Guida all'installazione e all'aggiornamento di vCloud Director

vCloud Director 8.0

Questo documento supporta la versione di ogni prodotto elencato e di tutte le versioni successive finché non è sostituito da una nuova edizione. Per controllare se esistono versioni più recenti di questo documento, vedere http://www.vmware.com/it/support/pubs.

IT-001716-00

vmware®

È possibile consultare la documentazione tecnica più aggiornata sul sito Web all'indirizzo:

http://www.vmware.com/it/support/

Sul sito Web di VMware sono inoltre disponibili gli aggiornamenti più recenti del prodotto.

Inoltrare eventuali commenti sulla documentazione al seguente indirizzo:

docfeedback@vmware.com

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

VMware, Inc.
P.le Biancamano 8
20121 Milano
tel: 02-6203.2075
fax: 02-6203.4000
www.vmware.com/it

Contenuti

Guida all'installazione e l'aggiornamento di VMware vCloud Director

Nella *Guida all'installazione e all'aggiornamento di VMware vCloud Director* sono contenute informazioni sull'installazione e sull'aggiornamento del software VMware® vCloud Director® e sulla relativa configurazione per l'utilizzo con VMware vCenter™ per offrire servizi VMware vCloud®.

Destinatari della guida

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

Panoramica di vCloud Director installazione, configurazione e aggiornamento

1

Un VMware vCloud® combina un gruppo di server vCloud Director con la piattaforma vSphere. Per creare un gruppo di server vCloud Director è necessario installare il software vCloud Director in uno o più server, connettendo i server a un database condiviso e integrando il gruppo di server vCloud Director con vSphere.

La configurazione iniziale di vCloud Director, comprese le informazioni di database e di rete, viene effettuata durante l'installazione. Quando si effettua l'aggiornamento di una installazione esistente di vCloud Director, si aggiorna il software vCloud Director e lo schema del database, mantenendo le relazioni esistenti tra server, il database e vSphere.

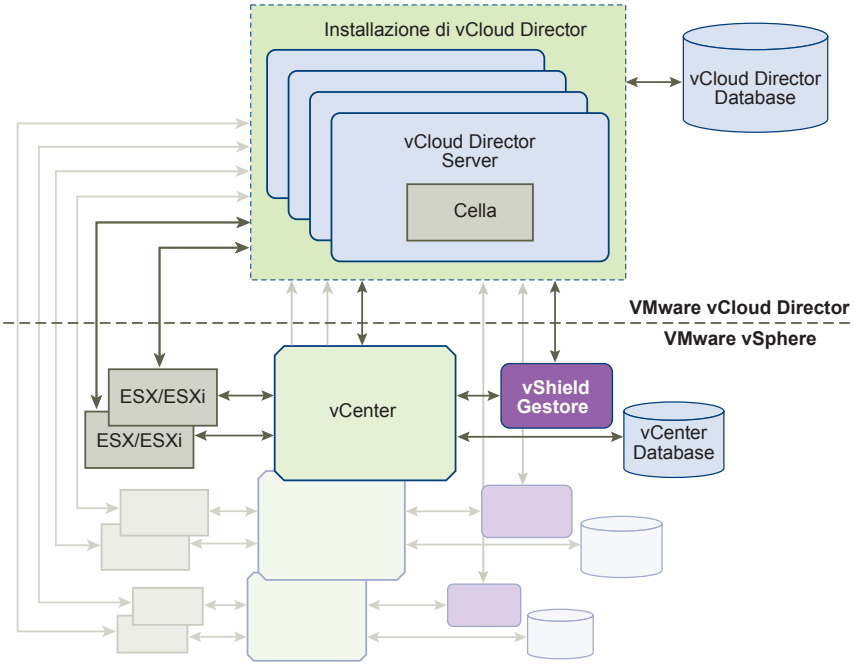
Questo capitolo include i seguenti argomenti:

Architettura di vCloud Director

Un gruppo di server vCloud Director è costituito da uno o più server vCloud Director. Questi server condividono un database comune e sono collegati a un numero arbitrario di sistemi vCenter Server e host ESXi. I servizi di rete vengono forniti ai sistemi vCenter Server e a vCloud Director dal componente VMware vShield Manager™ da VMware vCloud® Networking and Security™, oppure dal componente VMware NSX Manager™ da VMware NSX™ for vSphere®.

Un'installazione tipica crea un gruppo server di vCloud Director che comprende diversi server. Su ogni server del gruppo viene eseguita una raccolta di servizi denominata cella vCloud Director. Tutti i membri del gruppo condividono un singolo database. Ogni cella nel gruppo si connette a più sistemi vCenter Server, agli host che gestiscono e a ogni vShield Manager o NSX Manager configurato per supportare ciascun sistema vCenter Server connesso.

Figura 1-1. Diagramma dell'architettura di vCloud Director per l'installazione che utilizza vShield Manager



Il processo di configurazione e installazione di vCloud Director crea le celle, le connette al database condiviso e stabilisce le prime connessioni a un sistema vCenter Server, al vShield Manager o al NSX Manager associato a quel sistema vCenter Server e ai relativi host. Un amministratore di sistema può quindi utilizzare la console Web di vCloud Director per aggiungere in qualsiasi momento i sistemi vCenter Server, il vShield Manager o NSX Manager associato al sistema vCenter Server aggiunto e gli host del sistema vCenter Server aggiunto al gruppo di server di vCloud Director.

Pianificazione della configurazione

vSphere fornisce funzionalità di rete, di calcolo e di storage a vCloud Director. Prima di iniziare l'installazione, valutare la capacità vSphere e vCloud Director necessaria, 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 un server (cella) vCloud Director per ogni sistema vCenter Server che si desidera rendere accessibile nel cloud.
- Assicurarsi che tutti i server vCloud Director soddisfino almeno i requisiti minimi di memoria, CPU e storage descritti dettagliatamente in "Requisiti hardware e software di vCloud Director", pag. 9.
- Configurare il database vCloud Director come descritto in "Installazione e configurazione di un database vCloud Director", pag. 15.

Requisiti hardware e software di vCloud Director

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 vCenter Server, a un vShield Manager o NSX Manager e a uno o più host ESXi.

Piattaforme supportate

Le informazioni aggiornate sulle piattaforme VMware supportate da questa versione di vCloud Director sono disponibili nelle *matrici di compatibilità dei prodotti VMware* all'indirizzo http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Requisiti per la configurazione di vSphere

I server e gli host da utilizzare con vCloud Director devono soddisfare determinati requisiti di configurazione.

- Le reti vCenter da utilizzare come reti esterne o come pool di reti vCloud Director devono essere disponibili per tutti gli host di un cluster da utilizzare con vCloud Director. La possibilità di rendere tali reti disponibili per tutti gli host di un data center semplifica il task di aggiunta di nuovi server vCenter a vCloud Director.
- È necessario utilizzare vSphere Distributed Switch per applicare la priorità tra gli host e allocare i pool di reti.
- È necessario configurare il DRS dello storage dei cluster di vCenter utilizzati con vCloud Director con un livello di automazione corrispondente a **Completamente automatico**. Questa configurazione richiede lo storage condiviso collegato a tutti gli host ESXi in un cluster DRS. vCloud Director può sfruttare completamente il DRS Storage, incluso il supporto per il provisioning rapido.
- I 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 per la licenza di vSphere

vCloud Director richiede le licenze vSphere seguenti:

- VMware DRS, concesso in licenza da vSphere Enterprise ed Enterprise Plus.
- VMware Distributed Switch e dvFilter, concessi in licenza da vSphere Enterprise Plus. Questa licenza consente la creazione e l'utilizzo di reti vCloud Director isolate.

Sistemi operativi dei server vCloud Director supportati

Tavola 1-1. Sistemi operativi dei server vCloud Director supportati

Sistema operativo (solo 64-bit)	Aggiornamenti
CentOS 6	4
Red Hat Enterprise Linux 5	4-10
Red Hat Enterprise Linux 6	1-5

Requisiti di spazio su disco

Ogni server vCloud Director richiede circa 1450 MB di spazio libero per i file di installazione e di registro.

Requisiti di memoria

È necessario eseguire il provisioning di ogni server vCloud Director con almeno 4 GB di memoria.

Pacchetti software Linux

Ciascun server vCloud Director deve includere le installazioni dei pacchetti software Linux più comuni. Per impostazione predefinita, i pacchetti vengono generalmente installati con il software del sistema operativo. Se mancano uno o più pacchetti, l'esecuzione del programma di installazione non riesce e viene restituito un messaggio diagnostico.

Tavola 1-2. Pacchetti software richiesti

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

Nota: Diverse procedure per la configurazione delle connessioni di rete e la creazione di certificati SSL richiedono l'uso del comando `nslookup` di Linux, disponibile nel pacchetto `bind-utils` di Linux.

Database vCloud Director supportati

vCloud Director supporta i database Oracle e Microsoft SQL Server. Le informazioni più aggiornate sui database supportati da questa versione di vCloud Director sono disponibili nelle *matrici di compatibilità dei prodotti VMware* situate in VMware Partner Central. Accedere a VMware Partner Central utilizzando le informazioni dell'account di VMware Partner.

Per le configurazioni dei server di database consigliate, vedere "Installazione e configurazione di un database vCloud Director", pag. 15.

Server LDAP supportati

Tavola 1-3. Server LDAP supportati

Piattaforma	Server LDAP	Metodi di autenticazione
Windows Server 2003	Active Directory	Semplice, SSL semplice, Kerberos, Kerberos SSL
Windows Server 2008	Active Directory	Semplice
Windows 7 (2008 R2)	Active Directory	Semplice, SSL semplice, Kerberos, Kerberos SSL
Linux	OpenLDAP	Semplice, SSL semplice

Supporto per il sistema operativo guest

Consultare la *Guida per gli utenti di vCloud Director* per un elenco dei sistemi operativi guest supportati.

Database supportati per la memorizzazione dei dati di cronologia dei valori.

È possibile configurare l'installazione di vCloud Director per memorizzare i valori raccolti da vCloud Director circa le prestazioni delle macchine virtuali e il consumo delle risorse. I dati della cronologia dei valori sono memorizzati in un database KairosDB supportato da Cassandra. Per ulteriori informazioni, vedere Capitolo 6, “Installazione e configurazione del software di database opzionale per memorizzare e recuperare la cronologia dei valori delle prestazioni delle macchine virtuali”, pag. 71.

vCloud Director supporta le seguenti versioni di KairosDB e Cassandra.

- KairosDB 0.9.1
- Cassandra 1.2 e 2.0

Browser supportati in vCloud Director

La console Web di vCloud Director è compatibile con le versioni recenti di Google Chrome, Mozilla Firefox e Microsoft Internet Explorer.

Nota: La console Web di vCloud Director è compatibile solo con i browser a 32 bit. Se un browser è incluso nell'elenco di browser supportati su una piattaforma a 64 bit, l'utilizzo di un browser a 32 bit sulla piattaforma a 64 bit è implicito.

Supporto browser sulle piattaforme Linux

Su queste piattaforme Linux, la console Web vCloud Director è compatibile con la versione più recente di Mozilla Firefox e Google Chrome e con le relative versioni immediatamente precedenti.

Tavola 1-4. Supporto dei browser e compatibilità con i sistemi operativi sulle piattaforme Linux

Piattaforma	Google Chrome	Mozilla Firefox
CentOS 6.*x*	Sì	Sì
Red Hat Enterprise Linux 6.*x*	Sì	Sì
Ubuntu 12.*x*	Sì	Sì

Supporto browser sulle piattaforme Windows

Sulle piattaforme Windows, la console Web vCloud Director è compatibile con almeno una versione di Microsoft Internet Explorer. Alcune piattaforme Windows sono compatibili anche con la versione più recente di Mozilla Firefox e Google Chrome e con le relative versioni immediatamente precedenti.

Tavola 1-5. Supporto dei browser e compatibilità con i sistemi operativi sulle piattaforme Microsoft Windows

Piattaforma	Google Chrome	Mozilla Firefox	Internet Explorer 8.*x*	Internet Explorer 9.*x*	Internet Explorer 10.*x*
Windows XP Pro	Sì	Sì	Sì	No	No
Windows Server 2003 Enterprise Edition	Sì	Sì	Sì	No	No
Windows Server 2008	Sì	Sì	Sì	Sì	Sì
Windows Server 2008 R2	Sì	Sì	Sì	Sì	Sì
Windows Vista	Sì	No	Sì	Sì	Sì
Windows 7	Sì	Sì	Sì	Sì	Sì
Windows 8	Sì	Sì	No	No	Sì

Supporto browser sulle piattaforme Macintosh

Sulle piattaforme Macintosh, la console Web vCloud Director è compatibile con la versione più recente di Mozilla Firefox e Google Chrome e con le relative versioni immediatamente precedenti.

Versioni supportate di Adobe Flash Player

La console Web di vCloud Director richiede Adobe Flash Player 11,2 o successiva. È supportata solo la versione a 32 bit.

Versioni di Java supportate

È necessario che nei client vCloud Director sia installato e abilitato JRE 1.6.0 Update 10 o versione successiva. È supportata solo la versione a 32 bit.

Protocolli di protezione e pacchetti di crittografia supportati

vCloud Director richiede le connessioni dei client per essere protetto. Nel protocollo SSL versione 3 sono state individuate gravi vulnerabilità della sicurezza e di conseguenza non è più nel set di protocolli predefiniti messi a disposizione dal server per la connessione di un client. Sono supportati i seguenti protocolli di protezione:

- TLS versione 1.0
- TLS versione 1.1
- TLS versione 1.2

È possibile utilizzare `cell-management-tool` per riconfigurare il set di protocolli predefiniti. Vedere "Gestione dell'elenco dei protocolli SSL consentiti", pag. 67.

I pacchetti di crittografia supportati includono quelli con le firme RSA, DSS o a curva ellittica e con crittografia DES3, AES-128 o AES-256. È possibile utilizzare `cell-management-tool` per riconfigurare il set di crittografie SSL consentite. Vedere "Gestione dell'elenco di crittografia SSL consentita", pag. 65

Riepilogo dei requisiti per la 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, di un servizio di riferimento orario di rete e di 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 vCenter Server e i componenti associati vCloud Networking and Security o NSX for vSphere devono soddisfare diversi requisiti:

Indirizzi IP

Ogni server vCloud Director richiede due indirizzi IP per poter supportare due connessioni SSL differenti, Una connessione è per il servizio HTTP. L'altra è per il servizio proxy della console. Per creare tali indirizzi è possibile utilizzare gli alias IP o più interfacce di rete. Non è possibile utilizzare il comando `ip addr add` di Linux per creare il secondo indirizzo.

Indirizzo proxy della console

L'indirizzo IP configurato come indirizzo 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.

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
```

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. Quando si utilizza un NFS per trasferire lo storage del server, alcune impostazioni della configurazione devono essere impostate in modo che ciascuna cella di vCloud Director nel gruppo di server vCloud Director possa montare e utilizzare lo storage del server di trasferimento basato su NFS. Vedere

http://kb.vmware.com/kb/2086127 per informazioni dettagliate. Ogni membro del gruppo server deve montare questo volume nello stesso punto, che in genere corrisponde a `/opt/vmware/vcloud-director/data/transfer`. Lo spazio di questo volume viene impiegato in due modi:

- I trasferimenti (caricamenti e download) occupano lo storage per tutta la durata del trasferimento e vengono rimossi al termine del trasferimento. 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 nei cataloghi pubblicati esternamente e che abilitano la cache di contenuti pubblicati occupano questo storage fino a quando sono presenti. (Gli elementi dei cataloghi pubblicati esternamente, ma che non consentono la cache, non occupano questo storage.) Se si abilitano le organizzazioni nel cloud a creare cataloghi pubblicati esternamente, è opportuno presumente che centinaia, o addirittura migliaia, di elementi di catalogo necessiteranno di spazio in questo volume e che ciascun elemento di catalogo avrà le dimensioni di una macchina virtuale in formato compresso OVF.

Nota: Se possibile, il volume utilizzato per trasferire lo storage del server deve essere facilmente espandibile.

Consigli per la 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. Il firewall deve rifiutare tutto il rimanente traffico in entrata da une rete pubblica.

Tavola 1-6. 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	ActiveMQ
61616	TCP	ActiveMQ

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

Tavola 1-7. 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

Tavola 1-7. Porte che devono consentire il passaggio di pacchetti in uscita dagli host vCloud Director (Continua)

Porta	Protocollo	Commenti
111	TCP, UDP	Portmapper NFS utilizzato dal servizio di trasferimento
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	Connessioni vCenter, vShield Manager, NSX Manager e ESX
514	UDP	Facoltativo. Consente l'utilizzo di syslog.
902	TCP	Connessioni vCenter ed ESX.
903	TCP	Connessioni vCenter ed ESX.
920	TCP, UDP	rpc.statd NFS utilizzato dal servizio di trasferimento.
1433	TCP	Porta di database predefinita di Microsoft SQL Server.
1521	TCP	Porta di database Oracle predefinita.
5672	TCP, UDP	Facoltativo. Messaggi AMQP per le estensioni dei task.
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

- Se possibile, instradare il traffico tra i server vCloud Director e il server di database vCloud Director 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.

Installazione e configurazione di un database vCloud Director

Le celle vCloud Director utilizzano un database per archiviare le informazioni condivise. Per poter completare l'installazione e la configurazione del software vCloud Director, è necessario che tale database sia già esistente.

Nota: Indipendentemente dal software di database scelto, è necessario creare uno schema di database dedicato separato da utilizzare con vCloud Director. vCloud Director non può condividere uno schema di database con altri prodotti VMware.

Configurazione di un database Oracle

I database Oracle presentano requisiti di configurazione specifici quando vengono utilizzati con vCloud Director. Installare e configurare un'istanza di database e creare l'account utente del database vCloud Director prima di installare vCloud Director.

Procedura

1 Configurare il server di database.

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

2 Creare l'istanza di database.

Utilizzare un comando con il formato seguente per creare uno spazio tabella CLOUD_DATA singolo:

```
Create Tablespace CLOUD_DATA datafile '$ORACLE_HOME/oradata/cloud_data01.dbf' size 1500M
autoextend on;
```

3 Creare l'account utente del database vCloud Director.

Il comando seguente consente di creare il nome utente del database `vcloud` con la password `vcloudpass`.

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

NOTA: Quando si crea l'account utente del database vCloud Director, è necessario specificare CLOUD_DATA come spazio tabella predefinito.

4 Configurare i parametri per le connessioni, i processi e le transazioni del database.

È necessario configurare il database in modo da consentire almeno 75 connessioni per ogni cella vCloud Director, oltre a circa 50 connessioni specifiche per Oracle. È possibile ottenere valori per altri parametri di configurazione in base al numero di connessioni, dove *C* rappresenta il numero di celle incluse nel cluster vCloud Director.

Parametro di configurazione Oracle	Valore per *C* celle
CONNECTIONS	75*C+50
PROCESSES	= CONNECTIONS
SESSIONS	= PROCESSES*1.1+5
TRANSACTIONS	= SESSIONS*1.1
OPEN_CURSORS	= SESSIONS

5 Creare l'account utente del database vCloud Director.

Non utilizzare l'account di sistema di Oracle come account utente del database vCloud Director. A tale scopo è necessario creare un account utente dedicato. Concedere all'account i privilegi di sistema seguenti:

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

6 Annotare il nome del servizio di database in modo da poterlo utilizzare durante la configurazione delle connessioni di rete e di database.

Per individuare il nome del servizio di database, aprire il file `$ORACLE_HOME/network/admin/tnsnames.ora` sul server di database e cercare una voce nel formato seguente:

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

Configurazione di un database Microsoft SQL Server

I database SQL Server presentano requisiti di configurazione specifici quando vengono utilizzati con vCloud Director. Installare e configurare un'istanza di database e creare l'account utente del database vCloud Director prima di installare vCloud Director.

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

Prerequisiti

- È necessario avere familiarità con i comandi, gli script e il funzionamento di Microsoft SQL Server.
- Per configurare Microsoft SQL Server, accedere al computer host SQL Server utilizzando le credenziali dell'amministratore. È possibile configurare SQL Server per l'esecuzione con l'identità LOCAL_SYSTEM o con qualsiasi identità che disponga del privilegio per l'esecuzione di un servizio Windows.

Procedura

1 Configurare il server di database.

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

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

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

3 Creare l'istanza di database.

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

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

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

4 Impostare il livello di isolamento della transazione.

   Lo script seguente consente di impostare il livello di isolamento del database su READ_COMMITTED_SNAPSHOT.

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

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

5 Creare l'account utente del database vCloud Director.

Lo script seguente consente di creare il nome utente del database `vcloud` con la password `vcloudpass`.

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE =[vcloud],
   DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
```

6 Assegnare i permessi all'account utente del database vCloud Director.

Lo script seguente consente di assegnare il ruolo `db_owner` all'utente del database creato in Step 5.

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

Creazione di certificati SSL

vCloud Director utilizza SSL per proteggere le comunicazioni tra client e server. Prima di installare e configurare un gruppo di server vCloud Director, è necessario creare due certificati per ogni membro del gruppo e importarli negli archivi chiavi dell'host.

Ogni server vCloud Director richiede due indirizzi IP per poter supportare due endpoint SSL differenti. Ogni endpoint richiede il suo certificato SSL. I certificati per entrambi gli endpoint devono includere un nome distinto X.500. Molte autorità di certificazione consigliano di includere un'estensione del nome alternativo del soggetto X.509 nei certificati che concedono. vCloud Director non richiede che i certificati includano un nome alternativo del soggetto.

Procedura

1 Elencare gli indirizzi IP del server.

Per individuarli, utilizzare un comando quale `ifconfig`.

2 Per ogni indirizzo IP, eseguire il comando riportato di seguito per recuperare il nome di dominio completo al quale è associato.

```
nslookup ip-address
```

3 Annotare ogni indirizzo IP e il nome di dominio completo a esso associato, specificando se vCloud Director deve utilizzare l'indirizzo per il servizio HTTP o 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 al database è necessario specificare gli indirizzi IP. Se l'indirizzo IP può essere raggiunto da altri nomi di dominio completi, prendere nota anche di questi, poiché sarà necessario specificarli se si desidera che il certificato includa un nome alternativo del soggetto.

4 Creare i certificati.

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

NOTA: I certificati firmati garantiscono il livello di attendibilità più elevato.

Creazione e importazione di un certificato SSL firmato

I certificati firmati offrono il livello di attendibilità più elevato per le comunicazioni SSL.

Ogni server vCloud Director richiede due certificati SSL, uno per il servizio HTTP e uno per il servizio proxy della console, in un file di archivio dati Java. È possibile utilizzare certificati firmati da un'autorità di certificazione attendibile o certificati autofirmati. I certificati firmati garantiscono il livello di attendibilità più elevato.

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.

Per creare e importare certificati autofirmati, vedere "Creazione di un certificato SSL autofirmato", pag. 22.

Prerequisiti

- Generare un elenco di nomi di dominio completi e dei relativi indirizzi IP associati su questo server.
- Scegliere un indirizzo da utilizzare per il servizio HTTP e un indirizzo da utilizzare per il servizio proxy della console. Vedere "Creazione di certificati SSL", pag. 18.
- Assicurarsi di disporre dell'accesso a un computer con un ambiente di runtime Java versione 7, in modo da poter utilizzare il comando `keytool` per creare il certificato. 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 versione 7 installato. L'utilizzo di certificati creati con un `keytool` proveniente da qualsiasi altra origine non è supportato con vCloud Director. La creazione e l'importazione dei certificati prima dell'installazione e della configurazione del software vCloud Director semplifica il processo di installazione e configurazione. Nelle righe di comando di esempio riportate di seguito si suppone che `keytool` si trovi nel percorso dell'utente. In tali esempi la password dell'archivio chiavi è rappresentata come *passwd*.
- I certificati per entrambi gli endpoint devono includere un nome distinto X.500. Molte autorità di certificazione consigliano di includere un'estensione del nome alternativo del soggetto X.509 nei certificati che concedono. vCloud Director non richiede che i certificati includano un nome alternativo del soggetto. Imparare l'utilizzo del comando `keytool`, incluse le opzioni `-dname` e `-ext`.
- Ottenere le informazioni necessarie per l'argomento dell'opzione keytool `-dname`.

Tavola 1-8. Informazioni richieste dall'opzione keytool `-dname`

Sotto-parte nome distinto X.500	parola chiave keytool	Descrizione	Esempio
commonName	CN	Il nome di dominio completo associato all'indirizzo IP di questo endpoint.	CN=vcd1.esempio.com
organizationalUnit	OU	Il nome di un'unità organizzativa, come ad esempio un reparto o un divisione, all'interno dell'organizzazione a cui è associato questo certificato	OU=Engineering
organizationName	O	Il nome dell'organizzazione a cui è associato questo certificato	O=Example Corporation
localityName	L	Il nome della città in cui si trova l'organizzazione.	L=Palo Alto

Tavola 1-8. Informazioni richieste dall'opzione keytool `–dname` (Continua)

Sotto-parte nome distinto X.500	parola chiave keytool	Descrizione	Esempio
stateName	S	Il nome dello stato o della provincia in cui si trova l'organizzazione.	S=California
country	C	Il nome del paese in cui si trova l'organizzazione	C=US

Procedura

1 Creare un certificato non attendibile per il servizio HTTP.

Il comando di esempio riportato di seguito consente di creare un certificato non attendibile in un file di archivio chiavi denominato `certificate.ks`. Le opzioni `keytool` sono state posizionate su righe separate per una migliore comprensione. Le informazioni di nome distinto X.500 fornite nell'argomento per l'opzione `–dname` utilizza i valori mostrati nei Requisiti preliminari. I valori DNS e IP mostrati nell'argomento per l'opzione `–ext` sono tipici. Assicurarsi di includere tutti i nomi DNS a cui questo endpoint può essere raggiunto, incluso quello specificato per il valore `commonName` (CN) nell'argomento dell'opzione `–dname`: Inoltre, è possibile includere gli indirizzi IP, come mostrato qui.

```
keytool
   –keystore certificates.ks
   –alias http
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

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.

2 Creare un certificato non attendibile per il servizio proxy della console.

Il comando seguente consente di aggiungere un certificato non attendibile al file di archivio chiavi creato in Step 1. Le opzioni `keytool` sono state posizionate su righe separate per una migliore comprensione. Le informazioni di nome distinto X.500 fornite nell'argomento per l'opzione `–dname` utilizza i valori mostrati nei Requisiti preliminari. I valori DNS e IP mostrati nell'argomento per l'opzione `–ext` sono tipici. Assicurarsi di includere tutti i nomi DNS a cui questo endpoint può essere raggiunto, incluso quello specificato per il valore `commonName` (CN) nell'argomento dell'opzione `–dname`. Inoltre, è possibile includere gli indirizzi IP, come mostrato qui.

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
```

```
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 Creare una richiesta di firma del certificato per il servizio HTTP.

   Il comando seguente consente di creare una richiesta di firma del certificato nel file `http.csr`.

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

4 Creare una richiesta di firma del certificato per il servizio proxy della console.

   Il comando seguente consente di creare una richiesta di firma del certificato nel file `consoleproxy.csr`.

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

5 Inviare le richieste di firma del certificato all'Autorità di certificazione.

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

6 Una volta ricevuti i certificati firmati, importarli nel file di archivio chiavi.

   a Importare il certificato root dell'Autorità di certificazione nel file di archivio chiavi.

      Il comando seguente consente di importare il certificato root dal file `root.cer` nel file di archivio chiavi `certificates.ks`.

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

   b (Facoltativo) Se si ricevono certificati intermedi, importarli nel file di archivio chiavi.

      Il comando seguente consente di importare i certificati intermedi dal file `intermediate.cer` nel file di archivio chiavi `certificates.ks`.

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

   c Importare il certificato per il servizio HTTP.

      Il comando seguente consente di importare il certificato dal file `http.cer` nel file di archivio chiavi `certificates.ks`.

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

   d Importare il certificato per il servizio proxy della console.

      Il comando seguente consente di importare il certificato dal file `consoleproxy.cer` nel file di archivio chiavi `certificates.ks`.

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

7 Per verificare che tutti i certificati siano stati importati, elencare il contenuto del file di archivio chiavi.

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

8 Ripetere questa procedura su tutti i server vCloud Director nel gruppo di server.

Passi successivi

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 sarà necessario specificare il nome del percorso del file di archivio chiavi. Vedere "Configurazione delle connessioni di rete e di database", pag. 32.

Creazione di un certificato SSL autofirmato

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, uno per il servizio HTTP e uno per il servizio proxy della console, in un file di archivio dati Java. È possibile utilizzare certificati firmati da un'autorità di certificazione attendibile o certificati autofirmati. I certificati firmati garantiscono il livello di attendibilità più elevato.

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.

Per creare e importare certificati firmati, vedere "Creazione e importazione di un certificato SSL firmato", pag. 19.

Prerequisiti

- Generare un elenco di nomi di dominio completi e dei relativi indirizzi IP associati su questo server.
- Scegliere un indirizzo da utilizzare per il servizio HTTP e un indirizzo da utilizzare per il servizio proxy della console. Vedere "Creazione di certificati SSL", pag. 18.
- Assicurarsi di disporre dell'accesso a un computer con un ambiente di runtime Java versione 7, in modo da poter utilizzare il comando `keytool` per creare il certificato. 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 versione 7 installato. L'utilizzo di certificati creati con un `keytool` proveniente da qualsiasi altra origine non è supportato con vCloud Director. La creazione e l'importazione dei certificati prima dell'installazione e della configurazione del software vCloud Director semplifica il processo di installazione e configurazione. Nelle righe di comando di esempio riportate di seguito si suppone che `keytool` si trovi nel percorso dell'utente. In tali esempi la password dell'archivio chiavi è rappresentata come *passwd*.
- I certificati per entrambi gli endpoint devono includere un nome distinto X.500. Molte autorità di certificazione consigliano di includere un'estensione del nome alternativo del soggetto X.509 nei certificati che concedono. vCloud Director non richiede che i certificati includano un nome alternativo del soggetto. Imparare l'utilizzo del comando `keytool`, incluse le opzioni `-dname` e `-ext`.

- Ottenere le informazioni necessarie per l'argomento dell'opzione keytool `–dname`.

Tavola 1-9. Informazioni richieste dall'opzione keytool `–dname`

Sotto-parte nome distinto X.500	parola chiave keytool	Descrizione	Esempio
commonName	CN	Il nome di dominio completo associato all'indirizzo IP di questo endpoint.	CN=vcd1.esempio.com
organizationalUnit	OU	Il nome di un'unità organizzativa, come ad esempio un reparto o un divisione, all'interno dell'organizzazione a cui è associato questo certificato	OU=Engineering
organizationName	O	Il nome dell'organizzazione a cui è associato questo certificato	O=Example Corporation
localityName	L	Il nome della città in cui si trova l'organizzazione.	L=Palo Alto
stateName	S	Il nome dello stato o della provincia in cui si trova l'organizzazione.	S=California
country	C	Il nome del paese in cui si trova l'organizzazione	C=US

Procedura

1 Creare un certificato non attendibile per il servizio HTTP.

Il comando di esempio riportato di seguito consente di creare un certificato non attendibile in un file di archivio chiavi denominato `certificate.ks`. Le opzioni `keytool` sono state posizionate su righe separate per una migliore comprensione. Le informazioni di nome distinto X.500 fornite nell'argomento per l'opzione `–dname` utilizza i valori mostrati nei Requisiti preliminari. I valori DNS e IP mostrati nell'argomento per l'opzione `–ext` sono tipici. Assicurarsi di includere tutti i nomi DNS a cui questo endpoint può essere raggiunto, incluso quello specificato per il valore `commonName` (CN) nell'argomento dell'opzione `–dname`: Inoltre, è possibile includere gli indirizzi IP, come mostrato qui.

```
keytool
   –keystore certificates.ks
   –alias http
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

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.

2 Creare un certificato non attendibile per il servizio proxy della console.

Il comando seguente consente di aggiungere un certificato non attendibile al file di archivio chiavi creato in Step 1. Le opzioni `keytool` sono state posizionate su righe separate per una migliore comprensione. Le informazioni di nome distinto X.500 fornite nell'argomento per l'opzione `–dname` utilizza i valori mostrati nei Requisiti preliminari. I valori DNS e IP mostrati nell'argomento per l'opzione `–ext` sono tipici. Assicurarsi di includere tutti i nomi DNS a cui questo endpoint può essere raggiunto, incluso quello specificato per il valore `commonName` (CN) nell'argomento dell'opzione `–dname`. Inoltre, è possibile includere gli indirizzi IP, come mostrato qui.

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 Per verificare che tutti i certificati siano stati importati, elencare il contenuto del file di archivio chiavi.

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

4 Ripetere questa procedura su tutti i server vCloud Director nel gruppo di server.

Passi successivi

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 sarà necessario specificare il nome del percorso del file di archivio chiavi. Vedere "Configurazione delle connessioni di rete e di database", pag. 32.

Installazione e configurazione di vShield Manager per una nuova installazione di vCloud Director

vCloud Director è subordinato alla presenza di vShield Manager o NSX Manager per fornire i servizi di rete al cloud. Prima di eseguire una nuova installazione di vCloud Director, è necessario installare e configurare vShield Manager o NSX Manager e associare un'istanza unica a vShield Manager o NSX Manager con ciascun vCenter Server che si intende includere nell'installazione di vCloud Director.

vShield Manager è incluso nel download di VMware vCloud Networking and Security. Le informazioni aggiornate sulle versioni supportate di vShield Manager, compatibili con vCloud Director, sono disponibili nelle *matrici di compatibilità dei prodotti VMware* che si trovano in VMware Partner Central. Accedere a VMware Partner Central utilizzando le informazioni dell'account di VMware Partner. Per informazioni sui requisiti di rete, vedere "Requisiti hardware e software di vCloud Director", pag. 9.

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 3, "Eseguire l'aggiornamento di vCloud Director", pag. 41.

Prerequisiti

- Assicurarsi che ogni sistema vCenter Server soddisfi i requisiti preliminari per l'installazione di vShield Manager.
- Eseguire l'installazione per la virtual appliance di vShield Manager, come descritto nella *Guida all'installazione e all'aggiornamento di vShield*.

Procedura

1. Accedere alla virtual appliance di vShield Manager installata e confermare le impostazioni specificate durante l'installazione.
2. Associare la virtual appliance di vShield Manager installata con il sistema vCenter Server che si intende aggiungere a vCloud Director durante l'installazione pianificata di vCloud Director.

Passi successivi

Configurare il supporto VXLAN nel vShield Manager associato. vCloud Director crea pool di reti VXLAN per fornire risorse di rete ai VDC del provider. Se il supporto VXLAN non è configurato nel vShield 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 ulteriori informazioni sulla configurazione del supporto VXLAN, consultare la *Guida per l'amministratore di vShield*.

Installazione e configurazione di NSX Manager per una nuova installazione di vCloud Director

vCloud Director è subordinato alla presenza di vShield Manager o NSX Manager per fornire i servizi di rete al cloud. Prima di eseguire una nuova installazione di vCloud Director, è necessario installare e configurare vShield Manager o NSX Manager e associare un'istanza unica a vShield Manager o NSX Manager con ciascun vCenter Server che si intende includere nell'installazione di vCloud Director.

NSX è incluso nel download di VMware NSX for vSphere. Le informazioni aggiornate sulle versioni di NSX Manager supportate compatibili con vCloud Director sono disponibili nelle *matrici di compatibilità dei prodotti VMware* che si trovano in VMware Partner Central. Accedere a VMware Partner Central utilizzando le informazioni dell'account di VMware Partner. Per informazioni sui requisiti di rete, vedere "Requisiti hardware e software di vCloud Director", pag. 9.

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 3, "Eseguire l'aggiornamento di vCloud Director", pag. 41.

Prerequisiti

- Assicurarsi che ciascun sistema vCenter Server soddisfi i requisiti preliminari per l'installazione di NSX Manager.
- Eseguire l'installazione per la virtual appliance di NSX Manager descritta nella *Guida all'installazione e all'aggiornamento di NSX*.

Procedura

1. Accedere alla virtual appliance di NSX Manager installata e confermare le impostazioni specificate durante l'installazione.
2. Associare la virtual appliance di NSX Manager installata con il sistema vCenter Server che si intende aggiungere a vCloud Director durante l'installazione pianificata di vCloud Director.

Passi successivi

Configurare il supporto VXLAN nel NSX Manager associato. 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 ulteriori informazioni sulla configurazione del supporto VXLAN, consultare la *Guida per l'amministratore di NSX*.

Installazione e configurazione di un broker AMQP

Il protocollo AMQP (Advanced Message Queuing Protocol) è uno standard aperto per l'accodamento dei messaggi che supporta la messaggistica flessibile per i sistemi aziendali. vCloud Director include un servizio AMQP che è possibile configurare per l'utilizzo con un broker AMQP, quale RabbitMQ, in modo da poter fornire agli operatori del Cloud un flusso di notifiche sugli eventi che si verificano nel Cloud. Se si desidera utilizzare questo servizio, è necessario installare e configurare un broker AMQP.

L'utilizzo di un broker AMQP con vCloud Director è opzionale, tuttavia alcune integrazioni utilizzano AMQP per comunicare con vCloud Director. Consultare i documenti di installazione e configurazione per le integrazioni da utilizzare.

Procedura

1. Scaricare il server RabbitMQ da http://info.vmware.com/content/12834_rabbitmq.
2. Seguire le istruzioni per l'installazione di RabbitMQ per installare RabbitMQ in un host appropriato.

   L'host del server RabbitMQ deve essere raggiungibile nella rete da ogni cella vCloud Director.
3. Durante l'installazione di RabbitMQ, annotare i valori che sarà necessario specificare per configurare vCloud Director per l'utilizzo con questa installazione di RabbitMQ.
   - Il nome di dominio completo dell'host del server RabbitMQ, ad esempio `amqp.esempio.com`.
   - Un nome utente e una password validi per l'autenticazione con 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 "/".

Passi successivi

Per impostazione predefinita, il servizio AMQP di vCloud Director invia messaggi non crittografati. Se viene configurato per crittografare questi messaggi utilizzando SSL, verifica il certificato del broker utilizzando l'archivio affidabilità JCEKS predefinito dell'ambiente di runtime Java sul server vCloud Director. Tale ambiente generalmente si trova nella directory `$JRE_HOME/lib/security/cacerts`.

Per usare SSL con il servizio AMQP di vCloud Director, selezionare **Use SSL (Usa SSL)** nella sezione delle impostazioni del broker AMQP della pagina Extensibility (Estendibilità) della console web di vCloud Director, e fornire uno dei seguenti elementi:

- il percorso di un certificato SSL
- il percorso e la password di un archivio affidabilità JCEKS

Se non è necessario convalidare il certificato del broker AMQP, selezionare l'opzione per **accettare tutti i certificati**.

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.

Creazione di un gruppo di server vCloud Director 2

Un gruppo di server vCloud Director è composto da uno o più server vCloud Director che condividono un database comune e altri dettagli sulla configurazione. Per creare un gruppo di server, installare e configurare il software vCloud Director sul primo membro del gruppo. L'installazione e la configurazione del primo membro del gruppo crea un file di risposta da utilizzare per configurare membri aggiuntivi del gruppo.

Requisiti preliminari per la creazione di un gruppo di server vCloud Director

IMPORTANTE: Questa procedura è valida solo per le nuove installazioni. Se si sta aggiornano un'installazione di vCloud Director esistente, vedere Capitolo 3, "Eseguire l'aggiornamento di vCloud Director", pag. 41

Prima di iniziare a installare e configurare vCloud Director, completare tutti i task elencati di seguito.

1. Verificare che un sistema vCenter Server supportato sia in esecuzione e sia configurato correttamente per l'utilizzo con vCloud Director. Per le versioni supportate e i requisiti di configurazione, vedere "Piattaforme supportate", pag. 9.
2. Verificare che un NSX Manager o vShield Manager supportato sia in esecuzione, associato al sistema vCenter Server e correttamente configurato per l'utilizzo con vCloud Director. Per le versioni supportate, vedere "Piattaforme supportate", pag. 9. Per informazioni dettagliate sull'installazione e sulla configurazione, vedere "Installazione e configurazione di vShield Manager per una nuova installazione di vCloud Director", pag. 24 e "Installazione e configurazione di NSX Manager per una nuova installazione di vCloud Director", pag. 25.
3. Assicurarsi di disporre di almeno una piattaforma del server supportata per l'esecuzione del software vCloud Director e che la piattaforma del server sia configurata con la quantità di memoria e storage adeguata. Per le piattaforme supportate e i requisiti di configurazione, vedere "Sistemi operativi dei server vCloud Director supportati", pag. 10.
   - Ogni membro di un gruppo di server richiede due indirizzi IP, uno per supportare una connessione SSL per il servizio HTTP e un'altra per il servizio proxy della console.
   - Ogni server deve disporre di un certificato SSL per ciascun indirizzo IP. Tutte le directory incluse nel nome di percorso dei certificati SSL devono essere leggibili da qualsiasi utente. Vedere "Creazione di certificati SSL", pag. 18.
   - Per il servizio di trasferimento, è necessario che ogni server monti un NFS o un altro volume di storage condiviso in `/opt/vmware/vcloud-director/data/transfer`. Questo volume deve essere accessibile a tutti i membri del gruppo di server. Vedere "Riepilogo dei requisiti per la configurazione di rete per vCloud Director", pag. 13.
   - Ogni server deve disporre di accesso a un pacchetto di distribuzione Microsoft Sysprep. Vedere "Installazione dei file Microsoft Sysprep nei server", pag. 37.

4 Assicurarsi di aver creato un database vCloud Director accessibile da tutti i server del gruppo. Per un elenco di software di database supportati, vedere "Database vCloud Director supportati", pag. 10.

   - Verificare di aver creato un account database per l'utente del database vCloud Director e che esso disponga di tutti i privilegi richiesti. Vedere "Installazione e configurazione di un database vCloud Director", pag. 15.
   - Verificare che il servizio di database venga avviato al riavvio del server di database.

5 Assicurarsi che tutti i vCloud Director server, i server di database, i sistemi vCenter Server e i componenti di vShield Manager o NSX Manager associati a quei sistemi vCenter Server, siano in grado di risolvere i nomi uno dell'altro, come descritto in "Riepilogo dei requisiti per la configurazione di rete per vCloud Director", pag. 13.

6 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 "Riepilogo dei requisiti per la configurazione di rete per vCloud Director", pag. 13.

7 Se si intende importare utenti o gruppi da un servizio LDAP, verificare che il servizio sia accessibile da ogni server vCloud Director.

8 Aprire le porte firewall come descritto in "Consigli per la sicurezza della rete", pag. 14. La porta 443 deve essere aperta tra vCloud Director e i sistemi vCenter Server.

Questo capitolo include i seguenti argomenti:

Installazione e configurazione del software vCloud Director nel primo membro di un gruppo di server

Tutti i membri di un vCloud Director condividono la connessione di database e altri dettagli di configurazione specificati durante l'installazione e la configurazione del primo membro del gruppo. Questi dettagli vengono raccolti in un file di risposta che è necessario utilizzare quando si aggiungono dei membri al gruppo.

Il software vCloud Director viene distribuito come file eseguibile Linux con firma digitale denominato `vmware-vcloud-director-8.0.0-`*nnnnnn*`.bin`, dove *nnnnnn* rappresenta un numero di build.

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. Dopo aver installato il software nel server di destinazione, è necessario eseguire uno script per configurare le connessioni di rete e al database del server. Questo script consente di creare un file di risposta che è necessario utilizzare durante la configurazione di membri aggiuntivi di questo gruppo di server.

Prerequisiti

- Verificare che il server di destinazione e la rete alla quale si connette soddisfino i requisiti specificati in "Riepilogo dei requisiti per la configurazione di rete per vCloud Director", pag. 13.
- Assicurarsi di disporre delle credenziali di utente con privilegi avanzati per il server di destinazione

- Verificare che il server di destinazione monti il volume di storage del servizio di trasferimento su `/opt/vmware/vcloud-director/data/transfer`.
- Per far sì che 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", pag. 27.

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 caricato su un CD o un altro supporto, copiare il file di installazione in una posizione accessibile da tutti i 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
   checksum-value installation-file
   ```

   Confrontare il *valore-checksum* creato da questo comando con il checksum MD5 copiato dalla pagina di download.
4. Verificare che il file di installazione sia eseguibile.

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

   ```
   [root@cell1 /tmp]# chmod u+x installation-file
   ```
5. In una console, una shell o una finestra del terminale eseguire il file di installazione.

   Per eseguire il file di installazione, digitarne 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.

   Il programma di installazione stampa un avviso nel formato seguente se la chiave pubblica VMware non è stata installata nel server di destinazione.

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

   Quando il programma di installazione viene eseguito, vengono effettuate le seguenti operazioni.

   a. Verifica che l'host soddisfi tutti i requisiti
   b. Verifica della firma digitale nel file di installazione
   c. Creazione dell'utente e il gruppo `vcloud`
   d. Apertura del pacchetto RPM vCloud Director
   e. Installazione del software

Installato il software, il programma di installazione richiede di eseguire lo script di configurazione, che configura le connessioni di database e rete del server.

Passi successivi

Stabilire se eseguire lo script di configurazione.

- Se sono stati completati i prerequisiti elencati in "Requisiti preliminari per la creazione di un gruppo di server vCloud Director", pag. 29, è possibile eseguire lo script di configurazione adesso. Digitare **y** e premere Invio.
- Se non si è pronti ad eseguire lo script di configurazione adesso, digitare **n** e premere Esci per uscire dalla shell.

Per ulteriori informazioni sull'esecuzione dello script di configurazione, vedere "Configurazione delle connessioni di rete e di database", pag. 32.

Configurazione delle connessioni di rete e di database

Dopo aver installato il software vCloud Director nel server, il programma di installazione richiede l'esecuzione di uno script per la configurazione delle connessioni di rete e di database del server.

Per poter eseguire lo script di configurazione, è innanzitutto necessario installare il software vCloud Director. Il programma di installazione richiede di eseguire lo script al termine dell'installazione, ma è possibile decidere di eseguirlo in un secondo momento.

Per eseguire lo script dopo l'installazione del software vCloud Director, eseguire il login come utente root, aprire una console, una shell o una finestra del terminale e digitare:

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

Lo script di configurazione crea connessioni di rete e di database per un singolo server vCloud Director. Crea inoltre un file di risposta in cui vengono conservate le informazioni sulle connessioni di database da utilizzare per le installazioni server successive.

Nota: Dopo avere eseguito lo script di configurazione per configurare il primo membro del gruppo di server, è necessario utilizzare l'opzione `-r` e specificare il nome percorso del file di risposta quando si configurano membri aggiuntivi del gruppo. Vedere "Protezione e riutilizzo del file di risposta", pag. 35.

Prerequisiti

- Verificare che il server vCloud Director possa accedere a un database di un tipo supportato. Vedere "Installazione e configurazione di un database vCloud Director", pag. 15 e "Requisiti hardware e software di vCloud Director", pag. 9.
- Recuperare le informazioni seguenti:
  - Posizione e password del file di archivio chiavi che include i certificati SSL per questo server. Vedere "Creazione e importazione di un certificato SSL firmato", pag. 19. Lo script di configurazione non viene eseguito con un'identità privilegiata, pertanto il file di archivio chiavi e la directory nella quale viene archiviato devono essere leggibili da qualsiasi utente.
  - La password di ogni certificato SSL.
  - Il nome host o l'indirizzo IP del server di database.
  - Il nome del database e la porta di connessione.
  - Le credenziali dell'utente del database (nome utente e password). Tale utente deve disporre di privilegi specifici per il database. Vedere "Installazione e configurazione di un database vCloud Director", pag. 15.

Procedura

1 Specificare gli indirizzi IP da utilizzare per i servizi proxy della console e HTTP in esecuzione sull'host.

Ogni membro di un gruppo di server richiede due indirizzi IP, in modo da poter supportare due diverse connessioni SSL: una per il servizio HTTP e un'altra per il servizio proxy della console. Per iniziare il processo di configurazione, scegliere quali tra gli indirizzi IP individuati dallo script si desidera utilizzare per ogni servizio.

```
Please indicate which IP address available on this machine should be used for the HTTP
service and which IP address should be used for the remote console proxy. The HTTP service
IP address is used for accessing the user interface and the REST API. The remote console
proxy IP address is used for all remote console (VMRC) connections and traffic. Please enter
your choice for the HTTP service IP address: 1: 10.17.118.158 2: 10.17.118.159 Choice
[default=1]:2
Please enter your choice for the remote console proxy IP address 1: 10.17.118.158 Choice
[default=1]:
```

2 Specificare il percorso completo del file di archivio chiavi Java.

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

3 Digitare le password per l'archivio chiavi e i certificati.

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

4 Configurare le opzioni per la gestione dei messaggi di controllo.

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 alla utility `syslog`, oltre che al database vCloud Director.

Opzione	Azione
Per registrare i messaggi di controllo sia in `syslog` che nel database vCloud Director	Digitare il nome host o l'indirizzo IP di `syslog`.
Per registrare i messaggi di controllo solo nel database vCloud Director	Premere Invio.

```
If you would like to enable remote audit logging to a syslog host please enter the hostname
or IP address of the syslog server. Audit logs are stored by vCloud Director for 90 days.
Exporting logs via syslog will enable you to preserve them for as long as necessary. Syslog
host name or IP address [press Enter to skip]:10.150.10.10
```

5 Specificare la porta sulla quale il processo `syslog` monitora il server specificato.

La porta predefinita è 514.

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

6 Specificare il tipo di database oppure premere Invio per accettare il valore predefinito.

```
The following database types are supported: 1. Oracle 2. Microsoft SQL Server Enter the
database type [default=1]: Using default value "1" for database type.
```

7 Specificare le informazioni relative alle connessioni di database.

Le informazioni richieste dallo script dipendono dal tipo di database scelto. In questo esempio vengono mostrati prompt che seguono la specifica di un database Oracle. I prompt per altri tipi di database sono simili.

a Digitare il nome host o l'indirizzo IP del server di database.

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

b Digitare la porta del database oppure premere Invio per accettare il valore predefinito.

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

c Digitare il nome del servizio di database.

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

Se si preme Invio, lo script di configurazione utilizza un valore predefinito che potrebbe non essere corretto per alcune installazioni. Per informazioni su come individuare il nome del servizio di database per un database Oracle, vedere "Configurazione di un database Oracle", pag. 15.

d Digitare il nome e la password dell'utente del database.

```
Enter the database username:vcloud
Enter the database password:
```

Lo script convalida le informazioni fornite e procede con l'esecuzione di altri tre passaggi.

1 Inizializza il database e vi connette il server.

2 Offre la possibilità di avviare i servizi di vCloud Director sull'host.

3 Mostra un URL che consente di connettersi all'installazione guidata in seguito all'avvio del servizio di vCloud Director.

Nel frammento di codice riportato di seguito viene mostrato un tipico messaggio di completamento dello script.

```
Connecting to the database: jdbc:oracle:thin:vcloud/vcloud@10.150.10.78:1521/vcloud
...........
Database configuration complete. Once the vCloud Director server has been started you will be
able to access the first-time setup wizard at this URL: http://vcloud.example.com Would you like
to start the vCloud Director service now? If you choose not to start it now, you can manually
start it at any time using this command: service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment). The service was started; it may
be several minutes before it is ready for use. Please check the logs for complete details.
vCloud Director configuration is now complete. Exiting...
```

Passi successivi

Nota: Le informazioni sulle connessioni di database e le altre risposte riutilizzabili fornite durante la configurazione vengono conservate in un file disponibile nel percorso `/opt/vmware/vcloud-director/etc/responses.properties` del server. In tale file sono contenute informazioni riservate da riutilizzare per l'aggiunta di altri server a un gruppo di server. Conservare il file in un luogo sicuro in modo che sia disponibile all'occorrenza.

Per aggiungere altri server al gruppo, vedere "Installazione del software vCloud Director su membri aggiuntivi di un gruppo di server", pag. 35.

Quando i servizi di vCloud Director sono in esecuzione su tutti i server, è possibile aprire l'installazione guidata quando viene visualizzato l'URL al completamento dello script. Vedere Capitolo 4, “Installazione di vCloud Director”, pag. 53.

Protezione e riutilizzo del file di risposta

I dettagli relativi alle connessioni di rete e di database forniti durante la configurazione del primo server vCloud Director vengono salvati in un file di risposta. In tale file sono contenute informazioni riservate da riutilizzare per l'aggiunta di altri server a un gruppo di server. Conservare il file in un luogo sicuro in modo che sia disponibile all'occorrenza.

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 di database. Quando si aggiungono altri server al gruppo, è necessario utilizzare una copia del file di risposta per specificare i parametri di configurazione condivisi tra tutti i server.

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
```

Passi successivi

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

Installazione del software vCloud Director su membri aggiuntivi di un gruppo di server

È possibile aggiungere server a un gruppo di server vCloud Director in qualsiasi momento. Dal momento che 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 per fornire queste informazioni quando si configurano membri aggiuntivi.

Prerequisiti

- Verificare che sia possibile accedere al file di risposta creato quando è stato installato e configurato il primo membro di questo gruppo di server. Vedere “Protezione e riutilizzo del file di risposta”, pag. 35.
- Verificare che il databasevCloud Director sia accessibile da questo server.

- Verificare che i certificati SSL creati per questo server siano installati in una posizione accessibile dall'installatore. Vedere "Creazione e importazione di un certificato SSL firmato", pag. 19. Lo script di configurazione non viene eseguito con un'identità privilegiata, pertanto il file di archivio chiavi e il percorso in cui viene archiviato devono essere leggibili da qualsiasi utente. Grazie all'utilizzo dello stesso percorso dell'archivio chiavi (ad esempio `/tmp/certificates.ks`) su tutti i membri di un gruppo di server, verrà semplificato il processo di installazione.
- Recuperare le informazioni seguenti:
  - La password del file di archivio chiavi che include i certificati SSL per questo server.
  - La password di ogni certificato SSL.

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 caricato su un CD o un altro supporto, copiare il file di installazione in una posizione accessibile da tutti i server di destinazione.

3 Verificare che il file di installazione sia eseguibile.

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

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

4 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.

5 In una console, shell o finestra terminale, eseguire il file di installazione utilizzando l'opzione `-r` e specificando il nome di percorso del file di risposta.

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

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

Il programma di installazione stampa un avviso nel formato seguente se la chiave pubblica VMware non è stata installata nel server di destinazione.

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

Quando il programma di installazione viene eseguito con l'opzione `-r`, vengono effettuate le seguenti operazioni.

a Verifica che l'host soddisfi tutti i requisiti

b Verifica della firma digitale nel file di installazione

c Creazione dell'utente e il gruppo `vcloud`

d Apertura del pacchetto RPM vCloud Director

e Installazione del software

f Copia del file di risposta in una posizione leggibile da vcloud.

g Esecuzione dello script di configurazione utilizzando il file di risposta come input

Quando lo script di configurazione è in esecuzione, ricerca i certificati nel percorso salvati nel file di risposta (ad esempio, `/tmp/certificates.ks`), quindi richiede di fornire le password dell'archivio chiavi e del certificato. Se lo script di configurazione non trovi certificati validi nel percorso salvato nel file di risposta, viene richiesto un percorso per i certificati.

6 (Facoltativo) Ripetere la procedura per aggiungere più server al gruppo di server.

Passi successivi

Se il cloud necessita di supportare la personalizzazione guest per alcuni sistemi operativi Microsoft obsoleti, installare i file Sysprep su tutti i membri del gruppo di server. Vedere "Installazione dei file Microsoft Sysprep nei server", pag. 37.

Al termine dell'esecuzione dello script di configurazione e quando i servizi vCloud Director sono in esecuzione su tutti i server, è possibile aprire l'installazione guidata utilizzando l'URL visualizzato al completamento dello script. Vedere Capitolo 4, "Installazione di vCloud Director", pag. 53.

Installazione dei file Microsoft Sysprep nei server

Per consentire l'esecuzione in vCloud Director della personalizzazione guest sulle macchine virtuali con determinati sistemi operativi guest Windows, è necessario installare i file Microsoft Sysprep 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 `$VCLOUD_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 `$VCLOUD_HOME/guestcustomization/default/windows/sysprep`.

I nomi delle sottodirectory sono specifici per un sistema operativo guest.

Tavola 2-1. Assegnazioni di sottodirectory per file Sysprep

Sistema operativo guest	Sottodirectory da creare in $VCLOUD_HOME/guestcustomization/default/windows/sysprep
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 $VCLOUD_HOME/guestcustomization
```

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.

Avvio o arresto dei servizi di vCloud Director

Dopo aver completato l'installazione e l'impostazione delle connessioni di database su un server, è possibile avviare i servizi di vCloud Director su tale server, nonché arrestarli se sono in esecuzione.

Lo script di configurazione richiede di avviare i servizi di vCloud Director. È possibile far sì che lo script avvii i servizi automaticamente o avviarli manualmente in un secondo momento. Tali servizi devono essere in esecuzione per poter completare e inizializzare l'installazione.

I servizi di vCloud Director vengono avviati ogni volta che si riavvia un server.

IMPORTANTE: Se si arrestano i servizi di vCloud Director durante un aggiornamento del software vCloud Director, è necessario utilizzare lo strumento di gestione delle celle per disattivare la cella prima di eseguire l'arresto. Vedere "Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server", pag. 44.

Procedura

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

2 Avviare o arrestare i servizi.

Opzione	Azione
Avviare i servizi	Aprire una console, una shell o una finestra del terminale ed eseguire il comando riportato di seguito. `service vmware-vcd start`
Arrestare i servizi mentre la cella è in uso	Utilizzare lo strumento di gestione delle celle.
Arrestare i servizi mentre la cella non è in uso	Aprire una console, una shell o una finestra del terminale ed eseguire il comando riportato di seguito. `service vmware-vcd stop`

Disinstallazione del software vCloud Director

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 console, una shell o una finestra del terminale ed eseguire il comando `rpm`.

```
rpm –e vmware-vcloud-director
```

Eseguire l'aggiornamento di vCloud Director

3

Per eseguire l'aggiornamento di vCloud Director a una nuova versione, installare la nuova versione in ogni server del gruppo di server vCloud Director, eseguire l'aggiornamento del database vCloud Director e riavviare i servizi di vCloud Director.

IMPORTANTE: Questa procedura di aggiornamento presuppone che si aggiorni un'installazione di vCloud Director che utilizza VMware vSphere e componenti di rete (VMware NSX for vSphere o VMware vCloud Networking and Security) che siano compatibili anche con vCloud Director 8.0. Prima di iniziare questa procedura, fare riferimento alle *matrici di compatibilità dei prodotti VMware* alla pagina http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php per informazioni sulle versioni degli altri prodotti VMware che sono compatibili con la versione di vCloud Director attualmente in esecuzione e anche con vCloud Director 8.0. Potrebbe essere necessario aggiornare alcuni di questi componenti nell'installazione corrente di vCloud Director alle versioni che sono compatibili anche con vCloud Director 8.0.

Dopo aver eseguito l'aggiornamento di un server vCloud Director, è anche necessario eseguire l'aggiornamento del database 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, è necessario verificare che non vi siano task attivi sul 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 la personalizzazione guest vengono copiati nella nuova installazione.

A meno che non si utilizzi un servizio di bilanciamento del carico per distribuire le richieste dei client ai membri del gruppo di server vCloud Director (vedere "Utilizzo di un servizio di bilanciamento del carico per ridurre il tempo di inattività dei servizi", pag. 42), l'aggiornamento richiede un downtime di vCloud Director sufficiente per aggiornare il database e almeno un server.

Aggiornamento di un gruppo di server vCloud Director

1. Disabilitare l'accesso degli utenti a vCloud Director. È possibile visualizzare anche un messaggio di manutenzione durante l'aggiornamento. Vedere "Visualizzazione del messaggio di manutenzione durante un aggiornamento", pag. 43.
2. Utilizzare lo strumento di gestione delle celle per disattivare tutte le celle incluse nel gruppo di server e chiudere i servizi di vCloud Director su ogni server. Vedere "Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server", pag. 44.

3 Eseguire l'aggiornamento del software vCloud Director su tutti i membri del gruppo di server. Vedere "Esecuzione dell'aggiornamento del software vCloud Director in un membro di un gruppo di server", pag. 45. È possibile eseguire l'aggiornamento dei server uno alla volta o in parallelo, ma è necessario non riavviare i servizi di vCloud Director su un membro aggiornato del gruppo prima di aver eseguito l'aggiornamento del database vCloud Director.

4 Eseguire l'aggiornamento del database vCloud Director. Vedere "Esecuzione dell'aggiornamento del database vCloud Director", pag. 48.

5 Riavviare vCloud Director sui server sottoposti ad aggiornamento. Vedere "Avvio o arresto dei servizi di vCloud Director", pag. 38.

6 Abilitare l'accesso degli utenti a vCloud Director.

7 (Facoltativo) Eseguire l'aggiornamento di ogni vShield Manager o NSX Manager associato. Tutte le installazioni di vShield Manager o di NSX Manager registrate per questo gruppo di server devono essere aggiornate a una versione del software vShield Manager o NSX Manager compatibile con la versione di vCloud Director installata dall'aggiornamento. Se il programma di aggiornamento rileva una versione non compatibile di vShield Manager o di NSX Manager, l'operazione non è consentita. È necessario eseguire l'aggiornamento alla versione più recente di vShield Manager o NSX Manager, come descritto in "Piattaforme supportate", pag. 9, al fine di utilizzare le funzionalità di rete introdotte nella presente versione di vCloud Director. Vedere "Aggiornamento della versione di vShield Manager o NSX Manager esistente associata a un sistema vCenter Server collegato", pag. 49.

8 (Facoltativo) Aggiornare tutti i sistemi vCenter Server e gli host associati. Vedere "Esecuzione dell'aggiornamento dei sistemi vCenter Server, degli host e delle appliance vShield Edge", pag. 51. Tutti i sistemi vCenter Server registrati per questo gruppo di server devono essere aggiornati a una versione del software vCenter Server compatibile con la versione di vCloud Director installata dall'aggiornamento. Al termine dell'aggiornamento, non è più possibile accedere ai sistemi vCenter Server non compatibili da vCloud Director. Vedere "Piattaforme supportate", pag. 9.

Nota: Al termine dell'aggiornamento, se la console Web di vCloud Director è aperta nel browser, disconnettersi e cancellare la cache del browser prima di accedere di nuovo alla console Web.

Utilizzo di un servizio di bilanciamento del carico per ridurre il tempo di inattività dei servizi

Se si utilizza un servizio di bilanciamento del carico o un altro strumento che può forzare l'invio delle richieste a specifici server, è possibile eseguire l'aggiornamento di un sottoinsieme del gruppo di server garantendo al tempo stesso la disponibilità dei servizi esistenti nel sottoinsieme rimanente. Questo approccio consente di ridurre il tempo di inattività dei servizi di vCloud Director all'intervallo di tempo richiesto per l'aggiornamento del database vCloud Director. Durante l'aggiornamento, gli utenti potrebbero riscontrare una certa riduzione delle prestazioni; tuttavia, i task in corso continueranno ad essere eseguiti fino a quando uno qualsiasi dei sottoinsiemi del gruppo di server è operativo. Le sessioni della console potrebbero essere interrotte, ma sarà possibile riavviarle.

1 Utilizzare il servizio di bilanciamento del carico per reindirizzare le richieste di vCloud Director a un sottoinsieme dei server inclusi nel gruppo. A tale scopo, seguire le procedure consigliate per il servizio.

2 Utilizzare lo strumento di gestione delle celle per disattivare le celle che non gestiscono più le richieste e chiudere i servizi di vCloud Director su tali server.

Nota: Le sessioni della console instradate attraverso un proxy della console del server sono interrotte quando il server si arresta. Per ripristinare, i client possono aggiornare la finestra della console.

Vedere "Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server", pag. 44.

3 Eseguire l'aggiornamento del software vCloud Director sui membri del gruppo di server sui quali è stato arrestato vCloud Director, ma non riavviare tali servizi. Vedere "Esecuzione dell'aggiornamento del software vCloud Director in un membro di un gruppo di server", pag. 45.

4 Utilizzare lo strumento di gestione delle celle per disattivare le celle di cui non è stato ancora eseguito l'aggiornamento e chiudere i servizi di vCloud Director su tali server.

5 Eseguire l'aggiornamento del database vCloud Director. Vedere "Esecuzione dell'aggiornamento del database vCloud Director", pag. 48.

6 Riavviare vCloud Director sui server sottoposti ad aggiornamento. Vedere "Avvio o arresto dei servizi di vCloud Director", pag. 38.

7 (Facoltativo) Eseguire l'aggiornamento di ogni vShield Manager o NSX Manager associato. Vedere "Aggiornamento della versione di vShield Manager o NSX Manager esistente associata a un sistema vCenter Server collegato", pag. 49.

8 (Facoltativo) Aggiornare tutti i sistemi vCenter Server e gli host associati. Vedere "Esecuzione dell'aggiornamento dei sistemi vCenter Server, degli host e delle appliance vShield Edge", pag. 51.

9 Utilizzare lo strumento di bilanciamento del carico per reindirizzare le richieste di vCloud Director ai server sottoposti ad aggiornamento.

10 Eseguire l'aggiornamento del software vCloud Director sui server del gruppo rimanenti e riavviare vCloud Director su tali server al termine degli aggiornamenti. Vedere "Esecuzione dell'aggiornamento del software vCloud Director in un membro di un gruppo di server", pag. 45.

Visualizzazione del messaggio di manutenzione durante un aggiornamento

Se si prevede un processo di aggiornamento che può richiedere molto tempo e si desidera che durante l'aggiornamento venga visualizzato un messaggio che notifica che la manutenzione è in corso, è necessario garantire che almeno una cella rimanga accessibile mentre le altre vengono aggiornate. Eseguire il comando `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` sulla cella accessibile per abilitare il messaggio di manutenzione.

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

Quando si è pronti per rimettere in servizio una cella aggiornata, eseguire il comando sulla cella per disattivare il messaggio di manutenzione.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# service vmware-vcd restart
```

Questo capitolo include i seguenti argomenti:

Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server

Prima di eseguire l'aggiornamento di un server vCloud Director, utilizzare lo strumento di gestione delle celle per disattivare e chiudere i servizi di vCloud Director nella cella del server.

In vCloud Director viene creato un oggetto task per tenere traccia di ogni operazione asincrona richiesta da un utente e gestirla. 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 le informazioni su questo task, è necessario assicurarsi che non vi siano task in esecuzione quando si inizia il processo di aggiornamento.

Grazie allo strumento di gestione delle celle, è possibile sospendere lo scheduler dei task in modo che non sia possibile avviare nuovi task e quindi controllare lo stato di tutti i task attivi. È possibile attendere il completamento dei task in esecuzione o eseguire il login a vCloud Director come amministratore di sistema e annullarli. Vedere Capitolo 5, “Guida di riferimento allo strumento di gestione delle celle”, pag. 57. Se non vi sono task in esecuzione, è possibile utilizzare lo strumento di gestione delle celle per arrestare i servizi di vCloud Director.

Prerequisiti

- Assicurarsi di disporre delle credenziali di utente con privilegi avanzati per il server di destinazione
- e delle credenziali di amministratore di sistema di vCloud Director.
- Se questa cella sarà accessibile ai client vCloud Director durante il suo aggiornamento, utilizzare il comando `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` per attivare il messaggio di manutenzione della cella.

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

  Questo comando consente alla cella di rispondere a tutte le richieste con un messaggio di manutenzione. Se si utilizza un servizio di bilanciamento del carico o uno strumento simile per rendere la cella inaccessibile durante l'aggiornamento, non sarà necessario attivare il messaggio di manutenzione della cella.

Procedura

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

2 Utilizzare tale strumento per chiudere la cella in modo normale.

a Recuperare lo stato del processo corrente.

Il comando `cell-management-tool` seguente fornisce le credenziali dell'amministratore di sistema e restituisce il numero di processi in esecuzione.

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

b Arrestare lo scheduler dei task per disattivare la cella.

Utilizzare un comando `cell-management-tool` con il formato seguente:

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

Tale comando impedisce l'avvio di nuovi processi. L'esecuzione dei processi esistenti continua finché non vengono completati o annullati. Per annullare un processo, utilizzare la console Web di vCloud Director o l'API REST.

c Quando `Job count` è `0` e `Is Active` è `false`, è possibile chiudere la cella in modo sicuro.

Utilizzare un comando `cell-management-tool` con il formato seguente:

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

NOTA: È possibile fornire la password dell'amministratore di sistema di vCloud Director sulla riga dei comandi `cell-management-tool`, ma è più sicuro omettere la password. Ciò comporta la richiesta della password da parte di `cell-management-tool`, che non viene visualizzata nella schermata quando si digita.

Le sessioni della console instradate attraverso un proxy della console del server sono interrotte quando il server si arresta. Se altri membri del gruppo di server sono ancora attivi, i clienti possono aggiornare la finestra della console per ripristinare.

Passi successivi

Quando lo strumento di gestione delle celle avrà arrestato i servizi di vCloud Director in esecuzione sul server, sarà possibile eseguire l'aggiornamento del software vCloud Director del server o completare altre operazioni di manutenzione richieste dal server.

Esecuzione dell'aggiornamento del software vCloud Director in un membro di un gruppo di server

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.

Il software vCloud Director viene distribuito come file eseguibile Linux denominato `vmware-vcloud-director-8.0.0-`*nnnnnn*`.bin`, dove *nnnnnn* rappresenta un numero di build. Dopo aver installato l'aggiornamento su un membro di un gruppo di server, è necessario eseguire uno strumento che effettui l'aggiornamento del database vCloud Director utilizzato dal gruppo per poter riavviare i servizi di vCloud Director sul server sottoposto ad aggiornamento.

Prerequisiti

- Assicurarsi di disporre delle credenziali di utente con privilegi avanzati per il server di destinazione

- Per far sì che 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", pag. 27.
- Per disattivare e chiudere i servizi di vCloud Director nella cella del server, utilizzare lo strumento di gestione delle celle.
- Assicurarsi di disporre di una chiave di licenza valida per utilizzare la versione del software vCloud Director a cui si desidera effettuare l'aggiornamento.

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 caricato su un CD o un altro supporto, copiare il file di installazione in una posizione accessibile da tutti i 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
checksum-value installation-file
```

Confrontare il *valore-checksum* creato da questo comando con il checksum MD5 copiato dalla pagina di download.

4 Verificare che il file di installazione sia eseguibile.

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

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

5 Per disattivare la cella e chiudere i servizi di vCloud Director sul server, utilizzare lo strumento di gestione delle celle.

Vedere "Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server", pag. 44.

6 In una console, una shell o una finestra del terminale eseguire il file di installazione.

Per eseguire tale file, digitarne il percorso completo, ad esempio `./file-di-installazione`. 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 installata nel server che corrisponde alla versione del file di installazione o è successiva a questa, viene visualizzato un messaggio di errore ed eseguita la chiusura. In caso contrario, viene richiesto di confermare che si è pronti a eseguire l'aggiornamento del server.

```
Checking architecture...done
Checking for a supported Linux distribution...done
Checking for necessary RPM prerequisites...done
Checking free disk space...done
An older version of VMware vCloud Director has been detected
```

7 Rispondere al prompt di aggiornamento.

Opzione	Azione
Continuare l'aggiornamento.	Digitare **y**.
Chiudere la shell senza apportare modifiche all'installazione corrente.	Digitare **n**.

Dopo aver confermato di essere pronti per l'aggiornamento del server, il programma di installazione verifica che l'host soddisfi tutti i requisiti, apre il pacchetto vCloud Director RPM, arresta i servizi di vCloud Director sul server ed esegue l'aggiornamento del software vCloud Director installato.

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

Il programma di installazione visualizza un avviso nel formato seguente se la chiave pubblica VMware non è stata installata nel server di destinazione.

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

Il programma di installazione visualizza un avviso nel formato seguente, quando esegue modifiche al file `global.properties` esistente sul server di destinazione.

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-director/etc/global.properties.rpmnew
```

La maggior parte degli aggiornamenti richiede tale modifica e visualizza questo avviso. Se sono state effettuate modifiche al file `global.properties` esistente, è possibile recuperarle da `global.properties.rpmnew`.

8 (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 `/opt/vmware/vcloud-director/etc/log4j.properties`.
Se le proprietà di registrazione sono state modificate	Unire il file `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` al file `/opt/vmware/vcloud-director/etc/log4j.properties` esistente. Tale unione consente di conservare le modifiche apportate.

Al termine dell'aggiornamento del software vCloud Director, il programma di installazione mostra un messaggio che indica la posizione di archiviazione dei file di configurazione obsoleti e ricorda all'utente di eseguire lo strumento di aggiornamento dei database.

Passi successivi

- Eseguire l'aggiornamento del database vCloud Director utilizzato dal server, se questa operazione non è già stata eseguita.

- Se si è già provveduto all'aggiornamento del database vCloud Director utilizzato dal gruppo di server, è possibile riavviare il server sottoposto ad aggiornamento. Vedere "Avvio o arresto dei servizi di vCloud Director", pag. 38.

Esecuzione dell'aggiornamento del database vCloud Director

Dopo aver eseguito l'aggiornamento di un server inclusi nel gruppo di server vCloud Director, è necessario eseguire l'aggiornamento del database vCloud Director del gruppo prima di riavviare i servizi di vCloud Director sul server.

Tutti i server di un gruppo server vCloud Director condividono lo stesso database quindi, a prescindere dalla quantità di server che si intende aggiornare, il database deve essere aggiornato solo una volta. Dopo l'aggiornamento del database, i server vCloud Director non sono in grado di stabilire la connessione con esso fino al loro aggiornamento.

Prerequisiti

IMPORTANTE: Prima di eseguire l'aggiornamento del database esistente, effettuarne il backup utilizzando le procedure consigliate dal fornitore del software di database.

Verificare che tutte le celle vCloud Director siano disattivate. Vedere "Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server", pag. 44

Procedura

1 Aprire una console, una shell o una finestra del terminale e digitare il comando riportato di seguito per eseguire lo script di aggiornamento del database.

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

IMPORTANTE: Se lo script di aggiornamento del database rileva che una versione di vShield Manager o di NSX Manager non compatibile è registrata per questa installazione di vCloud Director, viene visualizzato un messaggio di avviso e l'aggiornamento viene annullato.

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

2 Rispondere ai prompt di aggiornamento del database.

a Confermare che si desidera continuare con l'aggiornamento del database.

```
Welcome to the vCloud Director upgrade utility This product is intended for use only by service providers under the terms and conditions of the VMware Service Provider Partner (VSPP) Program. If you are a member of the VSPP Program, please locate your license key before proceeding. If you are not a member of this program, do not proceed with this upgrade. Upgrading without a proper key will invalidate your support contract. This utility will apply several updates to the database. Please ensure you have created a backup of your database prior to continuing. Do you wish to upgrade the product now? [Y/N]:
```

Eseguire una delle azioni seguenti:

Opzione	Azione
Continuare l'aggiornamento.	Digitare **y**.
Chiudere la shell senza apportate modifiche al database vCloud Director corrente.	Digitare **n**.

b (Facoltativo) Se necessario, attendere che le celle diventino inattive.

Se lo strumento di aggiornamento del database rileva delle celle ancora attive, il tool richiederà di continuare l'aggiornamento o di uscire.

```
Found active cell. Name: "cell-01", IP Address: 10.150.151.190, Identifier: a2eb...
Do you wish to upgrade the database while cells are still active? [Y/N]
```

Se viene visualizzato questo prompt, digitare `n` per uscire dalla shell, quindi attendere cinque minuti e riavviare lo strumento di aggiornamento del database. Se lo strumento di aggiornamento del database continua ad avvisare della presenza di celle ancora attive, tornare alla procedura in "Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server", pag. 44 e verificare che tutte le celle siano state disattivate.

Dopo avere risposto a tutti i prompt, lo strumento di aggiornamento del database esegue e visualizza i messaggi di avanzamento.

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

Dopo l'aggiornamento del database, lo script di aggiornamento richiede l'avvio dei servizi vCloud Director sull'host.

```
Would you like to start the vCloud Director service now? If you choose not to start it now, you
can manually start it at any time using this command: service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment). Avvio di vmware-vcd-watchdog:
[ OK ] Avvio di vmware-vcd-cell [ OK ]
```

Aggiornamento della versione di vShield Manager o NSX Manager esistente associata a un sistema vCenter Server collegato

Prima di effettuare l'aggiornamento a un sistema vCenter Server e agli host collegati a vCloud Director, è necessario aggiornare la versione di vShield Manager o di NSX Manager associata a quel sistema vCenter Server.

Durante l'aggiornamento di vShield Manager o NSX Manager l'accesso alle funzioni amministrative di vShield Manager o NSX Manager viene interrotto, mentre i servizi di rete rimangono attivi.

Prerequisiti

- Assicurarsi che almeno una cella aggiornata nell'installazione di vCloud Director sia in esecuzione, prima di avviare l'aggiornamento. La cella scrive i dati sulle versioni aggiornate di vShield Manager o NSX Manager nel database di vCloud Director.
- Verificare di disporre degli elementi necessari per l'aggiornamento di vShield Manager o NSX Manager, a seconda di quale versione si sta aggiornando.

vShield Manager	NSX Manager
Consultare le informazioni sull'aggiornamento disponibili nella sezione dedicata alla documentazione di VMware vCloud Networking and Security all'indirizzo https://www.vmware.com/support/pubs/vshield_pubs.html.	Consultare le informazioni sull'aggiornamento disponibili nella sezione dedicata alla documentazione di NSX for vSphere all'indirizzo https://www.vmware.com/support/pubs/nsx_pubs.html.

Procedura

1 Aggiornare l'installazione della versione di vShield Manager o NSX Manager associata seguendo la procedura adatta al prodotto e alla versione che si desidera aggiornare.

ATTENZIONE: Quando si effettua l'aggiornamento a una nuova versione di NSX Manager, non aggiornare le appliance vShield Edge associate esistenti alle appliance NSX Edge. vCloud Director non supporta le appliance NSX Edge. Quando si utilizza NSX Manager con vCloud Director, vCloud Director utilizza NSX Manager per creare le appliance vShield Edge.

Opzione	Azione
Aggiornare un vShield Manager associato a una versione successiva di vShield Manager.	Consultare le informazioni sull'aggiornamento di vShield Manager nella *Guida all'installazione e all'aggiornamento di vShield* all'indirizzo https://www.vmware.com/support/pubs/vshield_pubs.html. Aggiornare solo vShield Manager, ma nessun altro componente vShield. Non aggiornare le appliance vShield Edge assegnate esistenti.
Aggiornare un vShield Manager associato a NSX Manager oppure aggiornare un NSX Manager associato a una versione successiva di NSX Manager.	Consultare le informazioni sull'aggiornamento di NSX Manager nella *Guida all'installazione e all'aggiornamento di NSX* all'indirizzo https://www.vmware.com/support/pubs/nsx_pubs.html. Aggiornare solo vShield Manager o NSX Manager, ma non gli altri componenti vShield o NSX for vSphere. Non aggiornare le appliance vShield Edge assegnate esistenti.

2 Ripetere Step 1 per ciascun vShield Manager o NSX Manager associato agli altri sistemi vCenter Server registrati al cloud.

Al termine dell'aggiornamento, vShield Manager o NSX Manager aggiornato informa vCloud Director dell'avvenuto aggiornamento del software alla nuova versione. Possono essere necessari diversi minuti prima che la notifica venga inviata e che vCloud Director la elabori.

Passi successivi

Dopo aver aggiornato ciascun vShield Manager o NSX Manager associato, è necessario aggiornare tutti gli altri sistemi vCenter Server e host registrati, prima di utilizzare vCloud Director per aggiornare le appliance vShield Edge associate. Vedere "Esecuzione dell'aggiornamento dei sistemi vCenter Server, degli host e delle appliance vShield Edge", pag. 51.

Esecuzione dell'aggiornamento dei sistemi vCenter Server, degli host e delle appliance vShield Edge

Dopo aver effettuato l'aggiornamento di vCloud Director e di vShield Manager o NSX Manager, è necessario aggiornare gli host e i sistemi vCenter Server collegati al cloud. Una volta che tutti i sistemi e gli host vCenter Server sono stati aggiornati, è necessario utilizzare vCloud Director per aggiornare le appliance vShield Edge ridistribuendo i gateway edge o reimpostando le reti di vApp.

Prerequisiti

Assicurarsi di aver già effettuato l'aggiornamento di ogni vShield Manager o NSX Manager associato ai sistemi vCenter Server collegati al cloud. Vedere "Aggiornamento della versione di vShield Manager o NSX Manager esistente associata a un sistema vCenter Server collegato", pag. 49.

Procedura

1 Effettuare l'aggiornamento del sistema vCenter Server collegato.

   Vedere la *Guida all'installazione e la configurazione di vSphere*.

2 Verificare tutti gli URL pubblici e le catene di certificati di vCloud Director.

   Nella scheda **Amministrazione** della console Web vCloud Director, fare clic su **Indirizzi pubblici** nel riquadro sinistro. Immettere i valori in tutti i campi

3 (Facoltativo) Se vCloud Director è stato configurato per utilizzare vCenter Single Sign On, sarà necessario annullare la registrazione e registrare di nuovo vCloud Director con il servizio di ricerca di vCenter.

   a Accedere a vCloud Director come amministratore di sistema utilizzando un account LDAP o locale. Per questo accesso, non utilizzare vCenter Single Sign On.

   b Annullare la registrazione di vCloud Director con il servizio di ricerca di vCenter.

      Nella scheda **Amministrazione** della console Web di vCloud Director, fare clic su **Federazione** nel riquadro sinistro e fare clic su **Annulla registrazione**. Per completare quest'azione, è necessario fornire le credenziali di amministratore di vCenter appropriate.

   c Registrare vCloud Director con il servizio di ricerca di vCenter.

      Vedere "Configurazione di vCloud Director per l'utilizzo di vCenter Single Sign On" nella*Guida per gli amministratori di vCloud Director*

4 Aggiornare la registrazione del sistema vCenter Server con vCloud Director.

   a Nella console Web di vCloud Director fare clic sulla scheda **Gestisci e monitora**, quindi su **vCenter** nel riquadro a sinistra.

   b Fare clic con il pulsante destro del mouse sul nome del vCenter Server e scegliere **Aggiorna**.

   c Fare clic su **Sì**.

5 Eseguire l'aggiornamento di ogni host supportato dal sistema vCenter Server aggiornato.

   Vedere la *Guida all'installazione e la configurazione di vSphere*. Per l'aggiornamento di ciascun host, effettuare le seguenti operazioni:

   a Nella console Web di vCloud Director, disabilitare l'host.

      Nella pagina **Gestisci e monitora**, fare clic su **Host**, quindi fare clic con il pulsante destro del mouse e selezionare **Disabilita host**.

   b 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.

c Aggiornare l'host.

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.

d Utilizzare il sistema vCenter Server per riconnettere l'host.

e Aggiornare l'agente host vCloud Director sull'host.

Vedere la sezione sull'aggiornamento di un agente host ESX/ESXi nella *Guida per gli utenti di vCloud*.

f Nella console Web di vCloud Director, abilitare l'host.

Nella pagina **Gestisci e monitora**, fare clic su **Host**, quindi fare clic con il pulsante destro del mouse e selezionare **Abilita host**.

g Utilizzare il sistema vCenter Server per disattivare la modalità di manutenzione dell'host.

6 Utilizzare vCloud Director aggiornato per eseguire l'aggiornamento di tutte le appliance vShield Edge gestite dal vShield Manager o NSX Manager aggiornato associato al sistema vCenter Server aggiornato.

ATTENZIONE: Se il sistema vCenter Server aggiornato è associato a NSX Manager e non a vShield Manager, utilizzare solo i metodi descritti in questo passaggio per eseguire l'aggiornamento automatico delle appliance vShield Edge utilizzando vCloud Director. Non utilizzare altri metodi per eseguire l'aggiornamento delle appliance vShield Edge associate alle appliance NSX Edge. vCloud Director non supporta le appliance NSX Edge. Quando si utilizza NSX Manager con vCloud Director, vCloud Director utilizza NSX Manager per creare le appliance vShield Edge.

Quando si utilizza la console Web di vCloud Director o l'API REST per reimpostare una rete protetta da vShield Edge, viene eseguito un aggiornamento automatico dell'appliance vShield Edge corretta.

- Per un gateway edge, ridistribuendo il gateway edge, viene effettuato l'aggiornamento dell'appliance vShield Edge associata al gateway edge.
- Per le reti di vApp a cui si connettono le macchine virtuali, come le reti di vApp instradate, le reti di vApp isolate o le rete di virtual data center dell'organizzazione con priorità applicata, reimpostando la rete di vApp dall'interno del contesto della vApp, viene effettuato l'aggiornamento dell'appliance vShield Edge associata a quella rete. Per utilizzare la console Web di vCloud Director per reimpostare la rete di vApp dall'interno del contesto di una vApp, passare alla scheda **Rete** della vApp, visualizzare i relativi dettagli di rete, fare clic con il pulsante destro del mouse sulla rete di vApp e selezionare **Reimposta rete**.

Per ulteriori informazioni su come ridistribuire i gateway edge e reimpostare le reti di vApp, consultare la guida online della console Web di vCloud Director oppure la *Guida di programmazione delle API di vCloud*, a seconda del metodo si intende utilizzare.

Passi successivi

Ripetere questa procedura per gli altri sistemi vCenter Server registrati sul cloud.

Installazione di vCloud Director 4

Dopo aver configurato tutti i server del gruppo di server vCloud Director e averli connessi al database, è possibile inizializzare il database del gruppo di server con un codice di licenza, un account di amministratore di sistema e le informazioni correlate. Al termine del processo, è possibile utilizzare la console Web di vCloud Director per completare il provisioning iniziale del cloud.

Per poter eseguire la console Web di vCloud Director, è necessario eseguire l'installazione guidata, durante la quale vengono raccolte le informazioni richieste dalla console Web per l'avvio. Al termine di tale procedura, la console Web viene avviata e viene visualizzata la schermata di login. La console Web di vCloud Director offre un insieme di strumenti per il provisioning e la gestione di un cloud. Include inoltre una funzionalità di Avvio rapido che consente di eseguire i vari passaggi tra cui il collegamento di vCloud Director a vCenter e la creazione di un'organizzazione.

Prerequisiti

- Completare l'installazione di tutti i server vCloud Director e verificare che i servizi di vCloud Director siano stati avviati su ognuno di essi.
- Procurarsi l'URL che viene visualizzato al completamento dello script di configurazione.

> **NOTA:** Per individuare l'URL dell'installazione guidata al termine dello script, cercare il nome di dominio completo associato all'indirizzo IP specificato per il servizio HTTP durante l'installazione del primo server e utilizzarlo per creare un URL con il formato https://*nome-dominio-completo*, ad esempio https://mycloud.example.com. Sarà quindi possibile connettersi alla procedura guidata di tale URL.

Completare l'installazione di tutti i server vCloud Director e verificare che i servizi di vCloud Director siano stati avviati su ognuno di essi.

Procedura

1 Aprire un browser Web e connetterlo all'URL visualizzato al termine dello script di configurazione.

> **NOTA:** Prima che l'installazione guidata o la console Web diventino disponibili, potrebbe essere necessario attendere alcuni minuti dopo l'avvio dei servizi di vCloud Director.

2 Seguire i prompt per completare l'installazione.

Questo capitolo include i seguenti argomenti:

Controllo della licenza per utente finale

Per poter configurare un gruppo di server vCloud Director, è necessario controllare e accettare la licenza per utente finale.

Procedura

1 Controllare la licenza per utente finale.

2 Accettare o rifiutare la licenza.

Opzione	Azione
Per accettare la licenza per utente finale.	Fare clic su **Sì, accetto i termini della licenza**.
Per rifiutare la licenza per utente finale.	**No, non accetto i termini della licenza**.

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

Immissione del codice di licenza

Per eseguire un cluster vCloud Director è necessaria una licenza. Tale licenza viene specificata come numero di serie di prodotto, archiviato nel database vCloud Director.

Il numero di serie di prodotto vCloud Director non corrisponde al codice di licenza del server vCenter. Per utilizzare un vCloud, è necessario disporre di un numero di serie di prodotto vCloud Director e di un codice di licenza per il server vCenter. È possibile richiedere entrambi i tipi di codici di licenza dal portale delle licenze VMware.

Procedura

1 Richiedere un numero di serie di prodotto vCloud Director dal portale delle licenze VMware.

2 Digitare il numero di serie di prodotto nella casella di testo **Product serial number**.

Creazione dell'account di amministratore di sistema

Specificare il nome utente, la password e le informazioni di contatto dell'amministratore di sistema di vCloud Director.

L'amministratore di sistema di vCloud Director dispone dei privilegi di utente con privilegi avanzati in tutto il cloud. La creazione dell'account iniziale di amministratore di sistema viene eseguita durante l'installazione di vCloud Director. Al termine dell'installazione e della configurazione, l'amministratore di sistema potrà creare ulteriori account di amministratore di sistema in base alle esigenze.

Procedura

1 Digitare il nome utente dell'amministratore di sistema.

2 Digitare la password dell'amministratore di sistema e confermarla.

3 Digitare il nome completo dell'amministratore di sistema.

4 Digitare l'indirizzo e-mail dell'amministratore di sistema.

Specifica delle impostazioni di sistema

È possibile specificare le impostazioni di sistema che controllano il modo in cui vCloud Director interagisce con vSphere e vShield Manager o NSX Manager.

Durante il processo di configurazione viene creata una cartella nel sistema vCenter Server collegato da utilizzare con vCloud Director e viene specificato un ID di installazione da utilizzare per la creazione di indirizzi MAC per le schede NIC virtuali.

Procedura

1 Digitare un nome per la cartella vCenter Server vCloud Director nel campo **Nome sistema**.

2 Utilizzare il campo **ID installazione** per specificare l'ID installazione di vCloud Director.

Se un data center include più installazioni di vCloud Director, ogni installazione deve specificare un ID installazione univoco.

Login a vCloud Director

Dopo aver fornito tutte le informazioni richieste durante l'installazione guidata, è possibile confermare le impostazioni e completare la procedura guidata. Al termine della procedura, verrà visualizzata la schermata di login della console Web di vCloud Director.

Nella pagina Pronto per il login sono elencate tutte le impostazioni specificate durante la procedura guidata. Controllarle attentamente.

Prerequisiti

Assicurarsi di avere accesso al sistema vCenter Server che si desidera utilizzare con il cloud e al vShield Manager o al NSX Manager associato a quel sistema vCenter Server. La console Web di vCloud Director richiede l'accesso alle installazioni di vCenter Server e vShield Manager o NSX Manager che si desidera configurare insieme all'installazione di vCloud Director. Per poter completare questo task, è necessario che tali installazioni siano in esecuzione e configurate per interagire tra loro. Per ulteriori informazioni sui requisiti di configurazione, vedere "Requisiti hardware e software di vCloud Director", pag. 9.

Procedura

- Per modificare un'impostazione, fare clic su **Indietro** finché non verrà visualizzata la pagina di origine dell'impostazione.
- Per confermare tutte le impostazioni e completare il processo di configurazione, fare clic su **Fine**.

Dopo aver fatto clic su **Fine**, verranno applicate tutte le impostazioni specificate e verrà avviata la console Web di vCloud Director con la schermata di login visualizzata.

Passi successivi

Utilizzare la schermata di login per accedere alla console Web di vCloud Director utilizzando il nome utente e la password specificati per l'account dell'amministratore di sistema. Dopo aver eseguito il login, nella console verrà visualizzato un set di passaggi di Avvio rapido che è necessario completare per poter utilizzare il cloud. Al termine di queste operazioni, i Task guidati risulteranno abilitati e il cloud sarà pronto per l'utilizzo.

Guida di riferimento allo strumento di gestione delle celle 5

Lo strumento di gestione delle celle è una utilità della riga di comando utilizzabile per gestire una cella e i suoi certificati SSL, nonché esportare le tabelle dal database vCloud Director. Per alcune 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/cell-management-tool`.

Elenco dei comandi disponibili

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

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

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

```
[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
ciphers - Reconfigure the list of disallowed SSL ciphers for the cell
configure-metrics - Collects and stores properties necessary for collecting and querying metrics
data
dbextract - Exports the data from the given set of tables
fix-scheduler-data - Scan database for corrupt scheduler data.  Fix scheduler job data if
corrupt.
generate-certs - Generates self-signed SSL certificates for use with vCD cell.
recover-password - Change a forgotten System Administrator password. Database credentials are
required.
fail-tasks - Fail all tasks running on this cell and set a custom failure message.

For command specific help:
 cell-management-tool <commandName> -h
```

- Gestione di una cella pag. 59

  Grazie al comando `cell` è possibile sospendere lo scheduler dei task in modo che non sia possibile avviare nuovi task, controllare lo stato dei task attivi, controllare la modalità di manutenzione della cella e chiudere la cella in modo normale.

- Esportazione delle tabelle del database pag. 60

  Usare il comando `dbextract` dello strumento di gestione delle celle per esportare dati dal database di vCloud Director.

- Rilevamento e riparazione dei dati danneggiati dello scheduler pag. 62

  Se si conoscono il nome utente e la password del database vCloud Director, è possibile utilizzare il comando `fix-scheduler-data` dello strumento di gestione delle celle ed effettuare la scansione del database per rilevare dati danneggiati dello scheduler e, all'occorrenza, ripararli.

- Sostituzione di certificati SSL pag. 63

  Utilizzare il comando `certificates` dello strumento di gestione delle celle per sostituire i certificati SSL delle celle.

- Generazione di certificati SSL autofirmati pag. 64

  Usare il comando `generate-certs` dello strumento di gestione delle celle per generare nuovi certificati SSL autofirmati per la cella.

- Gestione dell'elenco di crittografia SSL consentita pag. 65

  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 pag. 67

  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 connessione del database di valori pag. 68

  Utilizzare il comando `configure-metrics` dello strumento di gestione delle celle per connettere la cella al database dei valori facoltativo.

- Recupero della password dell'amministratore di sistema pag. 69

  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 pag. 69

  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.

Gestione di una cella

Grazie al comando `cell` è possibile sospendere lo scheduler dei task in modo che non sia possibile avviare nuovi task, controllare lo stato dei task attivi, controllare la modalità di manutenzione della cella e chiudere la cella in modo normale.

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

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

sysadmin-username Il nome utente di un amministratore di sistema vCloud Director.

sysadmin-password La password di un amministratore di sistema vCloud Director.

> **NOTA:** È possibile fornire la password dell'amministratore di sistema di vCloud Director sulla riga dei comandi `cell-management-tool`, ma è più sicuro omettere la password. Ciò comporta la richiesta della password da parte di `cell-management-tool`, che non viene visualizzata nella schermata quando si digita.

command Un sottocomando `cell`.

Tavola 5-1. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `cell`

Comando	Argomento	Descrizione
`--help` (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
`--maintenance` (`-m`)	`true` o `false`	Controlla la modalità di manutenzione della cella. L'argomento `true` pone la cella in modalità di manutenzione. (È necessario innanzitutto chiudere la cella) L'argomento `false` rilascia la cella dalla modalità di manutenzione.
`--quiesce` (`-q`)	`true` o `false`	Disattiva la cella. L'argomento `true` sospende lo scheduler. L'argomento `false` riavvia lo scheduler.
`--shutdown` (`-s`)	Nessuno	Esegue la chiusura dei servizi di vCloud Director sul server.
`--status` (`-t`)	Nessuno	Mostra informazioni sul numero di task in esecuzione sulla cella e sullo stato della cella.
`--status-verbose` (`-tt`)	Nessuno	Mostra informazioni dettagliate sui task in esecuzione sulla cella e sullo stato della cella.

Esempio: Visualizzazione dello stato dei task

La linea di comando `cell-management-tool` seguente fornisce le credenziali dell'amministratore di sistema e restituisce il numero di task in esecuzione. Quando `Job count` è `0` e `Is Active` è `false`, è possibile chiudere la cella in modo sicuro.

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

Esportazione delle tabelle del database

Usare il comando `dbextract` dello strumento di gestione delle celle per esportare dati dal database di vCloud Director.

Per esportare tabelle del database, usare una riga di comando con la seguente struttura:

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

Tavola 5-2. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `dbextract`

Opzione	Argomento	Descrizione
`--help` (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
`-categories`	Un elenco separato da virgole delle categorie della tabella da esportare.	Facoltativo. `NETWORKING` è l'unica categoria supportata
`-dataFile`	Il percorso assoluto di un file che descrive i dati da esportare.	Facoltativo. Se non specificato, il comando utilizza `$VCLOUD_HOME/etc/data_to_export.properties`. Vedere "Impostazione delle tabelle e delle colonne da esportare", pag. 61.
`-dumpFolder`	Il percorso assoluto di una cartella in cui creare il dump. La cartella deve essere esistente e scrivibile da vcloud.	Tutti i dati saranno esportati in un file in questa cartella.
`-exportSettingsFile`	Il percorso assoluto di un file di proprietà delle impostazioni di esportazione dei dati	Facoltativo. Se non specificato, il comando utilizza `$VCLOUD_HOME/etc/data_export_settings.ini`. Vedere "Limitazione e ordinamento delle righe esportate", pag. 62.
`-properties`	Il percorso assoluto di un file di proprietà delle connessioni al database.	Facoltativo. Se non specificato, il comando utilizza le proprietà di connessione del database in `$VCLOUD_HOME/etc/global.properties`. Vedere "Indicazione di un file di proprietà", pag. 61.
`-tables`	Un elenco separato da virgole di tabelle.	Facoltativo. Esporta tutte le tabelle per visualizzare i singoli nomi di tabella.

Indicazione di un file di proprietà

Per impostazione predefinita, il comando `dbextract` estrae i dati dal database vCloud Director utilizzando le informazioni di connessione del database nel file `$VCLOUD_HOME/etc/global.properties` della cella corrente. Per estrarre i dati da un database vCloud Director differente, specificare le proprietà di connessione del database in un file e utilizzare l'opzione `–properties` per fornire il percorso di tale file nella riga di comando. Il file di proprietà è un file UTF-8 ed è caratterizzato dal seguente formato.

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

nome utente	Il nome utente del database vCloud Director.
password	La password del database vCloud Director.
nome_servizio_db	Il nome del servizio di database. Ad esempio, `orcl.example.com`.
porta_connessione_db	La porta del database.
indirizzo_ip_server_db	L'indirizzo IP del server di database.
tipo_db	Il tipo di database. Deve essere `Oracle` o `MS_SQL`.

Impostazione delle tabelle e delle colonne da esportare

Per limitare il set di dati esportati, usare l'opzione `–exportSettingsFile` e creare un file `data_to_export.properties` che specifichi le singole tabelle e, se desiderato, le colonne da esportare. Si tratterà di un file UTF-8 che contiene nessuna o più righe nel formato *TABLE_NAME*:*COLUMN_NAME*.

NOME_TABELLA	Il nome di una tabella del database. Per visualizzare un elenco dei nomi delle tabelle, esportare tutte le tabelle.
NOME_COLONNA	Il nome di una colonna nel nome tabella *TABLE_NAME* specificato.

Il presente file di esempio `data_to_export.properties` esporta le colonne delle tabelle `ACL` e `ADDRESS_TRANSLATION`.

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

Il comando cercherà il file in `$VCLOUD_HOME/etc/data_to_export.properties`, ma è possibile specificare un altro percorso.

Limitazione e ordinamento delle righe esportate

Per qualsiasi tabella, è possibile specificare quante righe esportare e come ordinare le righe esportate. Usare l'opzione `–exportSettingsFile` e creare un file `data_export_settings.ini` che specifichi singole tabelle. Si tratterà di un file UTF-8 che contiene nessuna o più voci nel seguente formato:

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

NOME_TABELLA Il nome di una tabella del database. Per visualizzare un elenco dei nomi delle tabelle, esportare tutte le tabelle.

NOME_COLONNA Il nome di una colonna nel nome tabella *TABLE_NAME* specificato.

L'esempio `data_export_settings.ini` limita i dati esportati dalla tabella `AUDIT_EVENT` alle prime 10000 righe e ordina le righe in base al valore della colonna `event_time`

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

Il comando cercherà il file in `$VCLOUD_HOME/etc/data_export_settings.ini`, ma è possibile specificare un altro percorso.

Esempio: Esportazione di tutte le tabelle dal database vCloud Director corrente.

Questo esempio esporta tutte le tabelle del database vCloud Director corrente sul file `/tmp/dbdump` .

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

Rilevamento e riparazione dei dati danneggiati dello scheduler

Se si conoscono il nome utente e la password del database vCloud Director, è possibile utilizzare il comando `fix-scheduler-data` dello strumento di gestione delle celle ed effettuare la scansione del database per rilevare dati danneggiati dello scheduler e, all'occorrenza, ripararli.

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
```

Tavola 5-3. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `fix-scheduler-data`

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

Sostituzione di certificati SSL

Utilizzare il comando `certificates` dello strumento di gestione delle celle per sostituire i certificati SSL delle celle.

Il comando `certificates` dello strumento di gestione delle celle automatizza la procedura di sostituzione dei certificati esistenti delle celle con quelli nuovi memorizzati nell'archivio chiavi JCEKS. Il comando `certificates` consente di sostituire i certificati autofirmati con quelli firmati. Per creare un archivio chiavi JCEKS che contenga i certificati firmati, vedere "Creazione e importazione di un certificato SSL firmato", pag. 19.

Per sostituire i certificati SSL di una cella, utilizzare un comando con la seguente struttura:

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

Tavola 5-4. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `certificates`

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

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
Certificato sostituito dall'archivio chiavi dell'utente specificato in /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.

Generazione di certificati SSL autofirmati

Usare il comando `generate-certs` dello strumento di gestione delle celle per generare nuovi certificati SSL autofirmati per la cella.

Il comando `generate-certs` dello strumento di gestione delle celle automatizza la procedura mostrata in "Creazione di un certificato SSL autofirmato", pag. 22.

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`*

Tavola 5-5. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `generate-certs`

Opzione	Argomento	Descrizione
`--help` (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
`--expiration` (-x)	*days-until-expiration*	Il numero di giorni alla scadenza del certificato. Impostazione predefinita: 365.
`--issuer` (-i)	*name=value* [, *name=value*, ...]	X.509 nome distinto dell'autorità emittente del certificato. Impostazione predefinita: `CN=`*`FQDN`*. dove *FQDN* 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.
`--httpcert` (-j)	Nessuno	Generare un certificato per l'endpoint http.
`--key-size` (-s)	*key-size*	Le dimensioni della coppia di chiavi espresse come numero intero di bit. Impostazione predefinita: 2048. Nota: le dimensioni delle chiavi inferiori a 1024 non sono più supportate, come riportato nella Pubblicazione speciale 800-131A del NIST.
`--keystore-pwd` (-w)	*keystore-password*	La password dell'archivio chiavi sull'host.

Tavola 5-5. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `generate-certs` (Continua)

Opzione	Argomento	Descrizione
`--out` (-o)	*keystore-pathname*	Il percorso completo dell'archivio chiavi sull'host.
`--consoleproxycert` (-p)	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 pressuppone 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.
```

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 "Esempio: Elencare tutta la crittografia consentita", pag. 66 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
```

Tavola 5-6. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `ciphers`

Opzione	Argomento	Descrizione
`--help` (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
`--all-allowed` (-a)	Nessuno	Elencare tutta la crittografia consentita.
`--compatible-reset` (-c)	Nessuno	Ripristinare sui valori predefiniti l'elenco della crittografia consentita, inoltre, ammettere la crittografia utilizzata dai certificati di questa cella.
`--disallow` (-d)	Elenco separato da virgole dei nomi di crittografia, come pubblicato all'indirizzo http://www.openssl.org/docs/apps/ciphers.html	Escludere la crittografia nell'elenco separato da virgole specificato.
`--list` (-l)	Nessuno	Elencare la crittografia attualmente configurata.
`--reset` (-r)	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 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
```

Tavola 5-7. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `ssl-protocols`

Opzione	Argomento	Descrizione
`--help` (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
`--all-allowed` (-a)	Nessuno	Elenco dei protocolli SSL supportati da vCloud Director.
`--disallow` (-d)	Elenco separato da virgole dei nomi dei protocolli SSL.	Consente di riconfigurare l'elenco dei protocolli SSL non consentiti con quelli specificati nell'elenco.
`--list` (-l)	Nessuno	Elenco dei set di protocolli SSL consentiti, correntemente supportati da vCloud Director.
`--reset` (-r)	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 TLSv1
```

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`.

In questo esempio, il protocollo SSL TLSv1 viene rimosso dall'elenco dei protocolli SSL consentiti.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool ssl-protocols -d TLSv1,SSLv3,SSLv2Hello
```

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

Configurazione della connessione del database di valori

Utilizzare il comando `configure-metrics` dello strumento di gestione delle celle per connettere la cella al database dei valori facoltativo.

vCloud Director può raccogliere i valori che forniscono informazioni attuali e cronologiche relative alle prestazioni e all'utilizzo di risorse delle macchine virtuali. I dati della cronologia dei valori sono memorizzati in un database KairosDB supportato da Cassandra. Vedere Capitolo 6, "Installazione e configurazione del software di database opzionale per memorizzare e recuperare la cronologia dei valori delle prestazioni delle macchine virtuali", pag. 71.

Per creare una connessione da KairosDB a un vCloud Director, utilizzare una riga di comando con la seguente struttura:

```
cell-management-tool configure-metrics options
```

Tavola 5-8. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `configure-metrics`

Comando	Argomento	Descrizione
`--help` (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
`--repository-host`	Nome host o indirizzo IP dell'host KairosDB	In presenza di più installazioni di KairosDB, è necessario fornire l'indirizzo del bilanciamento del carico qui.
`--repository-port`	Porta KairosDB da utilizzare.	Per impostazione predefinita, KairosDB riceve alla porta 8080.

Esempio: Configurazione della connessione del database di valori

In questo esempio viene configurato il sistema per utilizzare un'istanza KairosDB ospitata all'indirizzo IP 10.0.0.1 alla porta predefinita. L'indirizzo può essere quello di una macchina singola che sta eseguendo una sola istanza di KairosDB oppure quello di un bilanciamento del carico che distribuisce le richieste a più installazioni di KairosDB.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]#
./cell-management-tool configure-metrics --repository-host 10.0.0.1 --repository-port 8080
```

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
```

Tavola 5-9. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `recover-password`

Opzione	Argomento	Descrizione
`--help` (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
`--dbuser`	Il nome utente dell'utente del database di vCloud Director.	Deve essere specificato con la riga di comando.
`--dbpassword`	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
```

Tavola 5-10. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `fail-tasks`

Comando	Argomento	Descrizione
`--help` (-h)	Nessuno	Fornisce un riepilogo dei comandi disponibili in questa categoria.
`--message` (-m)	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.

Installazione e configurazione del software di database opzionale per memorizzare e recuperare la cronologia dei valori delle prestazioni delle macchine virtuali

6

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 della cronologia dei valori sono memorizzati in un database KairosDB supportato da un cluster di Cassandra.

Cassandra e KairosDB sono database open source che, quando distribuiti insieme, offrono una soluzione scalabile e a prestazioni elevate per la raccolta dei dati come i valori delle macchine virtuali. Per permettere al cloud di supportare il recupero della cronologia dei valori dalle macchine virtuali, è necessario installare e configurare Cassandra e KairosDB, quindi utilizzare l'utilità `cell-management-tool` per connettere vCloud Director a KairosDB. Per il recupero dei valori attuali non è necessario disporre del software di database facoltativo.

Per supportare il recupero della cronologia dei valori, è necessario che vCloud Director disponga di un cluster di Cassandra. Un cluster di Cassandra è composto da una o più macchine su cui è installato Cassandra ed è in esecuzione il servizio di Cassandra. Per un'installazione di vCloud Director tipica, è necessario avere almeno tre macchine in un cluster di Cassandra. Poiché la funzionalità di monitoraggio dei valori di vCloud Director utilizza un fattore di replica di due, disponendo di tre macchine, i nodi, nel cluster di Cassandra, assicura che un nodo sia sempre disponibile a gestire una transazione. È possibile utilizzare un solo cluster di Cassandra per l'installazione di vCloud Director.

Inoltre, è necessario disporre di almeno un'istanza di KairosDB configurata per il funzionamento con il cluster di Cassandra. Se il cloud raccoglie la cronologia dei valori da molte macchine virtuali, potrebbero essere necessarie altre istanze di KairosDB. È possibile sia installare e configurare KairosDB su uno dei nodi di Cassandra e puntare lo strumento di gestione delle celle a quell'endpoint, sia installare e configurare KairosDB su ogni nodo di Cassandra, aggiungere un bilanciamento del carico di fronte alla configurazione e puntare lo strumento di gestione delle celle all'endpoint del bilanciamento del carico. PoichévCloud Director prevede di comunicare con KairosDB a un indirizzo IP singolo, è necessario che le installazioni che includono più istanze di KairosDB utilizzino un bilanciamento del carico per fornire quell'indirizzo e distribuire le richieste di vCloud Director alle istanze di KairosDB.

Prerequisiti

- Assicurarsi che vCloud Director sia installato e in esecuzione, prima di configurare il software del database facoltativo.
- Se non si conoscono già Cassandra e KairosDB, consultare il materiale disponibile agli indirizzi http://cassandra.apache.org/ e https://code.google.com/p/kairosdb/.
- Scaricare Cassandra 1.2.*x* o Cassandra 2.0.*x* all'indirizzo http://cassandra.apache.org/download/.
- Scaricare KairosDB 0.9.1 all'indirizzo https://code.google.com/p/kairosdb/.
- Completare l'installazione e la configurazione del cluster di Cassandra che si intende utilizzare con l'installazione di vCloud Director, in base alla seguente configurazione:
  - Cassandra 1.2.*x* o Cassandra 2.0.*x* è installato su almeno tre macchine connesse alla stessa rete utilizzata dalle celle di vCloud Director.

  - Le macchine sono configurate in modo che ognuna abbia il proprio storage fisico, anziché uno storage condiviso.
  - Le macchine sono configurate come un cluster di Cassandra.
  - Nel cluster di Cassandra è attivato Java Native Access (JNA) versione 3.2.7 o successiva, per migliorare le prestazioni di utilizzo di memoria e di accesso al disco.
- Completare l'installazione e la configurazione di almeno un'istanza di KairosDB 0.9.1 su uno dei nodi di Cassandra, in modo da utilizzare il cluster come suo database. Inoltre, aggiungendo un bilanciamento del carico di fronte a quella configurazione, è possibile installare e configurare KairosDB su ogni nodo di Cassandra.
- Assicurarsi che KairosDB e Cassandra siano configurati correttamente. Utilizzare un browser Web per andare all'indirizzo `http://KairosDB-IP:8080/api/v1/metricnames`. Se la pagina si apre senza errori, KairosDB e Cassandra sono configurati correttamente.
- Assicurarsi di poter eseguire il comando `service` dell'utilità `cell-management-tool`. Per dettagli sul comando `service`, vedere "Avvio o arresto dei servizi di vCloud Director", pag. 38.

Procedura

1 Utilizzare l'utilità `cell-management-tool` per configurare una connessione tra vCloud Director e KairosDB.

  Utilizzare un comando come questo, dove *KairosDB-IP* è l'indirizzo IP della macchina su cui è installato KairosDB, oppure l'indirizzo IP del bilanciamento del carico che si sta utilizzando per distribuire le richieste a più istanze di KairosDB.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool configure-metrics --repository-host KairosDB-IP
--repository-port 8080
```

2 Riavviare ogni cella di vCloud Director utilizzando il comando `service` dell'utilità `cell-management-tool`.

Indice

V