare il database alla ricerca di eventuali dati danneggiati dello scheduler e ripararli secondo necessità.

Per effettuare la scansione del database per rilevare dati danneggiati dello scheduler, utilizzare la riga di comando con la seguente struttura:

```
cell-management-tool fix-scheduler-data options
```

Tabella 10-6. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `fix-scheduler-data`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--dbuser</code>	Il nome utente dell'utente del database di vCloud Director.	Deve essere specificato con la riga di comando.
<code>--dbpassword</code>	La password dell'utente del database di vCloud Director.	Se non fornita, viene richiesta.

Generazione di certificati autofirmati per gli endpoint proxy della console e HTTP

Utilizzare il comando `generate-certs` dello strumento di gestione delle celle per generare certificati SSL autofirmati per gli endpoint proxy della console e HTTP.

Ogni gruppo di server vCloud Director deve supportare due endpoint SSL, uno per il servizio HTTP e un altro per il servizio proxy della console. L'endpoint del servizio HTTP supporta il vCloud Director Service Provider Admin Portal, il vCloud Director Tenant Portal e l'API di vCloud. L'endpoint proxy della console remota supporta connessioni VMRC verso vApp e macchine virtuali.

Il comando `generate-certs` dello strumento di gestione delle celle automatizza la procedura [Creazione di certificati SSL autofirmati per vCloud Director in Linux](#).

Per generare nuovi certificati SSL autofirmati e aggiungerli a un archivio chiavi nuovo o già esistente, usare una riga di comando con la seguente struttura:

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

Tabella 10-7. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `generate-certs`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--expiration (-x)</code>	<i>days-until-expiration</i>	Il numero di giorni alla scadenza del certificato. Impostazione predefinita: 365.
<code>--issuer (-i)</code>	<i>name=value [, name=value, ...]</i>	X.509 nome distinto dell'autorità emittente del certificato. Impostazione predefinita: <i>CN=FQDN</i> , dove <i>FQDN</i> è il nome di dominio completo della cella o il suo indirizzo IP, se non è disponibile alcun nome di dominio completo. Se si specificano più coppie di attributi e valori, separarle con virgole e racchiudere l'intero argomento tra virgolette.
<code>--httpcert (-j)</code>	Nessuno	Generare un certificato per l'endpoint http.
<code>--key-size (-s)</code>	<i>key-size</i>	Le dimensioni della coppia di chiavi espresse come numero intero di bit. Impostazione predefinita: 2048. Le dimensioni chiave inferiori a 1024 bit non sono più supportate, come riportato nella Pubblicazione speciale 800-131A del NIST.

Tabella 10-7. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando generate-certs (continua)

Opzione	Argomento	Descrizione
<code>--keystore-pwd (-w)</code>	<i>keystore-password</i>	La password dell'archivio chiavi sull'host.
<code>--out (-o)</code>	<i>keystore-pathname</i>	Il percorso completo dell'archivio chiavi sull'host.
<code>--consoleproxycert (-p)</code>	Nessuno	Generare un certificato per l'endpoint proxy della console.

Nota Per mantenere la compatibilità con le versioni precedenti di questo sottocomando, se si omette sia `-j` che `-p`, equivale a fornire `-j` e `-p`.

Esempio: Creazione di certificati autofirmati

In entrambi gli esempi si presuppone l'esistenza di un archivio chiavi in `/tmp/cell.ks` con la password `kspw`. L'archivio chiavi viene creato qualora non fosse già presente.

Nel presente esempio vengono creati nuovi certificati usando le impostazioni predefinite. Il nome dell'autorità emittente è impostato su `CN=Unknown`. Il certificato utilizza una lunghezza chiave a 2048 bit predefinita, che scade un anno dopo la sua creazione.

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

In questo esempio viene creato un nuovo certificato solo per l'endpoint `http`. Inoltre, specifica i valori personalizzati per la dimensione della chiave e il nome dell'autorità emittente. Il nome dell'autorità emittente è impostato su `CN=Test, L=London, C=GB`. Il nuovo certificato per la connessione `http` ha una chiave a 4096 bit, che scade 90 giorni dopo la sua creazione. Il certificato esistente per l'endpoint proxy della console rimane inalterato.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool generate-certs -j -o /tmp/cell.ks -w kspw -i "CN=Test, L=London, C=GB" -s 4096 -x 90
New keystore created and written to /tmp/cell.ks.
```

Importante Il file di 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.

Sostituzione di certificati per gli endpoint proxy della console e HTTP

Utilizzare il comando `certificates` dello strumento di gestione delle celle per sostituire i certificati SSL per gli endpoint proxy della console e HTTP.

Il comando `certificates` dello strumento di gestione delle celle automatizza la procedura di sostituzione dei certificati esistenti con quelli nuovi memorizzati nell'archivio chiavi JCEKS. Utilizzare il comando `certificates` per sostituire i certificati autofirmati con certificati firmati o sostituire i certificati che stanno per scadere con nuovi certificati. Per creare un archivio chiavi JCEKS che contenga i certificati firmati, vedere [Creazione di certificati SSL autofirmati per vCloud Director in Linux](#).

Per sostituire i certificati SSL in uno o entrambi gli endpoint, utilizzare un comando con il seguente formato:

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

Tabella 10-8. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `certificates`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--config (-c)</code>	percorso completo del file <code>global.properties</code> della cella	Impostazione predefinita: <code>\$VCLLOUD_HOME/etc/global.properties</code> .
<code>--https (-j)</code>	Nessuno	Sostituisce il file di archivio chiavi nominato <code>certificates</code> utilizzato dall'endpoint <code>http</code> .
<code>--consoleproxyks (-p)</code>	Nessuno	Sostituisce il file di archivio chiavi nominato <code>proxycertificates</code> utilizzato dall'endpoint <code>proxy</code> della console.
<code>--responses (-r)</code>	percorso completo del file <code>responses.properties</code> della cella	L'impostazione predefinita è <code>\$VCLLOUD_HOME/etc/responses.properties</code> .
<code>--keystore (-k)</code>	<i>keystore-pathname</i>	Percorso completo dell'archivio chiavi JCEKS che contiene i certificati firmati. Forma abbreviata obsoleta di <code>-s</code> sostituita da <code>-k</code> .
<code>--keystore-password (-w)</code>	<i>keystore-password</i>	La password per l'archivio chiavi JCEKS a cui fa riferimento l'opzione <code>--keystore</code> . Sostituisce le opzioni obsolete <code>-kspassword</code> e <code>--keystorepwd</code> .

Esempio: Sostituzione dei certificati

È possibile omettere le opzioni `--config` e `--responses` a meno che i file non siano stati spostati dai percorsi predefiniti. In questo esempio si presuppone l'esistenza di un archivio chiavi in `/tmp/my-new-certs.ks` con la password `kspw`. In questo esempio il certificato dell'endpoint `http` esistente viene sostituito con quello trovato in `/tmp/my-new-certs.ks`

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

Nota Dopo aver sostituito i certificati è necessario riavviare la cella.

Importazione di certificati SSL da servizi esterni

Utilizzare il comando `import-trusted-certificates` dello strumento di gestione delle celle per importare certificati da utilizzare per stabilire connessioni protette a servizi esterni come AMQP e il database vCloud Director.

Per poter creare una connessione protetta a un servizio esterno, vCloud Director deve stabilire una catena di attendibilità valida per tale servizio importando i certificati del servizio all'interno del proprio archivio attendibilità. Per importare certificati attendibili nell'archivio attendibilità della cella, utilizzare un comando con il seguente formato:

```
cell-management-tool import-trusted-certificates options
```

Tabella 10-9. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `import-trusted-certificates`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--destination</code>	nome del percorso	Nome del percorso completo dell'archivio attendibilità di destinazione. Se non è indicato nella riga di comando, il valore predefinito è <code>/opt/vmware/vcloud-director/etc/certificates</code> .
<code>--destination-password</code>	stringa	Password dell'archivio attendibilità di destinazione. Se non viene specificata nella riga di comando, viene impostato come predefinito il valore di <code>vcloud.ssl.truststore.password</code> .

Tabella 10-9. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `import-trusted-certificates` (continua)

Opzione	Argomento	Descrizione
<code>--destination-type</code>	tipo di archivio chiavi	Tipo di archivio chiavi dell'archivio attendibilità di destinazione. Può essere JKS o JCEKS. L'impostazione predefinita è JCEKS.
<code>--force</code>	Nessuno	Sovrascrive i certificati esistenti nell'archivio attendibilità di destinazione.
<code>--source</code>	nome del percorso	Nome del percorso completo del file PEM di origine.

Esempio: Importazione di certificati attendibili

In questo esempio vengono importati i certificati da `/tmp/demo.pem` all'archivio chiavi locale di vCloud Director in `/opt/vmware/vcloud-director/etc/certificates`. vCloud Director archivia la password dell'archivio chiavi in un formato crittografato che il comando `import-trusted-certificates` consente di decrittografare.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool import-trusted-certificates --source /tmp/demo.pem
```

Gestione dell'elenco di crittografia SSL consentita

Utilizzare il comando `ciphers` dello strumento di gestione delle celle per configurare il set di pacchetti di crittografia messo a disposizione dalla cella, da utilizzare durante il processo di handshake SSL.

Quando un client effettua una connessione SSL a una cella vCloud Director, la cella mette a disposizione solo la crittografia configurata nell'elenco crittografia consentita predefinito. Diversi set di crittografia non sono inclusi nell'elenco in quanto potrebbero non essere abbastanza forti da proteggere la connessione oppure sono noti per determinare errori di connessione SSL. Quando si installa o si aggiorna vCloud Director, lo script di installazione o di aggiornamento esamina i certificati della cella. Se uno qualsiasi dei certificati è crittografato con una crittografia non inclusa nell'elenco della crittografia consentita, lo script modifica la configurazione della cella in modo da permettere l'uso di quella crittografia e visualizza un avviso. È possibile continuare a utilizzare i certificati esistenti nonostante dipendano da questa crittografia oppure si possono attuare i seguenti passaggi per sostituire i certificati e riconfigurare l'elenco della crittografia consentita:

- 1 Creare nuovi certificati che non utilizzano la crittografia non consentita. È possibile utilizzare `cell-management-tool ciphers -a`, come mostrato in [Elencare tutta la crittografia consentita](#) per elencare tutta la crittografia consentita nella configurazione predefinita.

- 2 Utilizzare il comando `cell-management-tool certificates` per sostituire i certificati esistenti della cella con quelli nuovi.
- 3 Utilizzare il comando `cell-management-tool ciphers` per riconfigurare l'elenco della crittografia consentita, per escludere la crittografia non utilizzata dai nuovi certificati. Escludendo questa crittografia, sarà più veloce stabilire una connessione SSL alla cella, poiché la crittografia disponibile durante l'handshake è ridotta al minimo.

Importante Poiché la console VMRC richiede l'utilizzo della crittografia AES256-SHA e AES128-SHA, non è possibile escluderla da quella consentita, se i client di vCloud Director utilizzano la console VMRC.

Per gestire l'elenco della crittografia SSL consentita, utilizzare una riga di comando con la seguente struttura:

```
cell-management-tool ciphers options
```

Tabella 10-10. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `ciphers`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--all-allowed (-a)</code>	Nessuno	Elencare tutta la crittografia consentita.
<code>--compatible-reset (-c)</code>	Nessuno	Ripristinare sui valori predefiniti l'elenco della crittografia consentita, inoltre, ammettere la crittografia utilizzata dai certificati di questa cella.
<code>--disallow (-d)</code>	Elenco separato da virgole dei nomi di crittografia, come pubblicato all'indirizzo https://www.openssl.org/docs/man1.0.2/man1/ciphers.html	Escludere la crittografia nell'elenco separato da virgole specificato.
<code>--list (-l)</code>	Nessuno	Elencare la crittografia attualmente configurata.
<code>--reset (-r)</code>	Nessuno	Ripristinare sui valori predefiniti l'elenco della crittografia consentita. Se i certificati di questa cella utilizzando la crittografia non consentita, non sarà possibile effettuare una connessione SSL alla cella finché non vengono installati nuovi certificati che utilizzando una crittografia consentita.

Esempio: Elencare tutta la crittografia consentita

Utilizzare l'opzione `--all-allowed (-a)` per elencare tutta la crittografia che la cella può mettere a disposizione durante un handshake SSL.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
* TLS_DHE_DSS_WITH_AES_256_CBC_SHA
* TLS_DHE_DSS_WITH_AES_128_CBC_SHA
* TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
* TLS_DHE_RSA_WITH_AES_256_CBC_SHA
* TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

Esempio: Esclusione di due tipi di crittografia

Utilizzare l'opzione `--disallow (-d)` per rimuovere uno o più tipi di crittografia dall'elenco della crittografia consentita. Quest'opzione richiede almeno un nome di crittografia. È possibile fornire più nomi di crittografia in un elenco separato da virgole. È possibile ottenere i nomi per questo elenco dall'output di `ciphers -a`. In questo esempio vengono rimossi due tipi di crittografia elencati nell'esempio precedente.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -d
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

Gestione dell'elenco dei protocolli SSL consentiti

Utilizzare il comando `ssl-protocols` dello strumento di gestione delle celle per configurare il set di protocolli SSL messo a disposizione dalla cella per l'utilizzo durante il processo di handshake SSL.

Quando un client effettua una connessione SSL a una cella vCloud Director, la cella mette a disposizione solo i protocolli configurati nell'elenco dei protocolli SSL consentiti. Diversi protocolli, inclusi TLSv1, SSLv3 e SSLv2Hello, non sono inclusi nell'elenco dei protocolli predefiniti perché sono noti per contenere gravi vulnerabilità della sicurezza.

Per gestire l'elenco dei protocolli SSL consentiti, utilizzare una riga di comando con la seguente struttura:

```
cell-management-tool ssl-protocols options
```

Tabella 10-11. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `ssl-protocols`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--all-allowed (-a)</code>	Nessuno	Elenco dei protocolli SSL supportati da vCloud Director.
<code>--disallow (-d)</code>	Elenco separato da virgole dei nomi dei protocolli SSL.	Consente di riconfigurare l'elenco dei protocolli SSL non consentiti con quelli specificati nell'elenco.
<code>--list (-l)</code>	Nessuno	Elenco dei set di protocolli SSL consentiti, correntemente supportati da vCloud Director.
<code>--reset (-r)</code>	Nessuno	Reimpostazione dell'elenco dei protocolli SSL configurati alle impostazioni di fabbrica

Importante Dopo avere eseguito `ssl-protocols --disallow` o `ssl-protocols reset`, è necessario riavviare la cella.

Esempio: Elenco dei protocolli SSL consentiti e configurati

Utilizzare l'opzione `--all-allowed (-a)` per elencare tutti i protocolli SSL che la cella può mettere a disposizione durante un handshake SSL.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

* TLSv1.2
* TLSv1.1
* TLSv1
* SSLv3
* SSLv2Hello
```

Questo elenco è in genere un superset di protocolli SSL che la cella è in grado di supportare. Per ottenere un elenco dei protocolli SSL, utilizzare l'opzione `--list (-l)`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

* TLSv1.2
* TLSv1.1
```

Esempio: Riconfigurazione dell'elenco dei protocolli SSL non consentiti

Utilizzare l'opzione `--disallow (-d)` per riconfigurare l'elenco dei protocolli SSL non consentiti. Questa opzione richiede un elenco separato da virgole del subset di protocolli consentiti prodotto da `ssl-protocols -a`.

Questo esempio aggiorna l'elenco di protocolli SSL consentiti, includendo anche il protocollo TLSv1. Le release di VMware® vCenter™ precedenti alla 5.5 aggiornamento 3e richiedono TLSv1.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -d SSLv3,SSLv2Hello
```

Una volta eseguito questo comando, è necessario riavviare la cella.

Configurazione della raccolta di metriche

Utilizzare il comando `configure-metrics` dello strumento di gestione delle celle per configurare il set di metriche da raccogliere.

vCloud Director può raccogliere i valori che forniscono informazioni attuali e cronologiche relative alle prestazioni e all'utilizzo di risorse delle macchine virtuali. Utilizzare questo sottocomando per configurare le metriche raccolte da vCloud Director. Utilizzare il sottocomando `cell-management-tool cassandra` per configurare un database Apache Cassandra da utilizzare come repository delle metriche di vCloud Director. Vedere [Configurazione di un database delle metriche Cassandra](#).

Per configurare le metriche raccolte da vCloud Director, utilizzare una riga di comando con il seguente formato:

```
cell-management-tool configure-metrics --metrics-config pathname
```

Tabella 10-12. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `configure-metrics`

Comando	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--repository-host (obsoleto)</code>	Nome host o indirizzo IP dell'host KairosDB	Obsoleto. Utilizzare l'opzione <code>--cluster-nodes</code> del sottocomando <code>cell-management-tool cassandra</code> per configurare un database Apache Cassandra da utilizzare come repository delle metriche di vCloud Director.

Tabella 10-12. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `configure-metrics` (continua)

Comando	Argomento	Descrizione
<code>--repository-port</code> (obsoleto)	Porta KairosDB da utilizzare.	Obsoleto. Utilizzare l'opzione <code>--port</code> del sottocomando <code>cell-management-tool cassandra</code> per configurare un database Apache Cassandra da utilizzare come repository delle metriche di vCloud Director.
<code>--metrics-config</code>	nome del percorso	Percorso del file di configurazione delle metriche

Esempio: configurazione della connessione del database di valori

Nell'esempio seguente viene configurata la raccolta delle metriche nel modo specificato nel file `/tmp/metrics.groovy`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool configure-metrics --metrics-config /tmp/metrics.groovy
```

Il servizio di raccolta delle metriche di vCloud Director implementa un sottoinsieme delle metriche raccolte da vSphere Performance Manager. Per ulteriori informazioni sui nomi delle metriche e i parametri di raccolta, consultare la documentazione di vSphere Performance Manager. Nel file `metrics-config` sono elencati uno o più nomi di metriche e vengono forniti parametri di raccolta per ciascuna metrica presente nell'elenco. Ad esempio:

```
configuration {
    metric("cpu.usage.average")
    metric("cpu.usagemhz.average")
    metric("cpu.usage.maximum")
    metric("disk.used.latest") {
        currentInterval=300
        historicInterval=300
        entity="VM"
        instance=""
        minReportingInterval=1800
        aggregator="AVERAGE"
    }
}
```

Sono supportati i seguenti nomi di metriche.

Tabella 10-13. Nomi di metriche

Nome metrica	Descrizione
<code>cpu.usage.average</code>	Visualizzazione host dell'utilizzo attivo medio della CPU della macchina virtuale come percentuale del totale disponibile. Include tutti i core di tutti i socket.
<code>cpu.usagemhz.average</code>	Visualizzazione host dell'utilizzo attivo medio della CPU della macchina virtuale come misurazione non elaborata. Include tutti i core di tutti i socket.
<code>cpu.usage.maximum</code>	Visualizzazione host dell'utilizzo attivo massimo della CPU della macchina virtuale come percentuale del totale disponibile. Include tutti i core di tutti i socket.
<code>mem.usage.average</code>	Memoria utilizzata dalla macchina virtuale come percentuale della memoria configurata totale.
<code>disk.provisioned.latest</code>	Spazio di storage allocato al disco rigido virtuale nel virtual data center dell'organizzazione che lo contiene.
<code>disk.used.latest</code>	Spazio di storage utilizzato da tutti i dischi rigidi virtuali.
<code>disk.read.average</code>	Velocità di lettura media per tutti i dischi rigidi virtuali.
<code>disk.write.average</code>	Velocità di scrittura media per tutti i dischi rigidi virtuali.

Nota Quando in una macchina virtuale sono presenti più dischi, le metriche vengono riportate sotto forma di aggregato per tutti i dischi. Le metriche relative alla CPU sono un aggregato di tutti i core e tutti i socket.

Per ciascuna metrica denominata, è possibile specificare i seguenti parametri di raccolta.

Tabella 10-14. Parametri di raccolta delle metriche

Nome parametro	Valore	Descrizione
<code>currentInterval</code>	Numero intero di secondi.	L'intervallo, espresso in secondi, da utilizzare durante l'esecuzione delle query per il recupero dei valori delle metriche più recenti disponibili (per le query relative alle metriche correnti). Se non si specifica alcun valore, viene utilizzato il valore predefinito 20. I valori superiori a 20 sono supportati solo per le metriche di livello 1, come definito da vSphere Performance Manager.
<code>historicInterval</code>	Numero intero di secondi.	L'intervallo, espresso in secondi, da utilizzare durante l'esecuzione delle query per il recupero dei valori della cronologia delle metriche. Se non si specifica alcun valore, viene utilizzato il valore predefinito 20. I valori superiori a 20 sono supportati solo per le metriche di livello 1, come definito da vSphere Performance Manager.
<code>entity</code>	Uno dei seguenti valori: HOST, VM	Il tipo di oggetto VC per il quale è disponibile la metrica. Se non si specifica alcun valore, viene utilizzato il valore predefinito VM. Non tutte le metriche sono disponibili per tutte le entità.

Tabella 10-14. Parametri di raccolta delle metriche (continua)

Nome parametro	Valore	Descrizione
instance	L'identificatore di un'istanza PerfMetricId di vSphere Performance Manager.	Indica se recuperare i dati per singole istanze di una metrica (ad esempio, per i singoli core di una CPU), per un aggregato di tutte le istanze o entrambi. Il valore "*" raccoglie tutte le metriche, ovvero le singole istanze e l'aggregato. Una stringa vuota "" raccoglie solo i dati aggregati. Una stringa specifica, ad esempio "DISKFILE", raccoglie solo i per tale istanza. Se non diversamente specificato, il valore predefinito è "*" .
minReportingInterval	Numero intero di secondi.	Specifica un intervallo di aggregazione predefinito, espresso in secondi, da utilizzare durante la creazione di report relativi a dati di serie temporali. Questo parametro consente un maggiore controllo sulla granularità dei report, quando la granularità dell'intervallo di raccolta non è sufficiente. Se non viene indicato alcun intervallo dedicato per la creazione dei report, il valore predefinito è 0.
aggregator	Uno dei seguenti valori: AVERAGE, MINIMUM, MAXIMUM, SUMMATION	Il tipo di aggregazione da eseguire durante l'intervallo specificato in minReportingInterval. Se non diversamente specificato, il valore predefinito è AVERAGE.

Configurazione di un database delle metriche Cassandra

Utilizzare il comando `cassandra` dello strumento di gestione delle celle per connettere la cella a un database delle metriche facoltativo.

vCloud Director può raccogliere i valori che forniscono informazioni attuali e cronologiche relative alle prestazioni e all'utilizzo di risorse delle macchine virtuali. Utilizzare questo sottocomando per configurare un database Apache Cassandra da utilizzare come repository delle metriche di vCloud Director. Utilizzare il sottocomando `cell-management-tool configure-metrics` per configurare il set di metriche da raccogliere. Vedere [Configurazione della raccolta di metriche](#).

I dati delle metriche cronologiche vengono archiviati in un database Apache Cassandra. Per ulteriori informazioni sulla configurazione di software di database opzionale per l'archiviazione e il recupero delle metriche relative alle prestazioni, vedere [Installazione e configurazione di un database Cassandra per l'archiviazione dei dati relativi alle metriche cronologiche](#).

Per creare una connessione tra vCloud Director e un database Apache Cassandra, utilizzare una riga di comando con il seguente formato:

```
cell-management-tool cassandra options
```

Tabella 10-15. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `cassandra`

Comando	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo delle opzioni disponibili per questo comando.
<code>--add-rollup</code>	Nessuno	Aggiorna lo schema di metriche per includere le metriche con rollup. Vedere Installazione e configurazione di un database Cassandra per l'archiviazione dei dati relativi alle metriche cronologiche .
<code>--cluster-nodes</code>	<i>address [, address ...]</i>	Elenco separato da virgole di nodi del cluster Cassandra da utilizzare per le metriche di vCloud Director.
<code>--clean</code>	Nessuno	Rimuove le impostazioni di configurazione di Cassandra dal database di vCloud Director.
<code>--configure</code>	Nessuno	Configura vCloud Director per l'utilizzo con un cluster Cassandra esistente.
<code>--dump</code>	Nessuno	Esegue il dump della configurazione della connessione corrente.
<code>--keyspace</code>	stringa	Imposta il nome dello spazio delle chiavi di vCloud Director in Cassandra su <i>string</i> . Impostazione predefinita: <code>vcloud_metrics</code> .
<code>--offline</code>	Nessuno	Configura Cassandra per l'utilizzo da parte di vCloud Director, ma non esegue il test della configurazione tramite connessione a vCloud Director.
<code>--password</code>	stringa	Password dell'utente del database Cassandra
<code>--port</code>	numero intero	Porta a cui effettuare la connessione in ciascun nodo del cluster. Impostazione predefinita: 9042.
<code>--ttl</code>	numero intero	Conserva i dati delle metriche per <i>integer</i> giorni. Impostare <i>integer</i> su 0 per conservare i dati delle metriche per sempre.

Tabella 10-15. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `cassandra` (continua)

Comando	Argomento	Descrizione
<code>--update-schema</code>	Nessuno	Inizializza lo schema di Cassandra per contenere i dati delle metriche di vCloud Director.
<code>--username</code>	stringa	Il nome utente dell'utente del database Cassandra.

Esempio: Configurazione della connessione del database Cassandra

Utilizzare un comando simile al seguente, dove *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 'P@55w0rd' --ttl 15
```

Una volta completato questo comando, è necessario riavviare la cella.

Recupero della password dell'amministratore di sistema

Se si conoscono il nome utente e la password del database di vCloud Director, è possibile usare il comando `recover-password` dello strumento di gestione delle celle per recuperare la password dell'amministratore di sistema di vCloud Director.

Con il comando `recover-password` dello strumento di gestione delle celle, un utente che conosce il nome utente e la password del database di vCloud Director può recuperare la password dell'amministratore di sistema di vCloud Director.

Per recuperare la password dell'amministratore di sistema, usare un comando con la seguente struttura:

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

Tabella 10-16. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `recover-password`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--dbuser</code>	Il nome utente dell'utente del database di vCloud Director.	Deve essere specificato con la riga di comando.
<code>--dbpassword</code>	La password dell'utente del database di vCloud Director.	Se non fornita, viene richiesta.

Aggiornamento dello stato di errore di un task

Utilizzare il comando `fail-tasks` dello strumento di gestione delle celle per aggiornare lo stato di completamento associato ai task che erano in esecuzione quando la cella è stata deliberatamente chiusa. Non è possibile utilizzare il comando `fail-tasks` se tutte le celle non sono state chiuse.

Quando si disattiva una cella utilizzando il comando `cell-management-tool -q`, i task in esecuzione dovrebbero terminare in modo normale entro pochi minuti. Se l'esecuzione dei task continua in una cella che è stata disattivata, l'utente con privilegi avanzati può chiudere la cella, forzando così errori di esecuzione dei task. Dopo che una chiusura ha forzato gli errori di esecuzione dei task, l'utente con privilegi avanzati può eseguire `cell-management-tool fail-tasks` per aggiornare lo stato di completamento di tali task. Questo tipo di aggiornamento dello stato di completamento di un task è facoltativo, ma aiuta a mantenere l'integrità dei registri di sistema identificando chiaramente gli errori causati da un'azione dell'amministratore.

Per generare un elenco di task ancora in esecuzione in una cella disattivata, utilizzare una riga di comando con la seguente struttura:

```
cell-management-tool -u sysadmin-username cell --status-verbose
```

Tabella 10-17. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `fail-tasks`

Comando	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--message (-m)</code>	Testo messaggio.	Testo del messaggio da posizionare nello stato di completamento task.

Esempio: Errore del task in esecuzione sulla cella

In questo esempio, viene aggiornato lo stato di completamento di un task associato a un task che era ancora in esecuzione quando la cella è stata chiusa.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool fail-tasks -m "administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system, Organization: org1
Would you like to fail the tasks listed above?
```

Digitando **y**, si aggiorna il task con uno stato di completamento per **chiusura dell'amministratore**. Digitando **n**, si consente al task di continuare l'esecuzione.

Nota Se nella risposta vengono restituiti più task, stabilire se tutti non devono riuscire, oppure non fare nulla. Non è possibile scegliere la non riuscita di un sottoinsieme di task.

Configurazione della gestione dei messaggi di controllo

Utilizzare il comando `configure-audit-syslog` dello strumento di gestione delle celle per configurare la modalità di registrazione dei messaggi di controllo da parte del sistema.

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` di Linux, oltre che al database di vCloud Director.

Lo script di configurazione del sistema consente di specificare la modalità di gestione dei messaggi di controllo. Vedere "Configurazione delle connessioni di rete e di database" nella *Guida all'installazione e all'aggiornamento di vCloud Director*. Le opzioni di registrazione specificate durante la configurazione del sistema vengono conservate in due file: `global.properties` e `responses.properties`. È possibile modificare la configurazione relativa alla registrazione dei messaggi di controllo in entrambi i file mediante una riga di comando dello strumento di gestione delle celle con la seguente struttura:

```
cell-management-toolconfigure-audit-syslog options
```

Le modifiche apportate mediante questo sottocomando dello strumento di gestione delle celle vengono mantenute nei file `global.properties` e `responses.properties` della cella. Le modifiche saranno effettive solo dopo il riavvio della cella.

Tabella 10-18. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `configure-audit-syslog`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--disable (-d)</code>	Nessuno	Disabilita la registrazione degli eventi di controllo su <code>syslog</code> . Registra gli eventi di controllo solo sul database di vCloud Director. Questa opzione annulla l'impostazione dei valori delle proprietà <code>audit.syslog.host</code> e <code>audit.syslog.port</code> in <code>global.properties</code> e <code>responses.properties</code> .
<code>--syslog-host (-loghost)</code>	Indirizzo IP o nome di dominio completo dell'host del server <code>syslog</code>	Questa opzione imposta il valore della proprietà <code>audit.syslog.host</code> sull'indirizzo o il nome di dominio completo specificati.
<code>--syslog-port (-logport)</code>	Numero intero compreso nell'intervallo 0-65535	Questa opzione imposta il valore della proprietà <code>audit.syslog.port</code> sul numero intero specificato.

Quando si specifica un valore per `--syslog-host`, `--syslog-port` o entrambi, il comando verifica che il valore specificato sia nel formato corretto, ma non verifica la combinazione di host e porta per l'accessibilità alla rete o la presenza di un servizio syslog in esecuzione.

Esempio: modifica del nome host del server syslog

Importante Le modifiche apportate mediante questo comando vengono scritte nel file di configurazione globale e nel file di risposta. Prima di utilizzare questo comando, verificare che il file di risposta sia presente nel percorso `/opt/vmware/vcloud-director/etc/responses.properties` e sia scrivibile. Vedere la sezione relativa alla protezione e al riutilizzo del file di risposta nella *Guida all'installazione e all'aggiornamento di vCloud Director*.

Per modificare l'host a cui sono inviati i messaggi syslog, utilizzare un comando come quello descritto di seguito:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool configure-audit-syslog --loghost
syslog.example.com
Using default port 514
```

Questo esempio presuppone che il nuovo host cerchi i messaggi syslog sulla porta predefinita.

Il comando aggiorna `global.properties` e `responses.properties`, ma le modifiche saranno effettive solo dopo il riavvio della cella.

Configurazione dei modelli e-mail

Utilizzare il comando `manage-email` dello strumento di gestione delle celle per gestire i modelli utilizzati dal sistema durante la creazione degli avvisi e-mail.

Per impostazione predefinita, il sistema è configurato per l'invio di avvisi e-mail che informano gli amministratori di sistema in caso di eventi e condizioni che richiedono probabilmente il loro intervento. L'elenco di destinatari e-mail può essere aggiornato mediante console Web o API di vCloud. È possibile sovrascrivere il contenuto predefinito del messaggio e-mail per ciascun tipo di avviso mediante una riga di comando dello strumento di gestione delle celle con la seguente struttura:

```
cell-management-tool manage-email options
```

Tabella 10-19. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `manage-email`

Opzione	Argomento	Descrizione
<code>--help</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--delete</code>	Nome modello	Il nome del modello da eliminare.

Tabella 10-19. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `manage-email` (continua)

Opzione	Argomento	Descrizione
<code>--lookup</code>	Nome modello	Questo argomento è facoltativo. Se non viene fornito, il comando restituisce un elenco di tutti i nomi di modelli.
<code>--locale</code>	Impostazioni internazionali del modello	Per impostazione predefinita, questo comando agisce su modelli con impostazioni internazionali en-US. Utilizzare questa opzione per specificare impostazioni internazionali diverse.
<code>--set-template</code>	Nome del percorso di un file contenente un modello e-mail aggiornato	Questo file deve essere accessibile sull'host locale e leggibile dall'utente <code>vcloud.vcloud</code> . Ad esempio, <code>/tmp/my-email-template.txt</code>

Esempio: Aggiornare un modello di e-mail

Il comando seguente sostituisce il contenuto corrente del modello e-mail

`DISK_STORAGE_ALERT_VDCS` con il contenuto creato in un file denominato `/tmp/`

`DISK_STORAGE_ALERT_VDCS-new.txt`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-email --set-template
DISK_STORAGE_ALERT_VDCS /tmp/DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s): $pvdcList
"

Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from $productName
The $datastore is used by the followingProvider VDC(s): $pvdcList
"

VCD Email notification details:
name           : DISK_STORAGE_ALERT_VDCS
description    : Alert when used disk storage exceeds threshold
config key     : email.template.DISK_STORAGE_ALERT_VDCS.en-US
template placeholders : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcList]
template content      : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcList
```

Individuazione di macchine virtuali orfane

Utilizzare il comando `find-orphan-vm` dello strumento di gestione delle celle per trovare riferimenti a macchine virtuali presenti nel database di vCenter ma non nel database di vCloud Director.

Le macchine virtuali a cui si fa riferimento nel database di vCenter ma non nel database di vCloud Director sono considerate macchine virtuali orfane in quanto vCloud Director non può accedervi nonostante la possibilità che stiano utilizzando risorse di elaborazione e di storage. Questo tipo di mancata corrispondenza nei riferimenti può verificarsi per diversi motivi, tra cui carichi di lavoro di grandi dimensioni, errori nel database e interventi dell'amministratore. Il comando `find-orphan-vm` consente all'amministratore di elencare le macchine virtuali in modo che possano essere rimosse o reimportate in vCloud Director. Tale comando consente di specificare un archivio affidabilità, che potrebbe essere necessario qualora si stia lavorando con installazioni di vCloud Director o vCenter che utilizzano certificati autofirmati.

Utilizzare un comando con la seguente struttura:

```
cell-management-tool find-orphan-vm options
```

Tabella 10-20. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `find-orphan-vm`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--enableVerifyHostname</code>	Nessuno	Consente la verifica del nome host come parte dell'handshake SSL.
<code>--host</code>	Obbligatorio	Indirizzo IP o nome di dominio completo dell'installazione di vCloud Director per l'individuazione delle macchine virtuali orfane.
<code>--output-file</code>	Nome percorso o -	Nome completo del percorso del file in cui si desidera scrivere l'elenco di macchine virtuali orfane. Specificare un nome del percorso di - per scrivere l'elenco nell'output standard.
<code>--password (-p)</code>	Obbligatorio	Password dell'amministratore di sistema di vCloud Director.
<code>--port</code>	Porta HTTPS di vCloud Director.	Specificare questo valore solo se non si desidera che il comando utilizzi la porta HTTPS predefinita di vCloud Director.

Tabella 10-20. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `find-orphan-vm` (continua)

Opzione	Argomento	Descrizione
<code>--trustStore</code>	Nome completo del percorso di un file di archivio affidabilità Java.	Specificare questo valore solo se non si desidera che il comando utilizzi il file di archivio affidabilità vCloud Director predefinito.
<code>--trustStorePassword</code>	Password per il <code>--trustStore</code> specificato	Necessaria solo se si utilizza <code>--trustStore</code> per specificare un file di archivio affidabilità alternativo.
<code>--trustStoreType</code>	Il tipo di <code>--trustStore</code> specificato (PKCS12, JCEKS, ...)	Necessario solo se si utilizza <code>--trustStore</code> per specificare un file di archivio affidabilità alternativo.
<code>--user (-u)</code>	Obbligatorio	Nome utente dell'amministratore di sistema di vCloud Director.
<code>--vc-name</code>	Obbligatorio	Nome di vCenter per l'individuazione delle macchine virtuali orfane.
<code>--vc-password</code>	Obbligatorio	Password dell'amministratore di vCenter:
<code>--vc-user</code>	Obbligatorio	Nome utente dell'amministratore di vCenter.

Esempio: individuazione di macchine virtuali orfane

In questo esempio viene eseguita una query su un singolo server vCenter. Poiché `--output-file` è specificato come `-`, i risultati vengono restituiti in un output standard.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vm \
--host 10.20.30.40 -u vadmin -vc-name vcenter1 -vc-password P055w0rd --vc-user admin --output-file -
Querying for VC by name 10.20.30.40
Querying all vdc's associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc->resource pool mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc->VM Moref mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Processing 956 VM's on 5 VDC's across 20 resource pools
Analysis complete.
VDC: "ExampleOrgVDC [urn:vcloud:vdc:1a97...]" (org: "ExampleOrg") ResPool: primary (1a97...) [moref:
"resgroup-30515"]
The following 22 orphan VMs were discovered:
Orphan VM: "indDisk100-0-95411 (cbc358a0-e199-4024-8fff-2e5cfce20953)" (parent name: "Test VMs",
parent moref : "group-v30533")
...
Orphan VM: "indDisk12-0-51259 (0bbb4115-673e-4c84-ba26-6875159655e0)" (parent name: "Test VMs",
parent moref : "group-v30533")
```

Attivazione o disattivazione della partecipazione al programma CEIP VMware

Per partecipare o uscire dal programma CEIP di VMware, è possibile utilizzare il sottocomando `configure-ceip` dello strumento di gestione delle celle.

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 <http://www.vmware.com/trustvmware/ceip.html>. 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.

```
cell-management-tool
configure-ceip
options
```

Se si preferisce non partecipare al programma CEIP di VMware per questo prodotto specifico, eseguire il seguente comando con l'opzione `--disable`.

Tabella 10-21. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `configure-ceip`

Opzione	Argomento	Descrizione
<code>--help</code> (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--disable</code>	Nessuno	Disattiva la partecipazione al programma CEIP di VMware.
<code>--enable</code>	Nessuno	Attiva la partecipazione al programma CEIP di VMware.
<code>--status</code>	Nessuno	Visualizza lo stato di partecipazione corrente al programma CEIP di VMware.

Esempio: disattivazione della partecipazione al programma CEIP VMware

Per disattivare la partecipazione al programma CEIP di VMware, utilizzare un comando con il formato seguente:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
disableParticipation disabled
```

Dopo l'esecuzione del comando, il sistema smette di inviare informazioni al programma CEIP VMware.

Per verificare lo stato di partecipazione corrente al programma CEIP di VMware, utilizzare un comando con il formato seguente:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
statusParticipation disabled
```

Aggiornamento delle impostazioni di configurazione dell'applicazione

Con il sottocomando `manage-config` dello strumento di gestione delle celle è possibile aggiornare le diverse impostazioni di configurazione dell'applicazione, come le attività di limitazione del catalogo.

Tabella 10-22. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `manage-config`

Opzione	Argomento	Descrizione
<code>--help (-h)</code>	Nessuno	Fornisce un riepilogo delle opzioni disponibili con questo sottocomando.
<code>--delete (-d)</code>	Nessuno	Rimuove l'impostazione di configurazione di destinazione.
<code>--lookup (-l)</code>	Nessuno	Cerca il valore dell'impostazione di configurazione di destinazione.
<code>--name (-n)</code>	Nome dell'impostazione di configurazione	Nome dell'impostazione di configurazione di destinazione. Obbligatorio con le opzioni <code>-d</code> , <code>-l</code> e <code>-v</code> .
<code>--value (-v)</code>	Valore dell'impostazione di configurazione	Aggiunge o aggiorna il valore dell'impostazione di configurazione di destinazione.

Ad esempio, è possibile utilizzare il sottocomando `manage-config` per [Configurazione della limitazione della sincronizzazione del catalogo](#).

Configurazione della limitazione della sincronizzazione del catalogo

Quando si dispone di numerosi elementi del catalogo pubblicati o sottoscritti da altre organizzazioni, per evitare il sovraccarico del sistema durante le sincronizzazioni del catalogo è possibile configurare la limitazione della sincronizzazione del catalogo. È possibile utilizzare il sottocomando `manage-config` dello strumento di gestione delle celle per configurare la limitazione della sincronizzazione del catalogo limitando il numero di elementi della libreria che possono essere sincronizzati contemporaneamente.

Quando un catalogo sottoscritto avvia una sincronizzazione del catalogo, il catalogo pubblicato scarica innanzitutto gli elementi della libreria dal repository di vCenter Server verso lo storage del servizio di trasferimento di vCloud Director, quindi crea i collegamenti di download per il catalogo sottoscritto. È possibile limitare il numero di elementi della libreria che tutti i cataloghi pubblicati possono scaricare contemporaneamente. È possibile limitare il numero di elementi della libreria che tutti i cataloghi sottoscritti possono sincronizzare contemporaneamente. È possibile limitare il numero di elementi della libreria che un singolo catalogo sottoscritto può sincronizzare contemporaneamente.

È possibile utilizzare il sottocomando `manage-config` dello strumento di gestione delle celle per aggiornare le impostazioni di configurazione per la limitazione del catalogo. Per informazioni sull'utilizzo del sottocomando `manage-config`, vedere [Aggiornamento delle impostazioni di configurazione dell'applicazione](#).

Tabella 10-23. Impostazioni di configurazione per la limitazione del catalogo

Impostazione di configurazione	Valore predefinito	Descrizione
<code>vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit</code>	30	Limite di elementi della libreria che tutti i cataloghi pubblicati nell'istanza di vCloud Director possono scaricare da vCenter Server a vCloud Director contemporaneamente. Se il numero totale di elementi della libreria pubblicati per il download nell'istanza di vCloud Director supera questo limite, gli elementi della libreria vengono suddivisi in parti in base a questo limite e scaricati in sequenza.
<code>vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit</code>	30	Limite di elementi della libreria che tutti i cataloghi sottoscritti in un'istanza di vCloud Director possono sincronizzare contemporaneamente. Se il numero totale di elementi della libreria sottoscritti per la sincronizzazione nell'istanza di vCloud Director supera questo limite, gli elementi vengono suddivisi in parti in base a questo limite e sincronizzati in sequenza.
<code>contentLibrary.item.sync.batch.size</code>	10	Limite di elementi della libreria che un singolo catalogo sottoscritto può sincronizzare contemporaneamente. Se un catalogo sottoscritto tenta di sincronizzare un numero di elementi della libreria maggiore di questo limite, gli elementi vengono suddivisi in parti in base a questo limite e sincronizzati in sequenza.

Esempio: Configurazione della limitazione di sincronizzazione per cataloghi sottoscritti

Il comando seguente imposta un limite di cinque elementi della libreria che un singolo catalogo sottoscritto può sincronizzare contemporaneamente.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n  
contentLibrary.item.sync.batch.size -v 5
```

Se un catalogo sottoscritto contiene 13 elementi della libreria, la sincronizzazione del catalogo viene eseguita in tre parti in sequenza. La prima parte conterrà cinque elementi, la seconda conterrà i successivi cinque elementi e l'ultima conterrà i rimanenti tre elementi.

Risoluzione dei problemi relativi all'accesso non riuscito all'interfaccia utente di vCloud Director

Per visualizzare e aggiornare le voci DNS e gli indirizzi IP validi per le celle di vCloud Director nell'ambiente di vCloud Director, è possibile utilizzare il sottocomando `manage-config` dello strumento di gestione delle celle.

Problema

Dopo un accesso riuscito, non è possibile passare al vCloud Director Service Provider Admin Portal o al vCloud Director Tenant Portal.

Dopo aver immesso le credenziali nella schermata di accesso, viene visualizzato il seguente messaggio di errore: **Impossibile avviare. Si è verificato un errore durante l'inizializzazione.** Ciò può essere causato da problemi come l'accesso all'applicazione tramite un URL pubblico non supportato o una connessione instabile.

Causa

vCloud Director utilizza un'implementazione del filtro CORS (Cross-Origin Resource Sharing) per gestire un elenco di tutti gli endpoint validi che è possibile utilizzare per accedere al Service Provider Admin Portal e al vCloud Director Tenant Portal.

L'elenco dei filtri CORS viene compilato e aggiornato durante la configurazione della cella. Contiene voci HTTP e HTTPS con indirizzi IP e nomi DNS per tutte le celle nel gruppo di server. Contiene inoltre un indirizzo IP pubblico utilizzato dal programma di bilanciamento del carico che si trova di fronte al gruppo di server di vCloud Director.

Durante la configurazione della cella delle distribuzioni dell'appliance, l'elenco non viene aggiornato con i nomi DNS delle celle di vCloud Director e non è possibile utilizzare il nome DNS di una cella per accedervi.

Soluzione

- 1 Accedere o accedere tramite SSH come **root** a una delle celle nel gruppo di server.

- 2 Per elencare gli URL validi che è possibile utilizzare per accedere alle celle di vCloud Director nell'ambiente, eseguire la seguente riga di comando.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
webapp.allowed.origins -l
```

L'output del sistema è un elenco che contiene le voci HTTP e HTTPS con indirizzi IP e nomi DNS per tutte le celle nel gruppo di server. Contiene inoltre un indirizzo IP pubblico utilizzato dal programma di bilanciamento del carico che si trova di fronte al gruppo di server di vCloud Director.

L'elenco è una stringa separata da virgole, senza spazi tra le voci.

- 3 (Facoltativo) Per aggiornare l'impostazione di configurazione `webapp.allowed.origins`, eseguire la seguente riga di comando. Nella riga di comando, il parametro del valore dell'impostazione è un elenco di indirizzi IP e nomi DNS in una stringa separata da virgole senza spazi tra le voci.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
webapp.allowed.origins -v "comma_separated_list_of_URLs_without_spaces"
```

Debug dell'individuazione delle macchine virtuali vCenter

Utilizzando il sottocomando `debug-auto-import` dello strumento di gestione delle celle, è possibile cercare di scoprire il motivo per cui il meccanismo di individuazione delle vApp ignora una o più macchine virtuali vCenter.

Nella configurazione predefinita, un VDC dell'organizzazione individua automaticamente le macchine virtuali vCenter create nei pool di risorse che supportano il VDC. Vedere le informazioni relative alla scoperta e all'adozione di vApp nella *Guida del portale di amministrazione del provider di servizi di vCloud Director*. Se una macchina virtuale vCenter non viene visualizzata in una vApp individuata, è possibile eseguire il sottocomando `debug-auto-import` per questa macchina virtuale o per il VDC.

```
cell-management-tool debug-auto-import options
```

Il sottocomando `debug-auto-import` restituisce un elenco di macchine virtuali vCenter e informazioni sui possibili motivi per cui queste vengono ignorate dal meccanismo di individuazione. L'elenco include anche le macchine virtuali vCenter rilevate ma che non sono state importate nel VDC dell'organizzazione.

Tabella 10-24. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `debug-auto-import`

Opzione	Argomento	Descrizione
<code>--help</code> (<code>-h</code>)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--org</code>	Nome organizzazione	Facoltativa. Elenca le informazioni relative alle macchine virtuali ignorate per l'organizzazione specificata.
<code>--vm</code>	Nome o parte del nome della macchina virtuale	Elenca le informazioni relative alle macchine virtuali ignorate che contengono il nome della macchina virtuale specificato. Facoltativa se viene utilizzata l'opzione <code>--org</code> .

Esempio: Debug dell'individuazione delle macchine virtuali vCenter in base al nome di macchina virtuale `test`

Il seguente comando restituisce informazioni sulle macchine virtuali vCenter ignorate in tutte le organizzazioni.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool debug-auto-import -vm test
```

```
VM with name:vm22-test (09ad258c-0cb0-4f69-a0a6-201cf3fe7d6b), moref vm-50 in VC testbed-vc can be skipped for the following reasons:
```

- 1) Virtual machine is already imported in vCD or is managed by vCD
- 2) Virtual machine is created by vCD

```
VM with name:test-vm1 (32210d0d-ef64-4637-b1d6-6400743a6bd9), moref vm-44 in VC testbed-vc can be skipped for the following reasons:
```

- 1) Virtual machine is not present in a vCD managed resource pool

```
VM with name:import-test3, moref vm-52inVC testbed-vc can be skippedforthe following reasons:
```

- 1) Virtual machine autoimport is either pending,in-progress or has failed and pendingforretry

In questo esempio, l'output di sistema restituisce informazioni relative a tre macchine virtuali vCenter ignorate dal meccanismo di individuazione e i cui nomi contengono la stringa `test`. La macchina virtuale `import-test3` è un esempio di macchina virtuale rilevata ma non importata nel VDC.

Rigenerazione degli indirizzi MAC per reti estese multisito

Se si associano due siti di vCloud Director configurati con lo stesso ID di installazione, possono verificarsi conflitti di indirizzi MAC nelle reti estese di questi siti. Per evitare tali conflitti, è necessario rigenerare gli indirizzi MAC in uno dei siti in base a un valore di inizializzazione personalizzato diverso dall'ID di installazione.

Durante la configurazione iniziale di vCloud Director, si imposta un ID di installazione. vCloud Director utilizza l'ID di installazione per generare indirizzi MAC per le interfacce di rete delle macchine virtuali. Due installazioni di vCloud Director configurate con lo stesso ID di installazione possono generare indirizzi MAC identici. Gli indirizzi MAC duplicati possono causare conflitti nelle reti estese tra i due siti associati.

Prima di creare reti estese tra i siti associati configurati con lo stesso ID di installazione, è necessario rigenerare gli indirizzi MAC in uno dei siti utilizzando il sottocomando `mac-address-management` dello strumento di gestione delle celle.

```
cell-management-tool mac-address-management options
```

Per generare nuovi indirizzi MAC, è necessario impostare un valore di inizializzazione personalizzato diverso dall'ID di installazione. Il valore di inizializzazione non sovrascrive l'ID di installazione, ma il database archivia il valore di inizializzazione più recente come secondo parametro di configurazione, che sostituisce l'ID di installazione.

Eseguire il sottocomando `mac-address-management` da un membro di vCloud Director arbitrario del gruppo di server. Il comando viene eseguito nel database di vCloud Director, in modo da poter eseguire il comando una sola volta per un gruppo di server.

Importante La rigenerazione di indirizzi MAC richiede un breve periodo di inattività di vCloud Director. Prima di avviare la rigenerazione, è innanzitutto necessario disattivare le attività di tutte le celle nel gruppo di server.

Tabella 10-25. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `mac-address-management`

Opzione	Argomento	Descrizione
<code>--help</code> (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
<code>--regenerate</code>	Nessuno	Elimina tutti gli indirizzi MAC che non sono in uso e genera nuovi indirizzi MAC basati sul valore di inizializzazione corrente. Se non esiste un valore di inizializzazione precedentemente impostato, gli indirizzi MAC vengono rigenerati in base all'ID di installazione. Gli indirizzi MAC che sono in uso vengono mantenuti.

Nota Tutte le celle nel gruppo di server devono essere inattive. Per informazioni sulla disattivazione delle attività in una cella, vedere [Gestione di una cella](#).

Tabella 10-25. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `mac-address-management` (continua)

Opzione	Argomento	Descrizione
<code>--regenerate-with-seed</code>	Un valore di inizializzazione compreso tra 0 e 63	Imposta un nuovo valore di inizializzazione personalizzato nel database, elimina tutti gli indirizzi MAC che non sono in uso e genera nuovi indirizzi MAC basati sul valore di inizializzazione appena impostato. Gli indirizzi MAC che sono in uso vengono mantenuti. Nota Tutte le celle nel gruppo di server devono essere inattive. Per informazioni sulla disattivazione delle attività in una cella, vedere Gestione di una cella .
<code>--show-seed</code>	Nessuno	Restituisce il valore di inizializzazione corrente e il numero di indirizzi MAC che sono in uso per ogni valore di inizializzazione.

Importante Gli indirizzi MAC che sono in uso vengono mantenuti. Per sostituire un indirizzo MAC in uso con un indirizzo MAC rigenerato, è necessario reimpostare l'indirizzo MAC dell'interfaccia di rete. Per informazioni sulla modifica delle proprietà della macchina virtuale, vedere *vCloud Director Tenant Portal Guide*.

Esempio: Rigenerazione degli indirizzi MAC in base a un nuovo valore di inizializzazione personalizzato

Il comando seguente imposta il valore di inizializzazione corrente su 9 e rigenera tutti gli indirizzi MAC che non sono in uso in base al valore di inizializzazione appena impostato:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --
regenerate-with-seed 9
Successfully removed 65,535 unused MAC addresses.
Successfully generated new MAC addresses.
```

Esempio: Visualizzazione del valore di inizializzazione corrente e del numero di indirizzi MAC in uso per ogni valore di inizializzazione

Il comando seguente restituisce informazioni relative al valore di inizializzazione corrente e il numero di indirizzi MAC per valore di inizializzazione:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --show-seed
Current MAC address seed is '9' and based on MacAddressSeed config.
MAC address seed    9 is in use by    12 MAC addresses
MAC address seed    1 is in use by     1 MAC addresses
```

In questo esempio, l'output del sistema indica che 9 è il valore di inizializzazione corrente su cui sono basati 12 indirizzi MAC. Inoltre, è presente un indirizzo MAC basato su un valore di inizializzazione precedente o sull'ID di installazione 1.

Aggiornamento degli indirizzi IP del database nelle celle di vCloud Director

È possibile utilizzare lo strumento di gestione delle celle per aggiornare gli indirizzi IP delle celle di vCloud Director in un cluster a elevata disponibilità del database.

Prerequisiti

Per aggiornare gli indirizzi IP delle celle in un cluster a elevata disponibilità del database, è necessario fornire l'indirizzo IP del nodo primario corrente. Per trovare l'indirizzo IP, controllare lo stato del cluster per individuare quale nodo ha il ruolo primario. Il nodo deve essere in esecuzione. Da tale riga, utilizzare il valore dell'host dalla colonna *Stringa di connessione* per identificare l'indirizzo IP. Vedere [Controllo dello stato di un cluster a disponibilità elevata del database](#).

Procedura

- 1 Accedere o accedere tramite SSH come **root** al sistema operativo di una delle celle nel cluster.
- 2 Verificare che la cella sia in esecuzione in tale nodo.

```
service vmware-vcd pid cell
```

Se l'ID del processo della cella non è NULL, la cella di vCloud Director è in esecuzione ed è possibile modificare l'indirizzo IP del database senza riavviare la cella di vCloud Director.

- 3 Per aggiornare gli indirizzi IP in tutte le celle nel gruppo di server, eseguire il comando seguente:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address --pid cell process ID --remote-sudo-user postgres --private-key-path /opt/vmware/vcloud-director/id_rsa
```

L'output del sistema indica la corretta riconfigurazione.

- 4 (Facoltativo) Verificare che ogni cella di vCloud Director faccia riferimento all'indirizzo IP del database corretto.

```
grep "database.jdbcUrl" /opt/vmware/vcloud-director/etc/global.properties
```

L'output del sistema indica che la cella è aggiornata.

- 5 Se una delle celle non è aggiornata, eseguire il comando per riconfigurarla.

- Se la cella non è in esecuzione, eseguire il comando seguente:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host  
primary node IP address
```

- Se la cella è in esecuzione, eseguire il comando seguente:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host  
primary node IP address -i cell process ID
```

- 6 Se si riconfigura una cella che non è in esecuzione, eseguire il comando per riavviare il servizio vmware-vcd.

- a Eseguire il comando per arrestare il servizio.

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

- b Eseguire il comando per avviare il servizio.

```
systemctl start vmware-vcd
```


Dopo avere installato vCloud Director o distribuito l'appliance vCloud Director

11

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.

Dopo la creazione dell'appliance vCloud Director, è possibile utilizzare le funzionalità di rete di vSphere per aggiungere una nuova scheda interfaccia di rete (NIC). Vedere l'argomento sull'[aggiunta di una scheda di rete a una macchina virtuale](#) nella guida *Amministrazione delle macchine virtuali vSphere*.

Questo capitolo include i seguenti argomenti:

- [Installazione dei file Microsoft Sysprep nei server](#)
- [Modifica del fuso orario dell'appliance di vCloud Director](#)
- [Personalizzazione degli indirizzi pubblici](#)
- [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 11-1. 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 `vcloud.vcloud`.

A tal fine, utilizzare il comando `chown` di Linux.

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

Modifica del fuso orario dell'appliance di vCloud Director

Dopo aver distribuito correttamente l'appliance di vCloud Director, è possibile modificare il fuso orario di sistema dell'appliance. Tutte le istanze dell'appliance di vCloud Director nel gruppo di server e nello storage del server di trasferimento devono utilizzare le stesse impostazioni.

Prerequisiti

- Distribuire l'appliance di vCloud Director. Vedere [Capitolo 6 Distribuzione dell'appliance vCloud Director](#).
- Modificare il fuso orario dello storage del server di trasferimento nel nuovo fuso orario dell'appliance vCloud Director primaria.

Procedura

- 1 Utilizzando una console Web o una console remota per il nodo primario, in basso a sinistra della finestra della console, selezionare **Imposta fuso orario**.
- 2 Selezionare una posizione, un paese e una regione del fuso orario.
Il fuso orario appena selezionato viene visualizzato in basso a sinistra della finestra della console.
- 3 Accedere alla console dell'appliance di vCloud Director come utente **root**.
- 4 Per assicurarsi che l'appliance di vCloud Director utilizzi il nuovo fuso orario, riavviare il servizio `vmware-vcd`.
- 5 Ripetere dal [passaggio 1](#) al [Passaggio passaggio 4](#) per tutte le celle di standby e di applicazione nella distribuzione di vCloud Director.

Personalizzazione degli indirizzi pubblici


Per soddisfare i requisiti del bilanciamento del carico o del proxy, è possibile modificare gli indirizzi Web degli endpoint predefiniti per il portale Web di vCloud Director, l'API di vCloud 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 [Passaggio 6](#).

Prerequisiti

Solo l'**amministratore di sistema** può personalizzare gli endpoint pubblici.

Procedura

- 1 Dal menu principale () , selezionare **Amministrazione**.
- 2 Nel pannello sinistro, in **Impostazioni**, fare clic su **Indirizzi pubblici**.
- 3 Fare clic su **Modifica** per personalizzare gli endpoint pubblici.

4 Per personalizzare gli URL di vCloud Director, modificare gli endpoint del **Portale Web**.

- a Immettere un URL pubblico di vCloud Director personalizzato per le connessioni HTTP (non sicure).
- b Immettere un URL pubblico di vCloud Director personalizzato per le connessioni HTTPS (sicure) e fare clic su **Carica** per caricare i certificati che stabiliscono la catena di attendibilità per l'endpoint.

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 `consoleproxy`. La terminazione SSL delle connessioni del proxy della console in un bilanciamento del carico non è supportata. La catena di certificati deve includere un certificato di endpoint, certificati intermedi e un certificato root nel formato PEM senza una chiave privata.

5 (Facoltativo) Per personalizzare l'API REST di vCloud e gli URL di OpenAPI, disattivare l'opzione **Usa impostazioni portale Web**.

- 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 **Carica** 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.

6 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.

Ad esempio, per l'istanza di un'appliance vCloud Director con nome di dominio completo `vcloud.example.com`, immettere **`vcloud.example.com:8443`**.

vCloud Director utilizza l'indirizzo del proxy della console quando viene aperta una finestra di console remota in una macchina virtuale.

7 Per salvare le modifiche, fare clic su **Salva**.

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 'P@55w0rd' --ttl 15
```

Per informazioni sull'utilizzo dello strumento di gestione delle celle, vedere [Capitolo 10 Guida di riferimento allo strumento di gestione delle celle](#).

- 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 [Capitolo 10 Guida di riferimento allo strumento di gestione delle celle](#).

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.

Eseguire l'aggiornamento di vCloud Director

12

Per eseguire l'aggiornamento di vCloud Director a una nuova versione, chiudere i servizi di vCloud Director in tutte le celle nel gruppo di server, installare la nuova versione in ogni server, aggiornare il database di vCloud Director e riavviare le celle 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 10.0. Vedere [Capitolo 13 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 a una versione più recente dell'appliance vCloud Director. Utilizzare il programma di installazione di vCloud Director per Linux per aggiornare l'ambiente esistente solo come parte del flusso di lavoro della migrazione. Vedere [Migrazione all'appliance vCloud Director](#).

Per le installazioni di vCloud Director in Linux, è possibile eseguire un aggiornamento orchestrato oppure un aggiornamento manuale di vCloud Director. Vedere [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.

Per l'aggiornamento dell'appliance vCloud Director dalla versione 9.7 alla versione 10.0, vedere [Aggiornamento dell'appliance vCloud Director](#).

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 la tabella relativa ai [percorsi di aggiornamento e migrazione](#).
- 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. È possibile collocare gli host ESXi in modalità di manutenzione utilizzando vSphere 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>.

A partire da vCloud Director 10.0, i database di Microsoft SQL Server non sono supportati.

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. Per ulteriori informazioni, vedere la tabella relativa ai percorsi di aggiornamento e migrazione.
- La versione di VMware vSphere® correntemente utilizzata.
- La versione di VMware NSX® correntemente utilizzata.
- Tutti i componenti di terze parti che interagiscono direttamente con vCloud Director.

Per informazioni sulla compatibilità di vCloud Director con gli altri prodotti VMware e con i 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. Se si intende aggiornare i componenti di vSphere o NSX come parte dell'aggiornamento di vCloud Director, è necessario aggiornarli dopo aver eseguito l'aggiornamento di vCloud Director. Vedere [Capitolo 14 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*.

Flussi di lavoro e percorsi di aggiornamento e migrazione

Ambiente di origine	Ambiente di destinazione	
	vCloud Director 10.0 su Linux con un database PostgreSQL esterno	Appliance vCloud Director 10.0 con un database PostgreSQL incorporato
vCloud Director 9.0 e 9.1 con un database Oracle esterno	<ol style="list-style-type: none"> 1 Per vCloud Director 9.0 in Linux, eseguire l'aggiornamento a vCloud Director versione 9.1. Vedere Esecuzione dell'aggiornamento di vCloud Director. 2 Eseguire la migrazione del database Oracle in un database PostgreSQL. Vedere Migrazione a un database PostgreSQL. 3 Aggiornare l'ambiente a vCloud Director 10.0 su Linux. Vedere Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director o Aggiornamento manuale di un'installazione di vCloud Director. 	<ol style="list-style-type: none"> 1 Per vCloud Director 9.0 in Linux, eseguire l'aggiornamento a vCloud Director versione 9.1. Vedere Esecuzione dell'aggiornamento di vCloud Director. 2 Eseguire la migrazione del database Oracle in un database PostgreSQL. Vedere Migrazione a un database PostgreSQL. 3 Aggiornare l'ambiente a vCloud Director 10.0 su Linux. Vedere Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director o Aggiornamento manuale di un'installazione di vCloud Director. 4 Eseguire la migrazione all'appliance vCloud Director 10.0. Vedere Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director.
Appliance vCloud Director 9.5 con un database PostgreSQL esterno	Non supportato	<ol style="list-style-type: none"> 1 Aggiornare l'ambiente a vCloud Director 10.0 su Linux. Vedere Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director o Aggiornamento manuale di un'installazione di vCloud Director. 2 Eseguire la migrazione all'appliance vCloud Director 10.0. Vedere Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director.

Ambiente di origine	Ambiente di destinazione	
	vCloud Director 10.0 su Linux con un database PostgreSQL esterno	Appliance vCloud Director 10.0 con un database PostgreSQL incorporato
vCloud Director 9.0, 9.1 e 9.5 su Linux con un database PostgreSQL esterno	Aggiornare l'ambiente a vCloud Director 10.0 su Linux. Vedere Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director o Aggiornamento manuale di un'installazione di vCloud Director .	<ol style="list-style-type: none"> 1 Aggiornare l'ambiente a vCloud Director 10.0 su Linux. Vedere Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director o Aggiornamento manuale di un'installazione di vCloud Director. 2 Eseguire la migrazione all'appliance vCloud Director 10.0. Vedere Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director.
vCloud Director 9.0, 9.1 e 9.5 su Linux con un database Microsoft SQL Server esterno	<ol style="list-style-type: none"> 1 Aggiornare l'ambiente a vCloud Director 9.7 su Linux. Vedere Esecuzione dell'aggiornamento di vCloud Director. 2 Eseguire la migrazione del database Microsoft SQL Server in un database PostgreSQL. Vedere Migrazione a un database PostgreSQL. 3 Aggiornare l'ambiente a vCloud Director 10.0 in Linux. Vedere Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director o Aggiornamento manuale di un'installazione di vCloud Director. 	<ol style="list-style-type: none"> 1 Aggiornare l'ambiente a vCloud Director 9.7 su Linux. Vedere Esecuzione dell'aggiornamento di vCloud Director. 2 Eseguire la migrazione all'appliance vCloud Director 9.7. Vedere Migrazione di vCloud Director con un database Microsoft SQL esterno all'appliance vCloud Director. 3 Aggiornare l'ambiente all'appliance vCloud Director 10.0. Vedere Aggiornamento dell'appliance vCloud Director.
vCloud Director 9.7 su Linux con un database Microsoft SQL Server esterno	<ol style="list-style-type: none"> 1 Eseguire la migrazione del database Microsoft SQL Server in un database PostgreSQL. Vedere Migrazione a un database PostgreSQL. 2 Aggiornare l'ambiente a vCloud Director 10.0 in Linux. Vedere Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director o Aggiornamento manuale di un'installazione di vCloud Director. 	<ol style="list-style-type: none"> 1 Eseguire la migrazione all'appliance vCloud Director 9.7. Vedere Migrazione di vCloud Director con un database Microsoft SQL esterno all'appliance vCloud Director. 2 Aggiornare l'ambiente all'appliance vCloud Director 10.0. Vedere Aggiornamento dell'appliance vCloud Director.

Ambiente di origine	Ambiente di destinazione	
	vCloud Director 10.0 su Linux con un database PostgreSQL esterno	Appliance vCloud Director 10.0 con un database PostgreSQL incorporato
vCloud Director 9.7 su Linux con un database PostgreSQL esterno	Aggiornare l'ambiente a vCloud Director 10.0 in Linux. Vedere Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director o Aggiornamento manuale di un'installazione di vCloud Director .	<ol style="list-style-type: none"> 1 Eseguire la migrazione all'appliance vCloud Director 9.7. Vedere Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director. 2 Aggiornare l'ambiente all'appliance vCloud Director 10.0. Vedere Aggiornamento dell'appliance vCloud Director.
Appliance vCloud Director 9.7 con un database PostgreSQL incorporato	Non supportato	Aggiornare l'ambiente all'appliance vCloud Director 10.0. Vedere Aggiornamento dell'appliance vCloud Director .
vCloud Director 10.0 su Linux con un database PostgreSQL esterno	N/D	Eseguire la migrazione all'appliance vCloud Director 10.0. Vedere Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director .

Questo capitolo include i seguenti argomenti:

- [Aggiornamento dell'appliance vCloud Director](#)
- [Rollback di un'appliance di vCloud Director quando un aggiornamento non riesce](#)
- [Aggiornamento dell'appliance vCloud Director mediante il repository di aggiornamento di VMware](#)
- [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](#)

Aggiornamento dell'appliance vCloud Director

È possibile aggiornare l'appliance vCloud Director dalla versione 9.7 alla versione 10.0 oppure aggiornare vCloud Director 10.0 a una versione di patch.

Durante l'aggiornamento della 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 aggiornare 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 l'aggiornamento a ogni appliance di vCloud Director e completato l'aggiornamento del database, è necessario riavviare ogni appliance di vCloud Director.

Prerequisiti

Creare uno snapshot dell'appliance primaria di vCloud Director.

- 1 Accedere all'istanza di vCenter Server in cui si trova l'appliance primaria di vCloud Director del cluster ad alta disponibilità del database.
- 2 Passare all'appliance primaria di vCloud Director, fare clic con il pulsante destro del mouse sull'appliance e scegliere **Attiva > Spegni sistema operativo guest**.
- 3 Fare clic con il pulsante destro del mouse sull'appliance e scegliere **Snapshot > Crea snapshot**. Digitare un nome e, facoltativamente, una descrizione per lo snapshot, quindi fare clic su **OK**.
- 4 Fare clic con il pulsante destro del mouse sull'appliance vCloud Director e scegliere **Attiva > Attiva**.
- 5 Verificare che tutti i nodi della configurazione a disponibilità elevata del database funzionino correttamente. Vedere [Verifica dello stato di un cluster a disponibilità elevata del database](#).

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. È necessario aggiornare l'appliance primaria prima delle celle di standby e dell'applicazione. Quando si esegue il backup del database, è necessario utilizzare l'appliance primaria.

- 2 Scaricare il pacchetto di aggiornamento nell'appliance che si sta aggiornando.

Nota È necessario aggiornare prima l'appliance primaria.

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_10.0.0.4424-14420378_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 -zxvf VMware_vCloud_Director_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 dell'aggiornamento 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 Applicare l'aggiornamento disponibile.

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

- 9 Ripetere i passaggi da 2 a 8 nelle celle di standby e dell'applicazione rimanenti.

- 10 Dall'appliance primaria, eseguire il backup del database incorporato dell'appliance vCloud Director.

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

- 11 Da qualsiasi appliance, eseguire l'utilità di upgrade del database di vCloud Director.

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

- 12 Riavviare ciascuna appliance vCloud Director.

```
shutdown -r now
```

Operazioni successive

- Se l'aggiornamento riesce, è possibile eliminare lo snapshot dell'appliance vCloud Director.
- Se l'aggiornamento non viene eseguito correttamente, è possibile eseguire il rollback dell'appliance vCloud Director allo snapshot creato prima dell'aggiornamento. Vedere [Rollback di un'appliance di vCloud Director quando un aggiornamento non riesce](#).

Rollback di un'appliance di vCloud Director quando un aggiornamento non riesce

Se l'aggiornamento di un'appliance di vCloud Director non riesce, è possibile utilizzare lo snapshot dell'appliance creato prima dell'aggiornamento ed eseguire il rollback dell'appliance di vCloud Director.

Prima di iniziare il rollback, completare la procedura descritta in [Verifica dello stato di un cluster a disponibilità elevata del database](#). Prendere nota degli ID dei nodi di standby nel cluster.

- 1 Ripristinare l'appliance primaria di vCloud Director allo snapshot creato prima di iniziare l'aggiornamento.

Leggere come ripristinare gli snapshot delle macchine virtuali utilizzando le opzioni di ripristino. Vedere [Ripristinare gli snapshot della macchina virtuale tramite Ripristina](#) in *Guida all'amministrazione della macchine virtuali di vSphere*.

- 2 Accendere la cella dell'appliance primaria di vCloud Director.
- 3 Accedere direttamente o tramite un client SSH al sistema operativo di ogni cella dell'appliance di vCloud Director. È necessario accedere come utente **root**.
- 4 Arrestare i servizi di vCloud Director in tutte le celle dell'appliance.

```
service vmware-vcd stop
```

- 5 Utilizzare la cella primaria di vCloud Director per annullare la registrazione dei nodi secondari nel cluster.

- a Accedere direttamente o tramite un client SSH al sistema operativo della cella primaria come **root**.
- b Sostituire l'utente con **postgres**.

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

- c Eseguire il comando per annullare la registrazione di una cella dell'appliance di standby.

Per annullare la registrazione di un nodo di standby non in esecuzione, è necessario fornire l'ID del nodo.

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

- d Ripetere [5.c](#) per annullare la registrazione dell'altra cella dell'appliance di standby.
- 6 In vSphere Client, arrestare ed eliminare tutte le appliance di standby.
 - a In vSphere Client, passare alle appliance di standby.
 - b Fare clic con il pulsante destro del mouse su un'appliance di standby e scegliere **Attiva > Spegni sistema operativo guest**.
 - c Fare clic con il pulsante destro del mouse sull'appliance e scegliere **Elimina dal disco**.

- d Ripetere da [6.a](#) a [6.c](#) per l'altra cella dell'appliance di standby.
- 7 Verificare che la suite di strumenti `repmgr` e il database PostgreSQL incorporato della cella dell'appliance primaria di vCloud Director funzionino correttamente.
 - a Sostituire l'utente con **postgres**.

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

- b Eseguire il comando per controllare lo stato del cluster.

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

L'output della console include informazioni sull'unico nodo nel cluster.

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

- 8 Ridistribuire le appliance secondarie. Vedere [Distribuzione dell'appliance vCloud Director tramite vSphere Client](#).
- 9 Accedere direttamente o tramite un client SSH al sistema operativo di ogni cella dell'appliance di vCloud Director. È necessario accedere come utente **root**.
- 10 Avviare i servizi di vCloud Director.

```
service vmware-vcd start
```

Aggiornamento dell'appliance vCloud Director mediante il repository di aggiornamento di VMware

È possibile utilizzare il repository di aggiornamento di VMware per aggiornare l'appliance vCloud Director dalla versione 9.7 alla versione 10.0.

Nota È possibile utilizzare VMware Update Repository solo per aggiornare vCloud Director alla versione di vCloud Director più recente. In VMware Update Repository, è disponibile solo la versione più recente. Se si desidera aggiornare vCloud Director a una versione diversa, vedere [Aggiornamento dell'appliance vCloud Director](#).

Durante l'aggiornamento della 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 aggiornare 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 l'aggiornamento a ogni appliance di vCloud Director e completato l'aggiornamento del database, è necessario riavviare ogni appliance di vCloud Director.

Prerequisiti

Verificare che l'appliance vCloud Director disponga di accesso a `https://vapp-updates.vmware.com`.

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 il backup del database, è necessario utilizzare l'appliance primaria.

- 2 Reimpostare il repository di aggiornamento in modo che punti al repository di aggiornamento di VMware.

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

- 3 Verificare la disponibilità di aggiornamenti per verificare che il repository di aggiornamento di VMware disponga dell'aggiornamento desiderato.

Per impostazione predefinita, il comando `vamicli` punta al repository di aggiornamento di VMware.

```
vamicli update --check
```

La versione dell'aggiornamento viene visualizzata come **Aggiornamento disponibile**.

- 4 Arrestare vCloud Director eseguendo il comando seguente:

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

- 5 Applicare l'aggiornamento disponibile.

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

- 6 Ripetere i passaggi da [Passaggio 2](#) a [Passaggio 4](#) in ogni appliance.

- 7 Dall'appliance primaria, eseguire il backup del database incorporato dell'appliance vCloud Director.

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

- 8 Da qualsiasi appliance, eseguire l'utilità di upgrade del database di vCloud Director.

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

- 9 Riavviare ciascuna appliance vCloud Director.

```
shutdown -r now
```

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 13 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 o un database di Microsoft SQL Server, verificare di aver effettuato la migrazione a un database PostgreSQL prima di eseguire l'aggiornamento a vCloud Director versione 10.0. Per i percorsi di aggiornamento possibili, vedere [Capitolo 12 Eseguire l'aggiornamento di vCloud Director](#).

- 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 file-installazione
```

- 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 13 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 eseguire un aggiornamento orchestrato dell'installazione di vCloud Director. Vedere [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 o un database di Microsoft SQL Server, verificare di aver effettuato la migrazione a un database PostgreSQL prima di eseguire l'aggiornamento a vCloud Director versione 10.0. Per i percorsi di aggiornamento possibili, vedere [Capitolo 12 Eseguire l'aggiornamento di vCloud Director](#).

- 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](#).

- 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 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.
- [Aggiornamento di ciascun NSX Manager associato a un sistema vCenter Server collegato](#)
- Dopo l'aggiornamento di ogni NSX Manager, è possibile aggiornare i sistemi vCenter Server, gli host e gli NSX Edge. Vedere [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 file-installazione
```

- 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
Se le proprietà di registrazione esistenti non sono state modificate	Copiare questo file in <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> .
Se le proprietà di registrazione sono state modificate	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 si connettano 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 [Capitolo 10 Guida di riferimento allo strumento di gestione delle celle](#).
- Consultare l'argomento [Riferimento dell'utilità di aggiornamento del database](#).

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.

La posizione dell'utilità `upgrade` è `/opt/vmware/vcloud-director/bin/`.

Tabella 12-1. Opzioni e argomenti dell'utilità di aggiornamento del database

Opzione	Argomento	Descrizione
<code>--backup-completed</code>	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.
<code>--ceip-user</code>	Nome utente dell'account del servizio CEIP.	Se un utente con questo nome utente esiste già nell'organizzazione di sistema, l'aggiornamento non riesce. Predefinito: <code>phone-home-system-account</code>

Tabella 12-1. Opzioni e argomenti dell'utilità di aggiornamento del database (continua)

Opzione	Argomento	Descrizione
<code>--enable-ceip</code>	Scegliere tra: <ul style="list-style-type: none"> ■ <code>true</code> ■ <code>false</code> 	Specifica se l'installazione partecipa al programma di miglioramento dell'esperienza utente CEIP (Customer Experience Improvement Program) VMware. L'impostazione predefinita è <code>true</code> se non viene specificato alcun valore e se non si imposta il valore <code>false</code> 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 http://www.vmware.com/trustvmware/ceip.html . 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 Capitolo 10 Guida di riferimento allo strumento di gestione delle celle .
<code>--installer-path</code>	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 <code>vcloud.vcloud</code> .	Richiede l'opzione <code>--private-key-path</code> .
<code>--maintenance-cell</code>	Indirizzo IP	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 è stata riavviata, questa cella viene disattivata e aggiornata. Richiede l'opzione <code>--private-key-path</code> .

Tabella 12-1. Opzioni e argomenti dell'utilità di aggiornamento del database (continua)

Opzione	Argomento	Descrizione
<code>--multisite-user</code>	Nome utente per l'account di sistema multisito.	Questo account viene utilizzato dalla funzionalità multisito di vCloud Director. Se un utente con questo nome utente esiste già nell'organizzazione di sistema, l'aggiornamento non riesce. Predefinito: <code>multisite-system-account</code>
<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 Esecuzione di un aggiornamento orchestrato di un'installazione di vCloud Director 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.

Migrazione all'appliance vCloud Director

13

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 della versione precedente dell'ambiente vCloud Director esistente con un database PostgreSQL esterno a un ambiente vCloud Director costituito da distribuzioni dell'appliance vCloud Director 10.0.

È possibile eseguire la migrazione di un ambiente vCloud Director costituito da installazioni di vCloud Director su distribuzioni di appliance Linux o vCloud Director. A partire dalla versione 10.0, il database Microsoft SQL non è più supportato ed è possibile migrare solo un ambiente vCloud Director che utilizza un database PostgreSQL esterno.

Se l'ambiente vCloud Director utilizza un database Oracle esterno o un database Microsoft SQL esterno, è necessario eseguire la migrazione a un database PostgreSQL prima di eseguire l'aggiornamento a vCloud Director 10.0. Per i percorsi di aggiornamento, vedere [Capitolo 12 Eseguire l'aggiornamento di vCloud Director](#).

Questo capitolo include i seguenti argomenti:

- [Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director](#)

Migrazione di vCloud Director con un database PostgreSQL esterno all'appliance vCloud Director

Se l'ambiente vCloud Director corrente utilizza un database PostgreSQL esterno, è possibile eseguire la migrazione a un nuovo ambiente vCloud Director costituito da distribuzioni dell'appliance vCloud Director. 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
- 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 o successiva.
- 2 Aggiornare l'ambiente vCloud Director corrente alla versione 10.0.
Vedere [Capitolo 12 Eseguire l'aggiornamento 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`, `proxycertificates` e `truststore` da `/opt/vmware/vcloud-director/etc/` in `/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 10.0.

- 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, degli archivi attendibilità e dei certificati e copiare e sostituire questi file nella 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`, `truststore`, `certificates` e `proxycertificates` sono disponibili in `/opt/vmware/vcloud-director/etc/`.

- 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 Modificare la configurazione del bilanciamento del carico in modo che includa tutti i nuovi IP dell'appliance `eth0` nei pool di bilanciamento del carico per il traffico HTTP, HTTPS e TCP e rimuovere i vecchi IP delle celle vCloud Director Linux da tali pool.
- 16 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 Service Provider Admin Portal utilizzando l'indirizzo IP di rete `eth0` di una cella del nuovo gruppo di server, `https://eth0_IP_new_cell/provider`.
 - b Accedere a Service Provider Admin Portal con le credenziali dell'**amministratore di sistema** esistenti.
 - c Verificare che le risorse vSphere e cloud siano disponibili nel nuovo ambiente.
- 17 Dopo aver verificato correttamente la migrazione di vCloud Director, utilizzare Service Provider Admin Portal per eliminare le celle disconnesse che appartengono al vecchio ambiente vCloud Director.
 - a Dal menu principale () , selezionare **Risorse cloud**
 - b Nel riquadro a sinistra fare clic su **Celle cloud**.
 - c Selezionare una cella inattiva e fare clic su **Annulla registrazione**.

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

14

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](#)

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 Dal menu principale () del vCloud Director Service Provider Admin Portal, selezionare **Risorse vSphere**.
- b Nel riquadro a sinistra, fare clic su **vCenter**.
- c Selezionare il pulsante di opzione accanto al vCenter Server che si desidera disabilitare e fare clic su **Disattiva**.
- d Fare clic su **OK**.

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 Dal menu principale () , selezionare **Amministrazione**.
- b Nel pannello sinistro, in **Impostazioni**, fare clic su **Indirizzi pubblici**.
- c Verificare tutti gli indirizzi pubblici.

4 Aggiornare la registrazione di vCenter Server in vCloud Director.

- a Dal menu principale () del vCloud Director Service Provider Admin Portal, selezionare **Risorse vSphere**.
- b Nel riquadro a sinistra, fare clic su **vCenter**.
- c Selezionare il pulsante di opzione accanto al vCenter Server di destinazione e fare clic su **Riconnetti**.
- d Fare clic su **OK**.

- 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 utilizzare vCloud Director per aggiornare un gateway NSX Edge, è necessario intervenire sull'oggetto della rete di vCloud Director supportato da Edge:
 - Quando si utilizza 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.

Nota La redistribuzione è supportata solo per i gateway NSX Data Center for vSphere Edge.

- 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 reimpostare una rete di vApp dall'interno del contesto di una vApp, passare alla scheda **Reti** per la vApp, visualizzare i dettagli relativi alla rete, fare clic sul pulsante di opzione accanto al nome della rete di vApp e fare clic su **Reimposta**.

Per ulteriori informazioni sulle modalità di redistribuzione dei gateway Edge e sulla reimpostazione delle reti di vApp, vedere 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.

Visualizzazione dei registri di vCloud Director

15

vCloud Director fornisce informazioni di registrazione per ogni cella Cloud del sistema. È possibile visualizzare i registri per monitorare le celle e risolvere i problemi.

È possibile trovare i registri di una cella in `/opt/vmware/vcloud-director/logs`. [Tabella 15-1. Registri di vCloud Director](#) elenca i registri disponibili.

Tabella 15-1. Registri di vCloud Director

Nome registro	Descrizione
cell.log	Output di console della cella di vCloud Director.
cell-management-tool	Messaggi del registro dello strumento di gestione delle celle provenienti dalla cella.
cell-runtime	Messaggi del registro di runtime provenienti dalla cella.
cloud-proxy	Messaggi del registro del proxy cloud provenienti dalla cella.
console-proxy	Messaggi del registro del proxy della console remota provenienti dalla cella.
server-group-communications	Comunicazioni del gruppo di server provenienti dalla cella.
statsfeeder	Informazioni e messaggi di errore relativi al recupero delle metriche (da vCenter Server) e allo storage della macchina virtuale.
vcloud-container-debug.log	Messaggi di registro a livello di debug provenienti dalla cella.
vcloud-container-info.log	Messaggi di registro informativi provenienti dalla cella. Questo registro mostra anche gli avvisi o gli errori rilevati dalla cella.
vmware-vcd-watchdog.log	Messaggi di registro informativi provenienti dal watchdog della cella. Registra quando la cella si arresta in modo anomalo, viene riavviata e così via

Tabella 15-1. Registri di vCloud Director (continua)

Nome registro	Descrizione
diagnostics.log	Registro di diagnostica delle celle. Questo file è vuoto a meno che non sia abilitata la registrazione di diagnostica nella configurazione di registrazione locale.
AAAA_MM_GG.request.log	Registri di richieste HTTP nel formato di registro comune Apache.

È possibile utilizzare qualsiasi editor/visualizzatore di testo o strumento di terze parti per visualizzare i registri.

Risoluzione dei problemi relativi all'appliance vCloud Director

16

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

17

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.