

Guida all'installazione e configurazione di vCloud Director

vCloud Director 1.5

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/support/pubs>.

IT-000582-00

vmware[®]

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

<http://www.vmware.com/it/support/pubs>

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

Copyright © 2010, 2011 VMware Inc. Tutti i diritti sono riservati. Questo prodotto è tutelato dalle leggi statunitensi e internazionali sul copyright e sulla proprietà intellettuale. I prodotti VMware sono coperti da uno o più brevetti elencati sul sito <http://www.vmware.com/go/patents-it>.

VMware è un marchio registrato o marchio di VMware, Inc negli Stati Uniti e/o in altre giurisdizioni. Tutti gli altri marchi e nomi menzionati possono essere marchi delle rispettive società.

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 configurazione di VMware vCloud Director	5
1 Panoramica dell'installazione e della configurazione di vCloud Director	7
Architettura di vCloud Director	7
Pianificazione della configurazione	8
Requisiti hardware e software di vCloud Director	9
2 Creazione di un gruppo di server vCloud Director	25
Installazione e configurazione del software vCloud Director in un membro di un gruppo di server	26
Configurazione delle connessioni di rete e di database	28
Avvio o arresto dei servizi di vCloud Director	31
Installazione del software vCloud Director in altri server	32
Creazione di un pacchetto di distribuzione Microsoft Sysprep	33
Disinstallazione del software vCloud Director	34
3 Eseguire l'aggiornamento di vCloud Director	35
Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server	36
Esecuzione dell'aggiornamento del software vCloud Director in un membro di un gruppo di server	39
Esecuzione dell'aggiornamento del database vCloud Director	41
Esecuzione dell'aggiornamento degli host vCenter e ESX/ESXi	42
Esecuzione dell'aggiornamento di vShield Manager	43
Ripristino di un aggiornamento	43
4 Installazione di vCloud Director	45
Controllo della licenza per utente finale	46
Immissione del codice di licenza	46
Creazione dell'account di amministratore di sistema	46
Specifiche delle impostazioni di sistema	47
Login a vCloud Director	47
Indice	49

Guida all'installazione e configurazione di VMware vCloud Director

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

Destinatari della guida

La guida è rivolta a chiunque desideri installare e configurare il software VMware vCloud Director. 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 dell'installazione e della configurazione di vCloud Director

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.

VMware vCloud Director si basa su VMware vSphere[®] ed espone l'infrastruttura virtualizzata condivisa come virtual data center multi-tenant separati dall'hardware sottostante e isolati tra loro. È possibile esporre i vDC agli utenti tramite un portale basato su Web e definire ed esporre un catalogo di servizi distribuibili all'interno dei vDC.

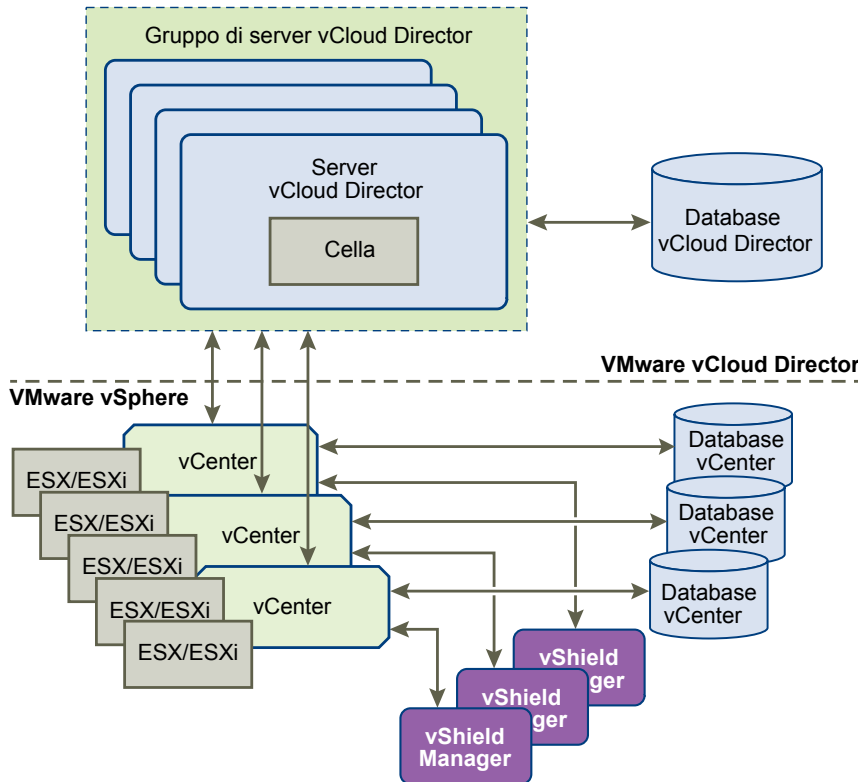
Questo capitolo include i seguenti argomenti:

- [“Architettura di vCloud Director”](#), pag. 7
- [“Pianificazione della configurazione”](#), pag. 8
- [“Requisiti hardware e software di vCloud Director”](#), pag. 9

Architettura di vCloud Director

Un gruppo di server vCloud Director è costituito da uno o più server vCloud Director. Tali server condividono un database comune e sono collegati a un numero arbitrario di server vCenter e di host ESX/ESXi. I server vShield Manager forniscono servizi di rete a vCenter e a vCloud Director.

Una semplice architettura cloud può contenere un gruppo di server vCloud Director che comprende più server. Ogni server può eseguire una raccolta di servizi denominata cella vCloud Director. Tutti i server inclusi nel gruppo condividono un singolo database. Il gruppo si connette a più server vCenter e agli host ESX/ESXi che essi gestiscono. Ogni server vCenter si connette a un server vShield Manager.

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

Durante il processo di installazione e di configurazione di vCloud Director, vengono create le celle e successivamente connesse al database condiviso, quindi vengono stabilite le prime connessioni a un server vCenter, vShield Manager e agli host ESX/ESXi. Un amministratore di sistema può quindi utilizzare la console Web di vCloud Director per connettere altri server vCenter, vShield Manager ed ESX/ESXi al gruppo di server vCloud Director in qualsiasi momento.

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 server vCenter 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 server vCenter, a un server vShield Manager e a uno o più host ESX/ESXi.

Versioni di vCenter, ESX/ESXi e vShield Manager supportate

Tavola 1-1. Versioni vCenter supportate

Versione vCenter	Note
4.0 Update 2	
4.0 Update 3	
4.1	
4.1 Update 1	
5.0	Richiesto per il supporto del provisioning rapido, della versione hardware 8 e della rete VPN

Tavola 1-2. Versioni di ESX/ESXi supportate

Versione ESX o ESXi	Note
4.0 Update 2	
4.0 Update 3	
4.1	
4.1 Update 1	
5.0	Richiesto per il supporto del provisioning rapido e della versione hardware 8

Tavola 1-3. Versioni di vShield Manager supportate

Versione vShield Manager	Note
1.0	
1.0 Update 1	
5.0	Richiesto per il routing statico e il supporto VPN

Requisiti per la configurazione di vSphere

I server vCenter e gli host ESX/ESXi 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 DVS per applicare la priorità tra gli host e allocare i pool di reti.
- I cluster vCenter utilizzati con vCloud Director devono essere configurati per l'utilizzo del DRS automatico, che richiede uno storage condiviso collegato a tutti gli host di un cluster DRS.
- I cluster vCenter 5 utilizzati con vCloud Director non devono abilitare il DRS dello storage.
- I server vCenter devono considerare attendibili i rispettivi host ESX/ESXi.

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 1-4. Sistemi operativi dei server vCloud Director supportati

Sistema operativo
Red Hat Enterprise Linux 5 (64 bit), Update 4
Red Hat Enterprise Linux 5 (64 bit), Update 5
Red Hat Enterprise Linux 5 (64 bit), Update 6

Requisiti di spazio su disco Ogni server vCloud Director richiede circa 950 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 1 GB di memoria, ma è consigliabile utilizzare 2 GB.

Per impostazione predefinita, i pacchetti richiesti 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 1-5. 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	

Database vCloud Director supportati

Tavola 1-6. Software di database vCloud Director supportati

Software di database	Patch o service pack richiesti
Oracle 10g Standard Edition Release 2	10.2.0.x
Oracle 10g Enterprise Edition Release 2	10.2.0.x
Oracle 11g Standard Edition	11.1.0.x
Oracle 11g Enterprise Edition	11.1.0.x

Tavola 1-6. Software di database vCloud Director supportati (Continua)

Software di database	Patch o service pack richiesti
Oracle 11g R2	11.2.0.x
Microsoft SQL Server 2005 Standard	SP4
Microsoft SQL Server 2005 Enterprise	SP4
Microsoft SQL Server 2008 Express (64 bit)	SP2
Microsoft SQL Server 2008 Standard (64 bit)	Aggiornamento cumulativo 2
Microsoft SQL Server 2008 Enterprise (64 bit)	Aggiornamento cumulativo 2

Per le configurazioni dei server di database consigliate, vedere [“Installazione e configurazione di un database vCloud Director”](#), pag. 15.

Server LDAP supportati

Tavola 1-7. 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

vCloud Director supporta macchine virtuali con i sistemi operativi guest elencati di seguito.

Tavola 1-8. Supporto per il sistema operativo guest

Sistema operativo guest	ESX 4.0 U2	ESX 4.0 U3	ESX 4.1	ESX 4.1 U1	ESX 5.0
Windows Server 2008 R2 (x64)	Sì	Sì	Sì	Sì	Sì
Windows Server 2008	Sì	Sì	Sì	Sì	Sì
Windows 7	Sì	Sì	Sì	Sì	Sì
Windows Vista	Sì	Sì	Sì	Sì	Sì
Windows XP/Embedded	Sì	Sì	Sì	Sì	Sì
Windows Server 2003	Sì	Sì	Sì	Sì	Sì
Windows Server 2000	Sì	Sì	Sì	Sì	Sì
Windows NT	Sì	Sì	Sì	Sì	Sì
CentOS 4/5	Sì	Sì	Sì	Sì	Sì
SLES 11	Sì	Sì	No	Sì	Sì
SLES 10		Sì	Sì	Sì	Sì
SLES 8,9	Sì	Sì	Sì	Sì	Sì
Asianux 4	No	No	No	No	Sì
Asianux 3	Sì	Sì	Sì	Sì	Sì
RHEL 6	Sì	Sì	Sì	Sì	Sì
RHEL 5	Sì	Sì	Sì	Sì	Sì
RHEL 4	Sì	Sì	Sì	Sì	Sì

Tavola 1-8. Supporto per il sistema operativo guest (Continua)

Sistema operativo guest	ESX 4.0 U2	ESX 4.0 U3	ESX 4.1	ESX 4.1 U1	ESX 5.0
RHEL 3	Sì	Sì	Sì	Sì	Sì
RHEL 2 (x32)	Sì	Sì	Sì	Sì	Sì
Debian GNU/Linux 6	No	No	No	No	Sì
Debian GNU/Linux 5	Sì	Sì	Sì	Sì	Sì
Debian GNU/Linux 4	Sì	Sì	Sì	Sì	Sì
Ubuntu	Sì	Sì	Sì	Sì	Sì
Oracle Enterprise Linux 4/5	Sì	Sì	No	Sì	Sì
Altri sistemi Linux 2.6.x	Sì	Sì	Sì	Sì	Sì
Altri sistemi Linux 2.4.x	Sì	Sì	Sì	Sì	Sì
Solaris 10	Sì	Sì	Sì	Sì	Sì

Browser supportati in vCloud Director

La console Web di vCloud Director è compatibile con diverse versioni di browser Web Firefox e 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.

Browser supportati sulle piattaforme Microsoft Windows

Tavola 1-9. Supporto dei browser e compatibilità con i sistemi operativi sulle piattaforme Microsoft Windows

Piattaforma	Internet Explorer 7.x	Internet Explorer 8.x	Internet Explorer 9.x	Firefox 3.6, 4.x	Firefox 5.x
Windows XP Pro a 32 bit	Sì	Sì	No	Sì	Sì
Windows XP Pro a 64 bit	Sì	Sì	No	Sì	Sì
Windows Server 2003 Enterprise Edition a 32 bit	Sì	Sì	No	Sì	Sì
Windows Server 2003 Enterprise Edition a 64 bit	Sì	Sì	No	Sì	Sì
Windows Server 2008	Sì	Sì	Sì	Sì	N/D
Windows Server 2008 R2	No	Sì	Sì	Sì	N/D
Windows Vista a 32 bit	Sì	Sì	Sì	Sì	Sì
Windows Vista a 64 bit	Sì	Sì	Sì	No	Sì
Windows 7 a 32 bit	No	Sì	Sì	Sì	Sì
Windows 7 a 64 bit	No	Sì	Sì	Sì	Sì

Browser supportati sulle piattaforme Linux

Tavola 1-10. Supporto dei browser e compatibilità con i sistemi operativi sulle piattaforme Linux

Piattaforma	Firefox 3	Firefox 4.x	Firefox 5.x
Red Hat Enterprise Linux 5 (32 bit), Update 6	No	Sì	Sì
Red Hat Enterprise Linux 6 (32 bit)	No	Sì	Sì
Red Hat Enterprise Linux 6 (64 bit)	No	Sì	Sì
SLES 11 a 32 bit	No	Sì	Sì
Ubuntu 10.10 a 32 bit	No	Sì	Sì
Ubuntu 10.10 a 64 bit	No	Sì	Sì

Versioni supportate di Adobe Flash Player

La console Web di vCloud Director richiede Adobe Flash Player versione 10.2 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.

Versioni dei protocolli TLS e SSL e pacchetti di crittografia supportati

vCloud Director richiede l'utilizzo di SSL sui client. Le versioni supportate includono SSL 3.0 e TLS 1.0. 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.

Riepilogo dei requisiti per la configurazione di rete

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 di database, i server vCenter e i server vShield Manager deve 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 <code>ip addr add</code> 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.

Risoluzione dei nomi host

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

```
nslookup mycloud
nslookup mycloud.example.com
```

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

```
nslookup 192.168.1.1
```

Storage del server di trasferimento

Per fornire uno storage temporaneo per i caricamenti e i download, è necessario che un NFS o un altro volume di storage condiviso sia accessibile da tutti i server di un cluster vCloud Director. Tale volume deve disporre dell'autorizzazione di scrittura per la directory root. Ogni host deve montare il volume nel percorso `$VCLLOUD_HOME/data/transfer`, che in genere corrisponde a `/opt/vmware/vcloud-director/data/transfer`. I caricamenti e i download occupano lo storage per un intervallo di tempo che va da alcune ore a un giorno. Poiché le immagini trasferite possono essere grandi, è necessario allocare almeno diverse centinaia di GB al volume.

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). Il firewall deve rifiutare tutto il rimanente traffico in entrata da una rete pubblica.

Tavola 1-11. 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 1-12. Porte che devono consentire il passaggio di pacchetti in uscita dagli host vCloud Director

Porta	Protocollo	Commenti
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	Portmapper NFS utilizzato dal servizio di trasferimento

Tavola 1-12. Porte che devono consentire il passaggio di pacchetti in uscita dagli host vCloud Director (Continua)

Porta	Protocollo	Commenti
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	Connessioni vCenter ed 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

- Non connettere computer host fisici a reti fisiche che rappresentano uplink per i commutatori distribuiti vNetwork che supportano i pool di reti vCloud Director.
- 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 comandi nel formato indicato di seguito per creare spazi tabelle di dati (CLOUD_DATA) e indici (CLOUD_INDX) separati:

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

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

3 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/tsnames.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 richiede 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 da utilizzare in un cluster vCloud Director richiede due certificati SSL, uno per ogni indirizzo IP.

NOTA: Tutte le directory incluse nel nome di percorso dei certificati SSL devono essere leggibili dall'utente vcloud.vcloud. Tale utente viene creato dal programma di installazione di vCloud Director.

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.

- 4 Creare i certificati.

È possibile utilizzare certificati firmati da un'autorità di certificazione attendibile o certificati autofirmati. 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 ogni indirizzo IP, in un file di archivio dati Java. È necessario creare due certificati SSL per ogni server che verrà utilizzato nel gruppo di server vCloud Director. È possibile utilizzare certificati firmati da un'autorità di certificazione attendibile o certificati autofirmati. I certificati firmati garantiscono il livello di attendibilità più elevato.

Per creare e importare certificati autofirmati, vedere [“Creazione di un certificato SSL autofirmato”](#), pag. 21.

Prerequisiti

- Generare un elenco di nomi di dominio completi con gli indirizzi IP associati sul server, insieme a un'opzione di servizio per ogni indirizzo IP. Vedere [“Creazione di certificati SSL”](#), pag. 18.
- Assicurarsi di disporre di accesso a un computer con un ambiente di runtime Java versione 6, 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 6 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*.

Procedura

- 1 Creare un certificato non attendibile per il servizio HTTP.

Il comando riportato di seguito consente di creare un certificato non attendibile in un file di archivio chiavi denominato `certificates.ks`.

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

- 2 Rispondere alle domande di `keytool`.

Quando `keytool` richiede l'immissione di nome e cognome, digitare il nome di dominio completo associato all'indirizzo IP da utilizzare per il servizio HTTP.

- 3 Per le domande rimanenti, fornire risposte appropriate all'organizzazione e alla posizione, come illustrato nell'esempio che segue.

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

- 4 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
```

- 5 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](#).

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

- 6 Quando keytool richiede l'immissione di nome e cognome, digitare il nome di dominio completo associato all'indirizzo IP da utilizzare per il servizio proxy della console.

- 7 Per le domande rimanenti, fornire risposte appropriate all'organizzazione e alla posizione, come illustrato nell'esempio in [Step 1](#).

- 8 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
```

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

- 10 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
```

- 11 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
```

- 12 Ripetere i passaggi da [Step 1](#) a [Step 11](#) su ognuno dei server vCloud Director rimanenti.

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. 28.

NOTA: Poiché lo script di configurazione di vCloud Director non viene eseguito con un'identità privilegiata, il file di archivio chiavi e la directory in cui è archiviato devono essere leggibili da qualsiasi utente.

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 ogni indirizzo IP, in un file di archivio dati Java. È necessario creare due certificati SSL per ogni server che verrà utilizzato nel gruppo di server vCloud Director. È possibile utilizzare certificati firmati da un'autorità di certificazione attendibile o certificati autofirmati. I certificati firmati garantiscono il livello di attendibilità più elevato.

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 con gli indirizzi IP associati sul server, insieme a un'opzione di servizio per ogni indirizzo IP. Vedere [“Creazione di certificati SSL”](#), pag. 18.
- Assicurarsi di disporre di accesso a un computer con un ambiente di runtime Java versione 6, 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 6 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*.

Procedura

- 1 Creare un certificato non attendibile per il servizio HTTP.

Il comando riportato di seguito consente di creare un certificato non attendibile in un file di archivio chiavi denominato `certificates.ks`.

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

- 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](#).

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

- 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 i passaggi da [Step 1](#) a [Step 3](#) su ognuno dei server vCloud Director rimanenti.

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. 28.

NOTA: Poiché lo script di configurazione di vCloud Director non viene eseguito con un'identità privilegiata, il file di archivio chiavi e la directory in cui è archiviato devono essere leggibili da qualsiasi utente.

Installazione e configurazione di vShield Manager

Per fornire servizi di rete al cloud, è necessario utilizzare vShield Manager con vCloud Director. Prima di avviare la procedura di installazione di vCloud Director, è dunque necessario installare e configurare vShield Manager.

Ogni vCenter Server aggiunto a vCloud Director deve essere associato a un'istanza univoca di vShield Manager. Per informazioni sui requisiti di rete e sulle versioni supportate di vShield Manager, vedere [“Requisiti hardware e software di vCloud Director”](#), pag. 9.

IMPORTANTE: Questa procedura è applicabile solo alle nuove installazioni di vCloud Director. Se si sta aggiornando un'installazione esistente di vCloud Director, è possibile aggiornarne facoltativamente l'installazione di vShield Manager associata. Non è possibile eseguire una nuova versione di vShield Manager con una versione esistente di vCloud Director. Vedere [“Esecuzione dell'aggiornamento di vShield Manager”](#), pag. 43.

Procedura

- 1 Utilizzare il vSphere Client per eseguire il login al vCenter Server.
- 2 Selezionare **File > Deploy OVF Template**.
- 3 Individuare la posizione del file `vShield Manager.ovf` e seguire i prompt per distribuirlo.
- 4 Dopo aver distribuito il file OVF, attivare la macchina virtuale vShield Manager e aprire la console.
- 5 Eseguire il login alla console con il nome utente **admin** e la password **default**.
- 6 Al prompt `manager` digitare **enable**.
- 7 Al prompt `Password`, digitare **default** per attivare la modalità di installazione.
Quando tale modalità viene attivata, la stringa del prompt cambia in `manager#`.
- 8 Al prompt `manager#` digitare **setup** per avviare la procedura di installazione.
- 9 Immettere l'indirizzo IP, la subnet mask e il gateway predefinito della macchina virtuale vShield Manager.
Queste informazioni sono necessarie per collegare un vCenter Server a Cloud Director.
- 10 Digitare **exit** per uscire dalla console.
- 11 Chiudere la console e lasciare in esecuzione la macchina virtuale.

Non è necessario sincronizzare vShield Manager con vCenter o registrare vShield Manager come plug-in di vSphere Client quando si utilizza vShield Manager con vCloud Director.

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.

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 utilizzare SSL con il servizio AMQP di vCloud Director, selezionare **Usa SSL** nella sezione Impostazioni broker AMQP della pagina Task bloccanti della console Web di vCloud Director e specificare il percorso del certificato SSL o il percorso e la password dell'archivio affidabilità JCEKS. Se non si desidera convalidare i certificati perché si ritengono affidabili tutti i computer connessi al servizio AMQP di vCloud Director, è possibile selezionare **Accetta 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 Ottenere e importare le chiavi pubbliche del pacchetto VMware.
 - a Creare una directory in cui archiviare le chiavi pubbliche del pacchetto VMware.
 - b Utilizzare un browser Web per scaricare tutte le chiavi pubbliche del pacchetto VMware dalla directory <http://packages.vmware.com/tools/keys>.
 - c Salvare i file di chiavi nella directory creata.
 - d 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.

- 2 (Facoltativo) Utilizzare lo strumento rpm di Linux per verificare la firma digitale del file scaricato.

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

Dopo aver verificato la firma digitale del file, è possibile utilizzarla per installare o aggiornare vCloud Director in qualsiasi server, senza dover installare la chiave pubblica in tale server. Il programma di installazione avvisa l'utente se non vi sono chiavi installate. È possibile ignorare l'avviso se la firma del file è stata già verificata.

Creazione di un gruppo di server vCloud Director

2

Un gruppo di server vCloud Director è costituito da uno o più server vCloud Director. Su ogni server del gruppo viene eseguita una raccolta di servizi denominata cella vCloud Director. Per creare un gruppo di server, installare il software vCloud Director in ogni server, configurarne le connessioni di rete e al database e avviarne i servizi vCloud Director.

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 aggiornando un'installazione di vCloud Director esistente, vedere [Capitolo 3, "Eseguire l'aggiornamento di vCloud Director"](#), pag. 35

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

- 1 Verificare che un server vCenter supportato sia in esecuzione e sia configurato correttamente per l'utilizzo con vCloud Director. Per le versioni supportate e i requisiti di configurazione, vedere ["Versioni di vCenter, ESX/ESXi e vShield Manager supportate"](#), pag. 9.
- 2 Verificare che un server vShield Manager supportato sia in esecuzione e sia configurato correttamente per l'utilizzo con vCloud Director. Per le versioni supportate, vedere ["Versioni di vCenter, ESX/ESXi e vShield Manager supportate"](#), pag. 9. Per informazioni dettagliate sull'installazione e sulla configurazione, vedere ["Installazione e configurazione di vShield Manager"](#), pag. 22.
- 3 Verificare che almeno una piattaforma server vCloud Director supportata sia in esecuzione e sia configurata con una quantità di memoria e di storage appropriata. 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 il supporto di una connessione SSL per il servizio HTTP e un altro 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 dall'utente `vccloud.vccloud`. Tale utente viene creato dal programma di installazione di vCloud Director. 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 `$VCLLOUD_HOME/data/transfer`, che in genere corrisponde a `/opt/vmware/vccloud-director/data/transfer`. Tale volume deve disporre dell'autorizzazione di scrittura per la directory `root`.
 - Ogni server deve disporre di accesso a un pacchetto di distribuzione Microsoft Sysprep. Vedere ["Creazione di un pacchetto di distribuzione Microsoft Sysprep"](#), pag. 33.

- 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.
 - Assicurarsi di disporre di un account per l'utente del database vCloud Director e dei privilegi di sistema 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 Verificare che tutti i server vCloud Director, il server di database e tutti i server vCenter e vShield Manager siano in grado di risolvere i rispettivi nomi reciprocamente, come descritto in [“Riepilogo dei requisiti per la configurazione di rete”](#), 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.
- 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 server vCenter.

Questo capitolo include i seguenti argomenti:

- [“Installazione e configurazione del software vCloud Director in un membro di un gruppo di server”](#), pag. 26
- [“Configurazione delle connessioni di rete e di database”](#), pag. 28
- [“Avvio o arresto dei servizi di vCloud Director”](#), pag. 31
- [“Installazione del software vCloud Director in altri server”](#), pag. 32
- [“Creazione di un pacchetto di distribuzione Microsoft Sysprep”](#), pag. 33
- [“Disinstallazione del software vCloud Director”](#), pag. 34

Installazione e configurazione 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 e vi installa il software vCloud Director.

Il software vCloud Director viene distribuito come file eseguibile Linux denominato `vmware-vccloud-director-1.5.0-nnnnnn.bin`, dove *nnnnnn* rappresenta un numero di build. 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.

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”](#), pag. 13.
- Assicurarsi di disporre delle credenziali di utente con privilegi avanzati per il server di destinazione
- Se si desidera creare un gruppo di server vCloud Director che includa più server, verificare che su ogni server sia montato lo storage del servizio di trasferimento condiviso nel percorso `$VCLLOUD_HOME/data/transfer`.
- Se si desidera che il programma di installazione verifichi la firma digitale del file di installazione, scaricare e installare la chiave pubblica VMware nel server di destinazione. Se la firma digitale del file di installazione è stata già verificata, non è necessario verificarla di nuovo durante l'installazione. Vedere [“Download e installazione della chiave pubblica VMware”](#), pag. 23.

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 con il formato seguente convalida il checksum per *file-di-installazione* utilizzando il *valore-checksum* MD5 copiato dalla pagina di download.

```
md5sum -c checksum-value installation-file
```

- 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 riportato di seguito, dove *file-di-installazione* è il percorso completo del file di installazione di vCloud Director.

```
chmod u+x file-di-installazione
```

- 5 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.

Il programma di installazione verifica che l'host soddisfi tutti i requisiti, verifica la firma digitale nel file di installazione, apre il pacchetto RPM di vCloud Director e installa il software. 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
```

Al termine dell'installazione del software, il programma di installazione richiede di eseguire lo script di configurazione per configurare le connessioni di rete e al database del server.

- 6 Stabilire quando eseguire tale script.

Opzione	Descrizione
Run the configuration script now	Digitare y e premere Invio.
Run the configuration script later	Digitare n e premere Invio per chiudere la shell.

Per ulteriori informazioni sull'esecuzione dello script di configurazione, vedere [“Configurazione delle connessioni di rete e di database”](#), pag. 28.

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 dei dettagli relativi alle connessioni di rete e di database.

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 eseguirlo in un secondo momento. Per eseguire lo script come operazione separata al termine dell'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.

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 in cui è 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 per poter supportare due connessioni SSL differenti: uno per il servizio HTTP e un altro 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 in altri server”](#), pag. 32.

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. 45.

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.

Copiare il file in una posizione accessibile dai server che verranno configurati. Il file deve essere di proprietà di **vcld** e il proprietario deve disporre di autorizzazioni di lettura e di scrittura, come illustrato nell'esempio. In caso contrario, lo script di configurazione non potrà utilizzarlo.

```
% ls -l responses.properties
-rw----- 1 vcloud vcloud 418 Jun 8 13:42
responses.properties
```

Passi successivi

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

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 i servizi di vCloud Director vengono arrestati durante un aggiornamento del software vCloud Director, è necessario scaricare e utilizzare lo strumento di gestione delle celle. Tale strumento consente di disattivare la cella prima di arrestare i servizi. Vedere [“Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server”](#), pag. 36.

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. <code>service vmware-vcd start</code>
Arrestare i servizi mentre la cella è in uso	Utilizzare lo strumento di gestione delle celle. Vedere “Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server” , pag. 36
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. <code>service vmware-vcd stop</code>

Installazione del software vCloud Director in altri server

È possibile aggiungere server a un gruppo di server vCloud Director in qualsiasi momento. Tutti i server di un gruppo di server devono essere configurati con gli stessi dettagli di connessione al database. Per assicurarsi che questo requisito venga soddisfatto, utilizzare il file di risposta creato in seguito all'installazione del primo server per fornire tali informazioni durante l'installazione degli altri server.

Prerequisiti

Una copia del file di risposta creato durante l'installazione del primo server nell'installazione corrente deve essere accessibile da tutti gli altri server aggiunti al gruppo. Vedere [“Protezione e riutilizzo del file di risposta”](#), pag. 31.

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 riportato di seguito, dove *file-di-installazione* è il percorso completo del file di installazione di vCloud Director.

```
chmod u+x file-di-installazione
```

- 4 Eseguire il file di installazione, specificando il percorso del file di risposta.

Specificare l'opzione `-r` nella riga di comando per l'installazione e immettere il percorso completo del file di risposta come argomento di tale opzione.

```
file-di-installazione -r percorso-file-di-risposta
```


5 (Facoltativo) Ripetere questa procedura per tutti gli altri server da aggiungere all'installazione.

Il programma di installazione richiede informazioni sulla connessione di rete e imposta le connessioni di rete e al database utilizzando le risposte fornite dal file di risposta.

Passi successivi

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. 45.

Creazione di un pacchetto di distribuzione Microsoft Sysprep

Per consentire l'esecuzione in vCloud Director della personalizzazione guest sulle macchine virtuali con determinati sistemi operativi guest Windows, è necessario creare un pacchetto di distribuzione Microsoft Sysprep in ogni cella Cloud presente nella propria installazione.

Durante l'installazione, vCloud Director inserisce alcuni file nella cartella `sysprep` dell'host del server vCloud Director. Non sovrascrivere tali file durante la creazione del pacchetto Sysprep.

Prerequisiti

Accedere ai file binari Sysprep per Windows 2000, Windows 2003 (a 32 e 64 bit) e Windows XP (a 32 e 64 bit).

Procedura

- 1 Copiare i file binari Sysprep di ogni sistema operativo in una posizione comoda su un host del server vCloud Director.

Ogni sistema operativo richiede la propria cartella.

NOTA: Per i nomi delle cartelle viene applicata la distinzione tra maiuscole e minuscole.

Sistema operativo guest	Destinazione di copia
Windows 2000	<code>SysprepBinariesDirectory /win2000</code>
Windows 2003 (a 32 bit)	<code>SysprepBinariesDirectory /win2k3</code>
Windows 2003 (a 64 bit)	<code>SysprepBinariesDirectory /win2k3_64</code>
Windows XP (a 32 bit)	<code>SysprepBinariesDirectory /winxp</code>
Windows XP (a 64 bit)	<code>SysprepBinariesDirectory /winxp_64</code>

`SysprepBinariesDirectory` rappresenta la posizione scelta dall'utente per la copia dei file binari.

- 2 Eseguire il comando `/opt/vmware/cloud-director/deploymentPackageCreator/createSysprepPackage.sh SysprepBinariesDirectory`.

Ad esempio, `/opt/vmware/cloud-director/deploymentPackageCreator/createSysprepPackage.sh /root/MySysprepFiles`.

- 3 Utilizzare il comando `service vmware-vcd restart` per riavviare la cella Cloud.
- 4 Se si dispone di più celle Cloud, copiare i file del pacchetto e delle proprietà in tutte le celle Cloud.

```
scp /opt/vmware/cloud-director/guestcustomization/vcloud_sysprep.properties
/opt/vmware/cloud-director/guestcustomization/windows_deployment_package_sysprep.cab
root@IP_cella_successiva:/opt/vmware/cloud-director/guestcustomization
```

- 5 Riavviare tutte le celle Cloud in cui vengono copiati i file.

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.

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 chiuderlo per l'aggiornamento.

L'aggiornamento consente di proteggere gli elementi seguenti:

- 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.
- I caricamenti in corso dei pacchetti OVF e delle immagini dei media vengono sospesi prima dell'inizio dell'aggiornamento e ripristinati al termine di quest'ultimo.

Se il cloud utilizza un servizio di bilanciamento del carico, è possibile eseguire l'aggiornamento di un sottoinsieme del gruppo di server, mantenendo disponibili i servizi esistenti sugli altri server. Se non si dispone di tale servizio, è necessario un tempo di inattività di vCloud Director sufficiente per eseguire l'aggiornamento del database e almeno di un server.

Aggiornamento di un gruppo di server vCloud Director

- 1 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. 36.
- 2 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. 39. 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 del gruppo prima di aver eseguito l'aggiornamento del database vCloud Director.
- 3 Eseguire l'aggiornamento del database vCloud Director. Vedere [“Esecuzione dell'aggiornamento del database vCloud Director”](#), pag. 41.
- 4 Riavviare vCloud Director sui server sottoposti ad aggiornamento. Vedere [“Avvio o arresto dei servizi di vCloud Director”](#), pag. 31.

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.

- 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. Vedere [“Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server”](#), pag. 36.
- 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. 39.
- 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. 41.
- 6 Riavviare vCloud Director sui server sottoposti ad aggiornamento. Vedere [“Avvio o arresto dei servizi di vCloud Director”](#), pag. 31.
- 7 Utilizzare lo strumento di bilanciamento del carico per reindirizzare le richieste di vCloud Director ai server sottoposti ad aggiornamento.
- 8 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. 39.

Questo capitolo include i seguenti argomenti:

- [“Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server”](#), pag. 36
- [“Esecuzione dell'aggiornamento del software vCloud Director in un membro di un gruppo di server”](#), pag. 39
- [“Esecuzione dell'aggiornamento del database vCloud Director”](#), pag. 41
- [“Esecuzione dell'aggiornamento degli host vCenter e ESX/ESXi”](#), pag. 42
- [“Esecuzione dell'aggiornamento di vShield Manager”](#), pag. 43
- [“Ripristino di un aggiornamento”](#), pag. 43

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 [“Guida di riferimento allo strumento di gestione delle celle”](#), pag. 37. Se non vi sono task in esecuzione, è possibile utilizzare lo strumento di gestione delle celle per arrestare i servizi di vCloud Director.

Prerequisiti

- Per poter eseguire lo strumento in un server vCloud Director 1.0 o 1.0.1, è necessario scaricare lo strumento e installarlo. Vedere <http://kb.vmware.com/kb/1033575>.
- 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.

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.

La riga di 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 -p Pa55w0rd 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 -p Pa55w0rd 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 -p Pa55w0rd cell --shutdown
```

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.

Guida di riferimento allo strumento di gestione delle celle

Grazie allo strumento di gestione delle celle è possibile sospendere lo scheduler dei task in modo che non sia possibile avviare nuovi task, controllare lo stato dei task attivi e chiudere la cella in modo normale.

Lo strumento di gestione delle celle viene installato in `/opt/vmware/vcloud-director/bin/cell-management-tool`. Rappresenta la modalità consigliata per arrestare i servizi in una cella.

Esecuzione del login e visualizzazione della Guida

Lo strumento di gestione delle celle richiede che l'utente esegua il login con le credenziali dell'amministratore di sistema di vCloud Director. Dopo aver eseguito il login allo strumento, è possibile utilizzarne i sottocomandi per gestire la cella.

Tavola 3-1. Opzioni e argomenti dello strumento di gestione delle celle, login e Guida

Opzione	Argomento	Descrizione
--help (-h)	Nessuno	Mostra un messaggio con la sintassi.
--username (-u)	Nome utente dell'amministratore di sistema di vCloud Director	È necessario disporre delle credenziali di amministratore di sistema per gestire lo scheduler dei task e visualizzare lo stato dei task.
--password (-p)	Password dell'amministratore di sistema di vCloud Director	Se si omette questo argomento, lo strumento richiede l'immissione della password.

Gestione di una cella

Per gestire una cella, utilizzare il sottocomando `cell`.

Tavola 3-2. Opzioni e argomenti dello strumento di gestione delle celle, sottocomando `cell`

Opzione	Argomento	Descrizione
--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 processi in esecuzione sulla cella e sullo stato della cella.

Esempio: Visualizzazione dello stato dei task

La riga di comando `cell-management-tool` seguente fornisce le credenziali dell'amministratore di sistema e restituisce il numero di processi 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 -p Pa55w0rd
cell --status
Job count = 3
Is Active = true
```

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-vccloud-director-1.5.0-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
- Se si desidera che il programma di installazione verifichi la firma digitale del file di installazione, scaricare e installare la chiave pubblica VMware nel server di destinazione. Se la firma digitale del file di installazione è stata già verificata, non è necessario verificarla di nuovo durante l'installazione. Vedere [“Download e installazione della chiave pubblica VMware”](#), pag. 23.
- Per disattivare e chiudere i servizi di vCloud Director nella cella del server, utilizzare lo strumento di gestione delle celle.

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 con il formato seguente convalida il checksum per *file-di-installazione* utilizzando il *valore-checksum* MD5 copiato dalla pagina di download.

```
md5sum -c checksum-value installation-file
```

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 riportato di seguito, dove *file-di-installazione* è il percorso completo del file di installazione di vCloud Director.

```
chmod u+x file-di-installazione
```

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. 36.

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. Would you like
to upgrade it to 1.5.0? The installer will stop the vmware-vcd service,
back up any configuration files from the previous release and migrate the
product configuration as necessary.
```

- 7 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.

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

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
```

- 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 <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> .
Se le proprietà di registrazione sono state modificate	Unire il file <code>/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew</code> al file <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> 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. 31.

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.

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 nessun server vCloud Director stia utilizzando il database. Vedere [“Utilizzo dello strumento di gestione delle celle per disattivare e chiudere un server”](#), pag. 36

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
```

- 2 Rispondere al prompt di aggiornamento del database.

```
Welcome to the vCloud Director upgrade utility
```

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

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

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

Viene eseguito lo strumento di aggiornamento dei database che mostra messaggi sullo stato di avanzamento.

```
Examining database at URL: jdbc:oracle:thin:@10.26.50.54:1521/orcl
Applying 1 upgrade batches
Executing upgrade batch: 1.0 to 1.5
Executing SQL statements from file: cc-tool-uninstall-graceful.sql
.....
Executing SQL statements from file: Upgrade.sql []
.....
Executing SQL statements from file: Upgrade_Data.sql []
.....
Executing SQL statements from file: NewInstall_Indexes.sql []
.....
```

```

Executing SQL statements from file: Upgrade_UUID.sql []
.....
Executing SQL statements from file: NewInstall_Funcs.sql []
.....

Successfully applied upgrade batch: 1.0 to 1.5
Running 2 upgrade tasks
Successfully ran upgrade task
Successfully ran upgrade task
Applying 1 upgrade batches
Executing upgrade batch: 1.0 to 1.5 cleanup
Executing SQL statements from file: NewInstall_Funcs.sql []
.....
Executing SQL statements from file: Upgrade_UUID_Clean.sql []
.....
Executing SQL statements from file: Upgrade_Clean.sql []
.....

Successfully applied upgrade batch: 1.0 to 1.5 cleanup
Database upgrade complete
+++++
```

Esecuzione dell'aggiornamento degli host vCenter e ESX/ESXi

Dopo aver eseguito l'aggiornamento di vCloud Director e del relativo database, è possibile eseguire l'aggiornamento dei server vCenter e degli host ESX/ESXi collegati al cloud per abilitare nuove funzionalità di vCloud Director.

Questo aggiornamento è facoltativo ma diverse funzionalità di vCloud Director dipendono da esso. Per un elenco di funzionalità di vCloud Director che dipendono dalle nuove versioni di vCenter e di ESX/ESXi, vedere [“Requisiti hardware e software di vCloud Director”](#), pag. 9.

Procedura

- 1 Eseguire l'aggiornamento del server vCenter.
- 2 Eseguire l'aggiornamento di ogni host ESX/ESXi supportato da server vCenter aggiornato.
 - a Utilizzare vCenter per attivare la modalità di manutenzione dell'host e consentire a tutte le macchine virtuali su tale host di eseguire la migrazione a un altro host.
 - b Aggiornare l'host.
 - c Disattivare la modalità di manutenzione dell'host.

NOTA: 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.

Al termine dell'aggiornamento dell'host, vCloud Director rileva la nuova versione e aggiorna l'agente host.

Esecuzione dell'aggiornamento di vShield Manager

Dopo aver eseguito l'aggiornamento di vCloud Director e del relativo database, è possibile eseguire l'aggiornamento dei server vShield Manager collegati al cloud per abilitare nuove funzionalità di vCloud Director.

IMPORTANTE: Non è possibile eseguire una nuova installazione di vShield Manager con una versione esistente di vCloud Director.

Dopo aver eseguito l'aggiornamento di un server vCenter collegato a vCloud Director, è possibile eseguire l'aggiornamento del server vShield Manager associato al server vCenter aggiornato. Sebbene questo aggiornamento sia facoltativo, diverse funzionalità di vCloud Director dipendono da esso. Per un elenco di funzionalità di vCloud Director che dipendono dalla nuova versione di vShield Manager, vedere [“Requisiti hardware e software di vCloud Director”](#), pag. 9.

L'aggiornamento di vShield Manager interrompe l'accesso alle funzioni amministrative di vShield Manager, ma non interrompe i servizi di rete. L'aggiornamento di un'appliance vShield Edge interrompe brevemente il servizio nelle reti da essa protette.

Prerequisiti

Prima di iniziare l'aggiornamento, è necessario che sia in esecuzione almeno una cella aggiornata nell'installazione di vCloud Director. La cella è responsabile della scrittura di dati sulla versione aggiornata di vShield Manager nel database vCloud Director.

Procedura

- 1 Eseguire l'aggiornamento di vShield Manager.

Seguire la procedura descritta nella *vShield Quick Start Guide*. Al termine dell'aggiornamento, vShield Manager notifica a vCloud Director la presenza di una nuova versione. L'invio di tale notifica e la relativa elaborazione in vCloud Director possono richiedere diversi minuti.

- 2 Eseguire l'aggiornamento di tutte le appliance vShield Edge gestite dalla versione aggiornata di vShield Manager.

Utilizzare l'interfaccia utente di vShield Manager per gestire tale aggiornamento.

NOTA: Se si utilizza la console Web di vCloud Director o l'API REST per reimpostare una rete protetta da vShield Edge, l'aggiornamento viene eseguito automaticamente. L'utilizzo dell'interfaccia utente di vShield Manager per gestire vShield Edge offre un controllo amministrativo migliore sul processo di aggiornamento e sul periodo di inattività della rete correlato.

Ripristino di un aggiornamento

Per annullare un aggiornamento e ripristinare una versione precedente dei servizi di vCloud Director, è necessario arrestare vCloud Director, ripristinare il database vCloud Director dai supporti di backup, disinstallare vCloud Director in tutti i membri del gruppo di server e installare la versione precedente di vCloud Director.

Procedura

- 1 Arrestare i servizi di vCloud Director su tutti i server di cui eseguire il downgrade.
- 2 Ripristinare il database vCloud Director appropriato utilizzando gli strumenti dei fornitori di database.
- 3 Disinstallare vCloud Director da tutti i server di cui eseguire il downgrade.
- 4 Installare la versione di vCloud Director corrispondente al database vCloud Director ripristinato.

Installazione di vCloud Director

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.
- 2 Seguire i prompt per completare l'installazione.

Questo capitolo include i seguenti argomenti:

- [“Controllo della licenza per utente finale”](#), pag. 46
- [“Immissione del codice di licenza”](#), pag. 46
- [“Creazione dell'account di amministratore di sistema”](#), pag. 46
- [“Specifiche delle impostazioni di sistema”](#), pag. 47
- [“Login a vCloud Director”](#), pag. 47

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 Si, 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.

Durante il processo di configurazione viene creata una cartella in vCenter 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 di 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 disporre di accesso a vCenter e a vShield Manager. La console Web di vCloud Director richiede l'accesso alle installazioni di vCenter e di vShield Manager che si desidera configurare insieme a vCloud Director. Per poter completare questo task, è necessario che tali installazioni siano in esecuzione e configurate per interagire tra loro. Per ulteriori informazioni, 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

Eeguire il login 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.

Indice

A

account di amministratore di sistema,
creazione **46**

aggiornamento

annullamento **43**

database **41**

del primo server **39**

flussi di lavoro **35**

archivio chiavi **18**

B

broker AMQP, installazione e configurazione **23**

browser, supportati **12**

C

certificato

autofirmato **21**

firmato **19**

configurazione, conferma delle impostazioni e
completamento **47**

D

database

dettagli connessione **28**

esecuzione dell'aggiornamento **41**

informazioni su **15**

Oracle **15**

piattaforme supportate **9**

SQL Server **17**

E

ESX/ESXi, esecuzione dell'aggiornamento **42**

F

file RPM, verifica della firma digitale **23**

firewall, porte e protocolli **14**

I

ID installazione, specifica **47**

installazione

configurazione **45**

creazione **25**

del primo server **26**

di altri server **32**

diagramma dell'architettura **7**

disinstallazione **34**

e pianificazione della capacità **8**

panoramica **7**

J

Java, versione JRE richiesta **12**

L

licenza per utente finale **46**

M

Microsoft Sysprep **33**

N

Nome sistema, specifica **47**

numero di serie di prodotto

immissione **46**

richiesta **46**

P

personalizzazione guest, preparazione **33**

R

rete

requisiti di configurazione **13**

sicurezza **14**

S

servizi, avvio **31**

strumento di gestione delle celle, opzioni **37**

V

vCenter

esecuzione dell'aggiornamento **42**

release supportate **9**

vShield Manager

esecuzione dell'aggiornamento **43**

installazione e configurazione **22**

release supportate **9**

