vCloud Director Installation and Upgrade Guide

vCloud Director 5.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000749-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

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

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2010–2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contents

VMware vCloud Director Installation and Upgrade Guide

The *VMware vCloud Director Installation and Upgrade Guide* provides information about installing or upgrading VMware vCloud Director software and configuring it to work with VMware vCenter™ to provide VMware-ready VMware vCloud® services.

Intended Audience

The *VMware vCloud Director Installation and Upgrade Guide* is intended for anyone who wants to install or upgrade VMware vCloud Director software. The information in this book is written for experienced system administrators who are familiar with Linux, Windows, IP networks, and VMware vSphere®.

Overview of vCloud Director Installation, Configuration, and Upgrade

1

A VMware vCloud® combines a vCloud Director server group with the vSphere platform. You create a vCloud Director server group by installing vCloud Director software on one or more servers, connecting the servers to a shared database, and integrating the vCloud Director server group with vSphere.

The initial configuration of vCloud Director, including database and network connection details, is established during installation. When you upgrade an existing installation to a new version of vCloud Director, you update the vCloud Director software and database schema, leaving the existing relationships between servers, the database, and vSphere in place.

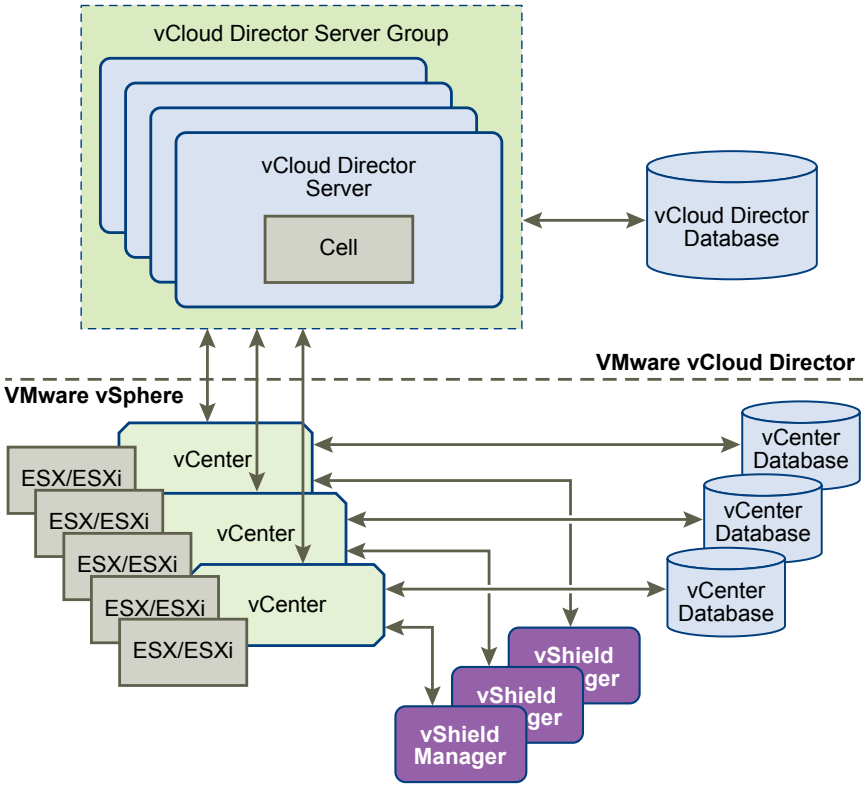
This chapter includes the following topics:

vCloud Director Architecture

A vCloud Director server group consists of one or more vCloud Director servers. These servers share a common database, and are linked to an arbitrary number of vCenter servers and ESX/ESXi hosts. vShield Manager servers provide network services to vCenter and vCloud Director.

A typical installation creates a vCloud Director server group comprising several servers. Each server in the group runs a collection of services called a vCloud Director cell. All members of the group share a single database. Each cell in the group connects to multiple vCenter servers, the ESX/ESXi hosts that they manage, and the vShield Manager servers that have been configured to support the vCenter servers.

Figure 1-1. vCloud Director Architecture Diagram



The vCloud Director installation and configuration process creates the cells, connects them to the shared database, and establishes the first connections to a vCenter server, vShield Manager, and ESX/ESXi hosts. A system administrator can then use the vCloud Director Web console to connect additional vCenter servers, vShield Manager servers, and ESX/ESXi servers to the vCloud Director server group at any time.

Configuration Planning

vSphere provides storage, compute, and networking capacity to vCloud Director. Before you begin installation, consider how much vSphere and vCloud Director capacity you need, and plan a configuration that can support it.

Configuration requirements depend on many factors, including the number of organizations in the cloud, the number of users in each organization, and the activity level of those users. The following guidelines can serve as a starting point for most configurations:

- Allocate one vCloud Director server (cell) for each vCenter server that you want to make accessible in your cloud.
- Be sure that all vCloud Director servers meet at least the minimum requirements for memory, CPU, and storage detailed in "vCloud Director Hardware and Software Requirements," on page 9.
- Configure the vCloud Director database as described in "Installing and Configuring a vCloud Director Database," on page 14.

vCloud Director Hardware and Software Requirements

Each server in a vCloud Director server group must meet certain hardware and software requirements. In addition, a supported database must be accessible to all members of the group. Each server group requires access to a vCenter server, a vShield Manager server, and one or more ESX/ESXi hosts.

Supported vCenter Server, ESX/ESXi, and vShield Manager Versions

Current information about supported vCenter Server, ESX/ESXi, and vShield Manager versions is available from the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

vSphere Configuration Requirements

vCenter servers and ESX/ESXi hosts intended for use with vCloud Director must meet specific configuration requirements.

- vCenter networks intended for use as vCloud Director external networks or network pools must be available to all hosts in any cluster intended for vCloud Director to use. Making these networks available to all hosts in a datacenter simplifies the task of adding new vCenter servers to vCloud Director.
- vSphere Distributed Switches must be used for cross-host fencing and network pool allocation.
- vCenter clusters used with vCloud Director must be configured to use automated DRS. Automated DRS requires shared storage attached to all hosts in a DRS cluster.
- vCenter servers must trust their ESX/ESXi hosts. All hosts in all clusters managed by vCloud Director must be configured to require verified host certificates. In particular, you must determine, compare, and select matching thumbprints for all hosts. See Configure SSL Settings in the *vCenter Server and Host Management* documentation.

vSphere Licensing Requirements

vCloud Director requires the following vSphere licenses:

- VMware DRS, licensed by vSphere Enterprise and Enterprise Plus.
- VMware Distributed Switch and dvFilter, licensed by vSphere Enterprise Plus. This license enables creation and use of vCloud Director isolated networks.

Supported vCloud Director Server Operating Systems

Table 1-1. Supported vCloud Director Server Operating Systems

Operating System
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
Red Hat Enterprise Linux 5 (64 bit), Update 8

Table 1-1. Supported vCloud Director Server Operating Systems (Continued)

Operating System
Red Hat Enterprise Linux 6 (64 bit), Update 1
Red Hat Enterprise Linux 6 (64 bit), Update 2

Disk Space Requirements

Each vCloud Director server requires approximately 950MB of free space for the installation and log files.

Memory Requirements

Each vCloud Director server must be provisioned with at least 1GB of memory. 2GB is recommended.

Linux Software Packages

Each vCloud Director server must include installations of several common Linux software packages. These packages are typically installed by default with the operating system software. If any are missing, the installer fails with a diagnostic message.

Table 1-2. Required Software Packages

Package Name	Package Name	Package Name
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	

Supported vCloud Director Databases

vCloud Director supports Oracle and Microsoft SQL Server databases. The most current information about supported databases is available from the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

For recommended database server configurations, see "Installing and Configuring a vCloud Director Database," on page 14.

Supported LDAP Servers

Table 1-3. Supported LDAP Servers

Platform	LDAP Server	Authentication Methods
Windows Server 2003	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Windows Server 2008	Active Directory	Simple
Windows 7 (2008 R2)	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Linux	OpenLDAP	Simple, Simple SSL

Guest OS Support

See the *vCloud Director User's Guide* for a list of supported guest operating systems.

Browsers That vCloud Director Supports

The vCloud Director Web Console is compatible with many versions of the Firefox and Internet Explorer Web browsers.

NOTE The vCloud Director Web Console is compatible only with 32-bit browsers. When a browser is listed as supported on a 64-bit platform, use of a 32-bit browser on the 64-bit platform is implied.

Browsers Supported on Microsoft Windows Platforms

Table 1-4. Browser Support and Operating System Compatibility on Microsoft Windows Platforms

Platform	Internet Explorer 7.*x*	Internet Explorer 8.*x*	Internet Explorer 9.*x*	Firefox 12.*x*, 13.*x*
Windows XP Pro 32-bit	YES	YES	No	YES
Windows XP Pro 64-bit	YES	YES	No	YES
Windows Server 2003 Enterprise Edition 32-bit	YES	YES	No	YES
Windows Server 2003 Enterprise Edition 64-bit	YES	YES	No	YES
Windows Server 2008	YES	YES	YES	YES
Windows Server 2008 R2	No	YES	YES	YES
Windows Vista 32-bit	YES	YES	YES	YES
Windows Vista 64-bit	YES	YES	YES	YES
Windows 7 32-bit	No	YES	YES	YES
Windows 7 64-bit	No	YES	YES	YES

Browsers Supported on Linux Platforms

Table 1-5. Browser Support and Operating System Compatibility on Linux Platforms

Platform	Firefox 11.*x*
Red Hat Enterprise Linux 5 (32 bit), Update 6	YES
Red Hat Enterprise Linux 6 (32 bit)	YES
Red Hat Enterprise Linux 6 (64 bit)	YES
SLES 11 32-bit	YES
Ubuntu 10.10 32-bit	YES
Ubuntu 10.10 64-bit	YES

Supported Versions of Adobe Flash Player

The vCloud Director Web Console requires Adobe Flash Player version 10.2 or later. Only the 32-bit version is supported.

Supported Versions of Java

vCloud Director clients must have JRE 1.6.0 update 10 or later installed and enabled. Only the 32-bit version is supported.

Supported TLS and SSL Protocol Versions and Cipher Suites

vCloud Director requires clients to use SSL. Supported versions include SSL 3.0 and TLS 1.0. Supported cipher suites include those with RSA, DSS, or Elliptic Curve signatures and DES3, AES-128, or AES-256 ciphers.

Summary of Network Configuration Requirements

Secure, reliable operation of vCloud Director depends on a secure, reliable network that supports forward and reverse lookup of hostnames, a network time service, and other services. Your network must meet these requirements before you begin installing vCloud Director.

The network that connects vCloud Director servers, the database server, vCenter servers, and vShield Manager servers, must meet several requirements:

IP addresses

Each vCloud Director server requires two IP addresses, so that it can support two different SSL connections. One connection is for the HTTP service. The other is for the console proxy service. You can use IP aliases or multiple network interfaces to create these addresses. You cannot use the Linux `ip addr add` command to create the second address .

Console Proxy Address

The IP address configured as the console proxy address must not be located behind an SSL-terminating load balancer or reverse proxy. All console proxy requests must be relayed directly to the console proxy IP address.

Network Time Service

You must use a network time service such as NTP to synchronize the clocks of all vCloud Director servers, including the database server. The maximum allowable drift between the clocks of synchronized servers is 2 seconds.

Server Time Zones

All vCloud Director servers, including the database server, must be configured to be in the same timezone.

Hostname Resolution

All host names that you specify during vCloud Director and vShield Manager installation and configuration must be resolvable by DNS using forward and reverse lookup of the fully qualified domain name or the unqualified hostname. For example, for a host named `mycloud.example.com`, both of the following commands must succeed on a vCloud Director host:

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

In addition, if the host `mycloud.example.com` has the IP address 192.168.1.1, the following command must return `mycloud.example.com`:

```
nslookup 192.168.1.1
```

Transfer Server Storage

To provide temporary storage for uploads and downloads, an NFS or other shared storage volume must be accessible to all servers in a vCloud Director cluster. This volume must have write permission for root. Each host must mount this volume at `$VCLOUD_HOME/data/transfer`, typically `/opt/vmware/vcloud-director/data/transfer`. Uploads and downloads occupy this storage for a few hours to a day. Transferred images can be large, so allocate at least several hundred gigabytes to this volume.

Network Security Recommendations

Secure operation of vCloud Director requires a secure network environment. Configure and test this network environment before you begin installing vCloud Director

Connect all vCloud Director servers to a network that is secured and monitored. vCloud Director network connections have several additional requirements:

- Do not connect vCloud Director directly to the public Internet. Always protect vCloud Director network connections with a firewall. Only port 443 (HTTPS) must be open to incoming connections. Ports 22 (SSH) and 80 (HTTP) can also be opened for incoming connections if needed. All other incoming traffic from a public network must be rejected by the firewall.

  Table 1-6. Ports That Must Allow Incoming Packets From vCloud Director Hosts

Port	Protocol	Comments
111	TCP, UDP	NFS portmapper used by transfer service
920	TCP, UDP	NFS rpc.statd used by transfer service
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

  Do not connect the ports used for outgoing connections to the public network.

  Table 1-7. Ports That Must Allow Outgoing Packets From vCloud Director Hosts

Port	Protocol	Comments
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	NFS portmapper used by transfer service
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	vCenter, vShield Manager, and ESX connections
514	UDP	Optional. Enables syslog use
902	TCP	vCenter and ESX connections
903	TCP	vCenter and ESX connections
920	TCP, UDP	NFS rpc.statd used by transfer service
1433	TCP	Default Microsoft SQL Server database port
1521	TCP	Default Oracle database port
5672	TCP, UDP	Optional. AMQP messages for task extensions
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

- Do not connect physical host computers to physical networks that are uplinks for the vNetwork distributed switches that back vCloud Director network pools.
- Route traffic between vCloud Director servers and the vCloud Director database server over a dedicated private network if possible.
- Virtual switches and distributed virtual switches that support provider networks must be isolated from each other. They cannot share the same level 2 physical network segment.

Installing and Configuring a vCloud Director Database

vCloud Director cells use a database to store shared information. This database must exist before you can complete installation and configuration of vCloud Director software.

NOTE Regardless of the database software you choose, you must create a separate, dedicated database schema for vCloud Director to use. vCloud Director cannot share a database schema with any other VMware product.

Configure an Oracle Database

Oracle databases have specific configuration requirements when you use them with vCloud Director. Install and configure a database instance and create the vCloud Director database user account the before you install vCloud Director.

Procedure

1 Configure the database server.

A database server configured with 16GB of memory, 100GB storage, and 4 CPUs should be adequate for most vCloud Director clusters.

2 Create the database instance.

Use commands of the following form to create separate data (CLOUD_DATA) and index (CLOUD_INDX) tablespaces:

```
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 Create the vCloud Director database user account.

The following command creates database user name `vcloud` with password `vcloudpass`.

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

NOTE When you create the vCloud Director database user account, you must specify CLOUD_DATA as the default tablespace.

4 Configure database connection, process, and transaction parameters.

The database must be configured to allow at least 75 connections per vCloud Director cell plus about 50 for Oracle's own use. You can obtain values for other configuration parameters based on the number of connections, where *C* represents the number of cells in your vCloud Director cluster.

Oracle Configuration Parameter	Value for *C* Cells
CONNECTIONS	75**C*+50
PROCESSES	= CONNECTIONS
SESSIONS	= PROCESSES*1.1+5
TRANSACTIONS	= SESSIONS*1.1
OPEN_CURSORS	= SESSIONS

5 Create the vCloud Director database user account.

Do not use the Oracle system account as the vCloud Director database user account. You must create a dedicated user account for this purpose. Grant the following system privileges to the account:

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

6 Note the database service name so you can use it when you configure network and database connections.

To find the database service name, open the file `$ORACLE_HOME/network/admin/tsnames.ora` on the database server and look for an entry of the following form:

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

Configure a Microsoft SQL Server Database

SQL Server databases have specific configuration requirements when you use them with vCloud Director. Install and configure a database instance, and create the vCloud Director database user account before you install vCloud Director.

vCloud Director database performance is an important factor in overall vCloud Director performance and scalability. vCloud Director uses the SQL Server `tmpdb` file when storing large result sets, sorting data, and managing data that is being concurrently read and modified. This file can grow significantly when vCloud Director is experiencing heavy concurrent load. It is a good practice to create the `tmpdb` file on a dedicated volume that has fast read and write performance. For more information about the `tmpdb` file and SQL Server performance, see http://msdn.microsoft.com/en-us/library/ms175527.aspx.

Prerequisites

- You must be familiar with Microsoft SQL Server commands, scripting, and operation.
- To configure Microsoft SQL Server, log on to the SQL Server host computer using administrator credentials. You can configure SQL server to run with the LOCAL_SYSTEM identity, or any identity with the privilege to run a Windows service.

Procedure

1 Configure the database server.

A database server configured with 16GB of memory, 100GB storage, and 4 CPUs should be adequate for most vCloud Director clusters.

2 Specify Mixed Mode authentication during SQL Server setup.

Windows Authentication is not supported when using SQL Server with vCloud Director.

3 Create the database instance.

The following script creates the database and log files, specifying the proper collation sequence.

```
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
```

The values shown for SIZE are suggestions. You might need to use larger values.

4 Set the transaction isolation level.

The following script sets the database isolation level to 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
```

For more about transaction isolation, see http://msdn.microsoft.com/en-us/library/ms173763.aspx.

5 Create the vCloud Director database user account.

The following script creates database user name `vcloud` with 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 Assign permissions to the vCloud Director database user account.

The following script assigns the `db_owner` role to the database user created in Step 5.

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

Create SSL Certificates

vCloud Director requires SSL to secure communications between clients and servers. Before you install and configure a vCloud Director server group, you must create two certificates for each member of the group and import the certificates into host keystores.

Each vCloud Director server that you intend to use in a vCloud Director cluster requires two SSL certificates, one for each of its IP addresses.

NOTE All directories in the pathname to the SSL certificates must be readable by the user `vcloud.vcloud`. This user is created by the vCloud Director installer.

Procedure

1 List the IP addresses for this server.

Use a command like `ifconfig` to discover this server's IP addresses.

2 For each IP address, run the following command to retrieve the fully qualified domain name to which the IP address is bound.

`nslookup` *`ip-address`*

3 Make a note of each IP address, the fully qualified domain name associated with it, and whether vCloud Director should use the address for the HTTP service or the console proxy service.

You need the fully qualified domain names when you create the certificates, and the IP addresses when you configure network and database connections.

4 Create the certificates.

You can use certificates signed by a trusted certification authority, or self-signed certificates. Signed certificates provide the highest level of trust. A 2,048-bit key length provides a high level of security.

Create and Import a Signed SSL Certificate

Signed certificates provide the highest level of trust for SSL communications.

Each vCloud Director server requires two SSL certificates, one for each of its IP addresses, in a Java keystore file. You must create two SSL certificates for each server that you intend to use in your vCloud Director server group. You can use certificates signed by a trusted certification authority, or self-signed certificates. Signed certificates provide the highest level of trust.

To create and import self-signed certificates, see "Create a Self-Signed SSL Certificate," on page 19.

Prerequisites

- Generate a list of fully-qualified domain names and their associated IP addresses on this server, along with a service choice for each IP address. See "Create SSL Certificates," on page 16.
- Verify that you have access to a computer that has a Java version 6 runtime environment, so that you can use the `keytool` command to create the certificate. The vCloud Director installer places a copy of `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`, but you can perform this procedure on any computer that has a Java version 6 runtime environment installed. Certificates created with a `keytool` from any other source are not supported for use with vCloud Director. Creating and importing the certificates before you install and configure vCloud Director software simplifies the installation and configuration process. These command-line examples assume that `keytool` is in the user's path. The keystore password is represented in these examples as *passwd*.

Procedure

1 Create an untrusted certificate for the HTTP service.

This command creates an untrusted certificate in a keystore file named `certificates.ks`.

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

The certificate is valid for 90 days.

2 Answer the `keytool` questions.

When `keytool` asks for your first and last name, type the fully qualified domain name associated with the IP address you want to use for the HTTP service.

3 For the remaining questions, provide answers appropriate for your organization and location, as shown in this example.

```
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 Create a certificate signing request for the HTTP service.

This command creates a certificate signing request in the file `http.csr`.

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

5 Create an untrusted certificate for the console proxy service.

This command adds an untrusted certificate to the keystore file created in Step 1.

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

The certificate is valid for 90 days.

6 When `keytool` asks for your first and last name, type the fully-qualified domain name associated with the IP address you want to use for the console proxy service.

7 For the remaining questions, provide answers appropriate for your organization and location, as shown in the example in Step 3.

8 Create a certificate signing request for the console proxy service.

This command creates a certificate signing request in the file `consoleproxy.csr`.

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

9 Send the certificate signing requests to your Certification Authority.

If your certification authority requires you to specify a Web server type, use Jakarta Tomcat.

10 When you receive the signed certificates, import them into the keystore file.

a Import the Certification Authority's root certificate into the keystore file.

This command imports the root certificate from the `root.cer` file to the `certificates.ks` keystore file.

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

b (Optional) If you received intermediate certificates, import them into the keystore file.

This command imports intermediate certificates from the `intermediate.cer` file to the `certificates.ks` keystore file.

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

c Import the certificate for the HTTP service.

This command imports the certificate from the `http.cer` file to the `certificates.ks` keystore file.

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

d Import the certificate for the console proxy service.

This command imports the certificate from the `consoleproxy.cer` file to the `certificates.ks` keystore file.

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

11 To verify that all the certificates are imported, list the contents of the keystore file.

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

12 Repeat steps Step 1 through Step 11 on each of the remaining vCloud Director servers.

What to do next

If you created the `certificates.ks` keystore file on a computer other than the server on which you generated the list of fully qualified domain names and their associated IP addresses, copy the keystore file to that server now. You will need the keystore path name when you run the configuration script. See "Configure Network and Database Connections," on page 25.

NOTE Because the vCloud Director configuration script does not run with a privileged identity, the keystore file and the directory in which it is stored must be readable by any user.

Create a Self-Signed SSL Certificate

Self-signed certificates can provide a convenient way to configure SSL for vCloud Director in environments where trust concerns are minimal.

Each vCloud Director server requires two SSL certificates, one for each of its IP addresses, in a Java keystore file. You must create two SSL certificates for each server that you intend to use in your vCloud Director server group. You can use certificates signed by a trusted certification authority, or self-signed certificates. Signed certificates provide the highest level of trust.

To create and import signed certificates, see "Create and Import a Signed SSL Certificate," on page 17.

Prerequisites

- Generate a list of fully-qualified domain names and their associated IP addresses on this server, along with a service choice for each IP address. See "Create SSL Certificates," on page 16.
- Verify that you have access to a computer that has a Java version 6 runtime environment, so that you can use the `keytool` command to create the certificate. The vCloud Director installer places a copy of `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`, but you can perform this procedure on any computer that has a Java version 6 runtime environment installed. Certificates created with a `keytool` from any other source are not supported for use with vCloud Director. Creating and importing the certificates before you install and configure vCloud Director software simplifies the installation and configuration process. These command-line examples assume that `keytool` is in the user's path. The keystore password is represented in these examples as *passwd*.

Procedure

1 Create an untrusted certificate for the HTTP service.

This command creates an untrusted certificate in a keystore file named `certificates.ks`.

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

2 Create an untrusted certificate for the console proxy service.

This command adds an untrusted certificate to the keystore file created in Step 1.

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

The certificate is valid for 90 days.

3 To verify that all the certificates are imported, list the contents of the keystore file.

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

4 Repeat Step 1 through Step 3 on each of the remaining vCloud Director servers.

What to do next

If you created the `certificates.ks` keystore file on a computer other than the server on which you generated the list of fully qualified domain names and their associated IP addresses, copy the keystore file to that server now. You will need the keystore path name when you run the configuration script. See "Configure Network and Database Connections," on page 25.

NOTE Because the vCloud Director configuration script does not run with a privileged identity, the keystore file and the directory in which it is stored must be readable by any user.

Installing and Configuring vShield Manager

vCloud Director depends on vShield Manager to provide network services to the cloud. Install and configure vShield Manager before you begin installing vCloud Director.

You must associate each vCenter Server that you add to vCloud Director with a unique instance of vShield Manager. For information about the network requirements and supported versions of vShield Manager, see "vCloud Director Hardware and Software Requirements," on page 9.

IMPORTANT This procedure applies only to new installations of vCloud Director. If you are upgrading an existing installation of vCloud Director, you can optionally upgrade its associated vShield Manager installation. A new release of vShield Manager cannot work with an existing release of vCloud Director. See "Upgrade vShield Manager," on page 46.

Procedure

1 Use the vSphere Client to log in to your vCenter Server.

2 Select **File > Deploy OVF Template**.

3 Browse to the location of the `vShield Manager.ovf` file and follow the prompts to deploy the OVF file.

4 After the OVF file is deployed, power on the vShield Manager virtual machine and open the console.

5 Log in to the console with the user name **`admin`** and password **`default.`**

6 At the `manager` prompt, type **`enable`**.

7 At the `Password` prompt, type **`default`** to enable setup mode.

When setup mode is enabled, the prompt string changes to `manager#`.

8 At the `manager#` prompt, type **`setup`** to begin the setup procedure.

9 Enter the IP address, subnet mask, and default gateway for the vShield Manager virtual machine.

You need this information to attach a vCenter Server to Cloud Director.

10 Type **`exit`** to log out.

11 Close the console and leave the virtual machine running.

It is not necessary to synchronize vShield Manager with vCenter or register the vShield Manager as a vSphere Client plug-in when you use vShield Manager with vCloud Director.

Installing and Configuring an AMQP Broker

AMQP, the Advanced Message Queuing Protocol, is an open standard for message queuing that supports flexible messaging for enterprise systems. vCloud Director includes an AMQP service that you can configure to work with an AMQP broker, such as RabbitMQ, to provide cloud operators with a stream of notifications about events in the cloud. If you want to use this service, you must install and configure an AMQP broker.

Procedure

1 Download the RabbitMQ Server from http://info.vmware.com/content/12834_rabbitmq.

2 Follow the RabbitMQ installation instructions to install RabbitMQ on any convenient host.

The RabbitMQ server host must be reachable on the network by each vCloud Director cell.

3 During the RabbitMQ installation, make a note of the values that you will need to supply when configuring vCloud Director to work with this RabbitMQ installation.

- The fully-qualified domain name of the RabbitMQ server host, for example `amqp.example.com`.
- A username and password that are valid for authenticating with RabbitMQ.
- The port at which the broker listens for messages. The default is `5672`.
- The RabbitMQ virtual host. The default is "/".

What to do next

By default, the vCloud Director AMQP service sends unencrypted messages. If you configure it to encrypt these messages using SSL, it verifies the broker's certificate by using the default JCEKS trust store of the Java runtime environment on the vCloud Director server. The Java runtime environment is typically located in the `$JRE_HOME/lib/security/cacerts` directory.

To use SSL with the vCloud Director AMQP service, select **Use SSL** on the AMQP Broker Settings section of the Extensibility page of the vCloud Director Web console, and provide either of the following:

- an SSL certificate pathname
- a JCEKS trust store pathname and password

If you do not need to validate the AMQP broker's certificate, you can select **Accept all certificates**.

Download and Install the VMware Public Key

The installation file is digitally signed. To verify the signature, you must download and install the VMware public key.

You can use the Linux `rpm` tool and the VMware public key to verify the digital signature of the vCloud Director installation file, or any other signed downloaded file from `vmware.com`. If you install the public key on the computer where you plan to install vCloud Director, the verification happens as part of the installation or upgrade. You can also manually verify the signature before you begin the installation or upgrade procedure, then use the verified file for all installations or upgrades.

NOTE The download site also publishes a checksum value for the download. The checksum is published in two common forms. Verifying the checksum verifies that the file contents that you downloaded are the same as the contents that were posted. It does not verify the digital signature.

Procedure

1 Obtain and import the VMware Packaging Public Keys.

   a Create a directory to store the VMware Packaging Public Keys.

   b Use a Web browser to download all of the VMware Public Packaging Public Keys from the http://packages.vmware.com/tools/keys directory.

   c Save the key files to the directory that you created.

   d For each key that you download, run the following command to import the key.

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

   key_path is the directory in which you saved the keys.

   key_name is the filename of a key.

2 (Optional) Use the Linux `rpm` tool to verify the digital signature of the downloaded file.

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

   After you verify the digital signature of the file, you can use it to install or upgrade vCloud Director on any server, without having to install the public key on that server. The installer warns you if no key is installed. You can ignore the warning if you already verified the signature of the file.

Creating a vCloud Director Server Group

2

A vCloud Director server group consists of one or more vCloud Director servers. Each server in the group runs a collection of services called a vCloud Director cell. To create a server group, you install vCloud Director software on each server, configure its network and database connections, and start its vCloud Director services.

Prerequisites for Creating a vCloud Director Server Group

Important This procedure is for new installations only. If you are upgrading an existing vCloud Director installation, see Chapter 3, "Upgrading vCloud Director," on page 33

Before you begin installing and configuring vCloud Director, complete all of the following tasks.

1. Verify that a supported vCenter server is running and properly configured for use with vCloud Director. For supported versions and configuration requirements, see "Supported vCenter Server, ESX/ESXi, and vShield Manager Versions," on page 9.
2. Verify that a supported vShield Manager server is running and properly configured for use with vCloud Director. For supported versions, see "Supported vCenter Server, ESX/ESXi, and vShield Manager Versions," on page 9. For installation and configuration details, see "Installing and Configuring vShield Manager," on page 20.
3. Verify that you have at least one supported vCloud Director server platform running and configured with an appropriate amount of memory and storage. For supported platforms and configuration requirements, see "Supported vCloud Director Server Operating Systems," on page 9.
   - Each member of a server group requires two IP addresses: one to support an SSL connection for the HTTP service and another for the console proxy service.
   - Each server must have an SSL certificate for each IP address. All directories in the pathname to the SSL certificates must be readable by the user `vcloud.vcloud`. This user is created by the vCloud Director installer. See "Create SSL Certificates," on page 16.
   - For the transfer service, each server must mount an NFS or other shared storage volume at `$VCLOUD_HOME/data/transfer`, typically `/opt/vmware/vcloud-director/data/transfer`. This volume must have write permission for root.
   - Each server should have access to a Microsoft Sysprep deployment package. See "Create a Microsoft Sysprep Deployment Package," on page 30.
4. Verify that you have created a vCloud Director database and that it is accessible to all servers in the group. For a list of supported database software, see "Supported vCloud Director Databases," on page 10.
   - Verify that you have created a database account for the vCloud Director database user and that the account has all required database privileges. See "Installing and Configuring a vCloud Director Database," on page 14.

- Verify that the database service starts when the database server is rebooted.

5 Verify that all vCloud Director servers, the database server, and all vCenter and vShield Manager servers can resolve each other's names as described in "Summary of Network Configuration Requirements," on page 12.

6 Verify that all vCloud Director servers and the database server are synchronized to a network time server with the tolerances noted in "Summary of Network Configuration Requirements," on page 12.

7 If you plan to import users or groups from an LDAP service, verify that the service is accessible to each vCloud Director server.

8 Open firewall ports as shown in "Network Security Recommendations," on page 13. Port 443 must be open between vCloud Director and vCenter servers.

This chapter includes the following topics:

Install and Configure vCloud Director Software on Any Member of a Server Group

The vCloud Director installer verifies that the target server meets all platform prerequisites and installs vCloud Director software on it.

vCloud Director software is distributed as a digitally signed Linux executable file named `vmware-vcloud-director-5.1.0-`*nnnnnn*`.bin`, where *nnnnnn* represents a build number. After the software is installed on the target server, you must run a script that configures the server's network and database connections.

Prerequisites

- Verify that the target server and the network it connects to meet the requirements specified in "Summary of Network Configuration Requirements," on page 12. The target server must not have an existing user or group named `vcloud`.
- Verify that you have superuser credentials for the target server.
- If you intend to create a vCloud Director server group that includes multiple servers, verify that the target server mounts the shared transfer service storage at `$VCLOUD_HOME/data/transfer`.
- If you want the installer to verify the digital signature of the installation file, download and install the VMware public key on the target server. If you have already verified the digital signature of the installation file, you do not need to verify it again during installation. See "Download and Install the VMware Public Key," on page 22.

Procedure

1 Log in to the target server as root.

2 Download the installation file to the target server.

If you purchased the software on a CD or other media, copy the installation file to a location that is accessible to all target servers.

3 Verify that the checksum of the download matches the one posted on the download page.

Values for both MD5 and SHA1 checksums are posted on the download page. Use the appropriate tool to verify that the checksum of the downloaded installation file matches the one shown on the download page. A Linux command of the following form validates the checksum for *installation-file* using the MD5 *checksum-value* copied from the download page.

```
md5sum –c checksum–value installation–file
```

4 Ensure that the installation file is executable.

The installation file requires execute permission. To be sure that it has this permission, open a console, shell, or terminal window and run the following Linux command, where *installation-file* is the full pathname to the vCloud Director installation file.

```
chmod u+x installation–file
```

5 In a console, shell, or terminal window, run the installation file.

To run the installation file, type its full pathname, for example `./installation–file`. The file includes an installation script and an embedded RPM package.

NOTE You cannot run the installation file from a directory whose pathname includes any embedded space characters.

The installer verifies that the host meets all requirements, verifies the digital signature on the installation file, unpacks the vCloud Director RPM package, and installs the software. The installer prints a warning of the following form if you have not installed the VMware public key on the target server.

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

After the software is installed, the installer prompts you to run the configuration script, which configures the server's network and database connections.

6 Decide when to run the configuration script.

Option	Description
Run the configuration script now	Type **y** and press Enter.
Run the configuration script later	Type **n** and press Enter to exit to the shell.

For more information about running the configuration script, see "Configure Network and Database Connections," on page 25.

Configure Network and Database Connections

After vCloud Director software is installed on the server, the installer prompts you to run a script that configures the server's network and database connections.

You must install vCloud Director software on the server before you can run the configuration script. The installer prompts you to run the script after installation is complete, but you can run it later. To run the script as a separate operation after the vCloud Director software is installed, log in as root, open a console, shell, or terminal window, and type:

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

The configuration script creates network and database connections for a single vCloud Director server. The script also creates a response file that preserves database connection information for use in subsequent server installations.

Prerequisites

- Verify that a database of a supported type is accessible from the vCloud Director server. See "Installing and Configuring a vCloud Director Database," on page 14 and "vCloud Director Hardware and Software Requirements," on page 9.
- Have the following information available:
  - Location and password of the keystore file that includes the SSL certificates for this server. See "Create and Import a Signed SSL Certificate," on page 17. The configuration script does not run with a privileged identity, so the keystore file and the directory in which it is stored must be readable by any user.
  - Password for each SSL certificate.
  - Hostname or IP address of the database server.
  - Database name and connection port.
  - Database user credentials (user name and password). This user must have specific database privileges. See "Installing and Configuring a vCloud Director Database," on page 14.

Procedure

1 Specify the IP addresses to use for the HTTP and console proxy services running on this host.

Each member of a server group requires two IP addresses, so that it can support two different SSL connections: one for the HTTP service an another for the console proxy service. To begin the configuration process, choose which of the IP addresses discovered by the script should be used for each service.

```
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 Specify the full path to the Java keystore file.

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

3 Type the keystore and certificate passwords.

```
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 Configure audit message handling options.

Services in each vCloud Director cell log audit messages to the vCloud Director database, where they are preserved for 90 days. To preserve audit messages longer, you can configure vCloud Director services to send audit messages to the `syslog` utility in addition to the vCloud Director database.

Option	Action
To log audit messages to both `syslog` and the vCloud Director database.	Type the `syslog` hostname or IP address.
To log audit messages only to the vCloud Director database	Press Enter.

```
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 Specify the port on which the `syslog` process monitors the specified server.

The default is port 514.

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

6 Specify the database type, or press Enter to accept the default value.

```
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 Specify database connection information.

The information that the script requires depends on your choice of database type. This example shows the prompts that follow specification of an Oracle database. Prompts for other database types are similar.

a Type the hostname or IP address of the database server.

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

b Type the database port, or press Enter to accept the default value.

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

c Type the database service name.

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

If you press Enter, the configuration script uses a default value, which might not be correct for some installations. For information about how to find the database service name for an Oracle database, see "Configure an Oracle Database," on page 14.

d Type the database user name and password.

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

The script validates the information you supplied, then continues with three more steps.

1 It initializes the database and connects this server to it.

2 It offers to start vCloud Director services on this host.

3 It displays a URL at which you can connect to the Setup wizard after vCloud Director service starts.

This fragment shows a typical completion of the 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...
```

What to do next

NOTE Database connection information and other reusable responses you supplied during configuration are preserved in a file located at `/opt/vmware/vcloud-director/etc/responses.properties` on this server. This file contains sensitive information that you must reuse when you add more servers to a server group. Preserve the file in a secure location, and make it available only when needed.

To add more servers to this group, see "Install vCloud Director Software on Additional Servers," on page 29.

After vCloud Director services are running on all servers, you can open the Setup wizard at the URL displayed when the script completes. See Chapter 4, "vCloud Director Setup," on page 51.

Protecting and Reusing the Response File

Network and database connection details that you supply when you configure the first vCloud Director server are saved in a response file. This file contains sensitive information that you must reuse when you add more servers to a server group. Preserve the file in a secure location, and make it available only when needed.

The response file is created at `/opt/vmware/vcloud-director/etc/responses.properties` on the first server for which you configure network and database connections. When you add more servers to the group, you must use a copy of the response file to supply configuration parameters that all servers share.

Procedure

1 Protect the response file.

Save a copy of the file in a secure location. Restrict access to it, and make sure it is backed up to a secure location. When you back up the file, avoid sending cleartext across a public network.

2 Reuse the response file.

Copy the file to a location accessible to the servers you are ready to configure. The file must be owned by **vcloud.vcloud** and have read and write permission for the owner, as shown in this example, or the configuration script cannot use it.

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

What to do next

After you configure the additional servers, delete the copy of the response file you used to configure them.

Start or Stop vCloud Director Services

After you complete installation and database connection setup on a server, you can start vCloud Director services on it. You can also stop these services if they are running.

The configuration script prompts you to start vCloud Director services. You can let the script start these services for you, or you can start the services yourself later. These services must be running before you can complete and initialize the installation.

vCloud Director services start whenever you reboot a server.

IMPORTANT If you are stopping vCloud Director services as part of a vCloud Director software upgrade, you must use the cell management tool, which allows you to quiesce the cell before stopping services. See "Use the Cell Management Tool to Quiesce and Shut Down a Server," on page 35.

Procedure

1 Log in to the target server as root.

2 Start or stop services.

Option	Action
Start services	Open a console, shell, or terminal window and run the following command. `service vmware–vcd start`
Stop services when the cell is in use	Use the cell management tool.
Stop services when the cell is not in use	Open a console, shell, or terminal window and run the following command. `service vmware–vcd stop`

Install vCloud Director Software on Additional Servers

You can add servers to a vCloud Director server group at any time. All servers in a server group must be configured with the same database connection details. To ensure that this requirement is met, use the response file that the first server installation creates to supply this information when you install additional servers.

Prerequisites

A copy of the response file created when you installed the first server in this installation must be accessible to any additional servers that you add to the group. See "Protecting and Reusing the Response File," on page 28.

Procedure

1 Log in to the target server as root.

2 Download the installation file to the target server.

   If you purchased the software on a CD or other media, copy the installation file to a location that is accessible to all target servers.

3 Ensure that the installation file is executable.

   The installation file requires execute permission. To be sure that it has this permission, open a console, shell, or terminal window and run the following Linux command, where *installation-file* is the full pathname to the vCloud Director installation file.

   ```
   chmod u+x installation-file
   ```

4 Run the installation file, supplying the pathname of the response file.

   Specify the `-r` option on the installation command line, and supply the full pathname to the response file as the argument to that option.

   ```
   installation-file -r path-to-response-file
   ```

5 (Optional) Repeat this procedure for any additional servers to add to this installation.

The installer requests network connection information and sets up network and database connections using the responses from the response file.

What to do next

After the configuration script finishes and vCloud Director services are running on all servers, you can open the Setup wizard at the URL that appears when the script completes. See Chapter 4, "vCloud Director Setup," on page 51.

Create a Microsoft Sysprep Deployment Package

Before vCloud Director can perform guest customization on virtual machines with certain Windows guest operating systems, you must create a Microsoft Sysprep deployment package on each cloud cell in your installation.

During installation, vCloud Director places some files in the `sysprep` folder on the vCloud Director server host. Do not overwrite these files when you create the Sysprep package.

Prerequisites

Access to the Sysprep binary files for Windows 2000, Windows 2003 (32- and 64-bit), and Windows XP (32- and 64-bit).

Procedure

1 Copy the Sysprep binary files for each operating system to a convenient location on a vCloud Director server host.

   Each operating system requires its own folder.

   NOTE Folder names are case-sensitive.

Guest OS	Copy Destination
Windows 2000	*SysprepBinariesDirectory* `/win2000`
Windows 2003 (32-bit)	*SysprepBinariesDirectory* `/win2k3`
Windows 2003 (64-bit)	*SysprepBinariesDirectory* `/win2k3_64`

Guest OS	Copy Destination
Windows XP (32-bit)	*SysprepBinariesDirectory* `/winxp`
Windows XP (64-bit)	*SysprepBinariesDirectory* `/winxp_64`

SysprepBinariesDirectory represents a location you choose to which to copy the binaries.

2 Run the `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh` *SysprepBinariesDirectory* command.

For example, `/opt/vmware/vcloud-director/deploymentPackageCreator/createSysprepPackage.sh /root/MySysprepFiles`.

3 Use the `service vmware-vcd restart` command to restart the cloud cell.

4 If you have multiple cloud cells, copy the package and properties file to all cloud cells.

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

5 Restart each cloud cell to which you copy the files.

Uninstall vCloud Director Software

Use the Linux `rpm` command to uninstall vCloud Director software from an individual server.

Procedure

1 Log in to the target server as root.

2 Unmount the transfer service storage, typically mounted at `/opt/vmware/vcloud-director/data/transfer`.

3 Open a console, shell, or terminal window and run the `rpm` command.

```
rpm –e vmware-vcloud-director
```

Upgrading vCloud Director 3

To upgrade vCloud Director to a new version, install the new version on each server in the vCloud Director server group, upgrade the vCloud Director database, and restart vCloud Director services. You must also upgrade the vSphere components that support vCloud Director, including vShield Manager, vCenter, and ESX/ESXi.

After you upgrade a vCloud Director server, you must also upgrade its vCloud Director database. The database stores information about the runtime state of the server, including the state of all vCloud Director tasks it is running. To ensure that no invalid task information remains in the database after an upgrade, you must ensure that no tasks are active on the server before you begin the upgrade.

IMPORTANT The upgrade process requires you to upgrade vCloud Director, vShield Manager, vCenter, and ESX/ESXi. You must prevent users from accessing vCloud Director until the vShield Manager upgrade step is complete.

The upgrade preserves the following artifacts:

- Local and global properties files are copied to the new installation.
- Microsoft sysprep files used for guest customization are copied to the new installation.

If your cloud uses a load balancer, you can upgrade a subset of the server group while keeping existing services available on the others. If you do not have a load balancer, the upgrade requires sufficient vCloud Director downtime to upgrade the database and at least one server. You might also have to upgrade registered vCenter servers if they are not running a compatible version of vCenter software. Upgrading vCenter servers or ESX/ESXi hosts can incur additional vCloud Director downtime, because virtual machines are inaccessible while their hosts or vCenter server are being upgraded.

Upgrading a vCloud Director Server Group

1. Disable user access to vCloud Director. If you want, you can also display a maintenance message while the upgrade is underway. See "Displaying the Maintenance Message During an Upgrade," on page 35.
2. Use the cell management tool to quiesce all cells in the server group and shut down vCloud Director services on each server. See "Use the Cell Management Tool to Quiesce and Shut Down a Server," on page 35.
3. Upgrade vCloud Director software on all members of the server group. See "Upgrade vCloud Director Software on Any Member of a Server Group," on page 42. You can upgrade the servers individually or in parallel, but you must not restart vCloud Director services on any upgraded member of the group before you upgrade the vCloud Director database.
4. Upgrade the vCloud Director database. See "Upgrade the vCloud Director Database," on page 44.
5. Restart vCloud Director on the upgraded servers. See "Start or Stop vCloud Director Services," on page 29.

6 Upgrade vShield Manager. All vShield Manager installations registered to this server group must be upgraded to a version of vShield Manager software that is compatible with the version of vCloud Director installed by the upgrade. If the upgrade program detects an incompatible version of vShield Manager, upgrading will not be allowed. The latest version of vShield manager listed in "Supported vCenter Server, ESX/ESXi, and vShield Manager Versions," on page 9 is required to use networking features introduced in this release of vCloud Director.See "Upgrade vShield Manager," on page 46

7 Re-enable user access to vCloud Director.

8 Upgrade vCenter and ESX/ESXi Hosts. See "Upgrade vCenter, ESX/ESXi Hosts, and vShield Edge Appliances," on page 47. All vCenter servers registered to this server group must be upgraded to a version of vCenter software that is compatible with the version of vCloud Director installed by the upgrade. Incompatible vCenter servers become inaccessible from vCloud Director after the upgrade is complete. See "Supported vCenter Server, ESX/ESXi, and vShield Manager Versions," on page 9.

9 Review the changes in your upgraded networks and reconfigure firewall rules as needed. See "Changes to Upgraded Networks," on page 48.

Using a Load Balancer to Reduce Service Downtime

If you are using a load balancer or other tool that can force requests to go to specific servers, you can upgrade a subset of the server group while keeping existing services available on the remaining subset. This approach reduces vCloud Director service downtime to the length of time required to upgrade the vCloud Director database.

1 Use the load balancer to redirect vCloud Director requests to a subset of the servers in the group. Follow the procedures recommended by your load balancer.

2 Use the cell management tool to quiesce the cells that are no longer handling requests and shut down vCloud Director services on those servers. See "Use the Cell Management Tool to Quiesce and Shut Down a Server," on page 35.

3 Upgrade vCloud Director software on the members of the server group on which you have stopped vCloud Director, but do not restart those services. See "Upgrade vCloud Director Software on Any Member of a Server Group," on page 42.

4 Use the cell management tool to quiesce the cells that you have not yet upgraded and shut down vCloud Director services on those servers.

5 Upgrade the vCloud Director database. See "Upgrade the vCloud Director Database," on page 44.

6 Restart vCloud Director on the upgraded servers. See "Start or Stop vCloud Director Services," on page 29.

7 Upgrade vShield Manager. See "Upgrade vShield Manager," on page 46.

8 Upgrade vCenter and ESX/ESXi Hosts. See "Upgrade vCenter, ESX/ESXi Hosts, and vShield Edge Appliances," on page 47.

9 Use the load balancer to redirect vCloud Director requests to the upgraded servers.

10 Upgrade vCloud Director software on the remaining servers in the group, and restart vCloud Director on those servers as the upgrades complete. See "Upgrade vCloud Director Software on Any Member of a Server Group," on page 42.

11 Review the changes in your upgraded networks and reconfigure firewall rules as needed. See "Changes to Upgraded Networks," on page 48.

Displaying the Maintenance Message During an Upgrade

If you anticipate a lengthy upgrade process and want to have the system display a maintenance message while the upgrade is underway, verify that at least one cell remains accessible while the others are being upgraded. Run the `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` command on that cell to turn on the cell maintenance message.

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

You can run this command on a cell before or after it has been upgraded. When you are ready to upgrade the cell or return an upgraded cell to service, run the following command on the cell to turn off the maintenance message.

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

This chapter includes the following topics:

Use the Cell Management Tool to Quiesce and Shut Down a Server

Before you upgrade a vCloud Director server, use the cell management tool to quiesce and shut down vCloud Director services on the server's cell.

vCloud Director creates a task object to track and manage each asynchronous operation that a user requests. Information about all running and recently completed tasks is stored in the vCloud Director database. Because a database upgrade invalidates this task information, you must be sure that no tasks are running when you begin the upgrade process.

With the cell management tool, you can suspend the task scheduler so that new tasks cannot be started, then check the status of all active tasks. You can wait for running tasks to finish or log in to vCloud Director as a system administrator and cancel them. See "Cell Management Tool Reference," on page 36. When no tasks are running, you can use the cell management tool to stop vCloud Director services.

Prerequisites

- Verify that you have superuser credentials for the target server.
- Verify that you have vCloud Director system administrator credentials.

Procedure

1 Log in to the target server as root.

2 Use the cell management tool to gracefully shut down the cell.

a Retrieve the current job status.

The following `cell-management-tool` command supplies system administrator credentials and returns the count of running jobs.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator -p Pa55w0rd cell --status
Job count = 3
Is Active = true
```

b Stop the task scheduler to quiesce the cell.

Use a `cell-management-tool` command of the following form.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator -p Pa55w0rd cell --quiesce true
```

This command prevents new jobs from being started. Existing jobs continue to run until they finish or are cancelled. To cancel a job, use the vCloud Director Web Console or the REST API.

c When the `Job count` value is `0` and the `Is Active` value is `false`, it is safe to shut down the cell.

Use a `cell-management-tool` command of the following form.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator -p Pa55w0rd cell --shutdown
```

What to do next

After the cell management tool stops vCloud Director services on this server, you can upgrade the server's vCloud Director software.

Cell Management Tool Reference

The cell management tool is a command-line utility that you can use to manage a cell and its SSL certificates, and to export tables from the vCloud Director database. Superuser or system administrator credentials are required for some operations.

The cell management tool is installed in `/opt/vmware/vcloud-director/bin/cell-management-tool`.

Listing Available Commands

To list the available cell management tool commands, use the following command line.

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

Example: Cell Management Tool Usage Help

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

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

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

```
required

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

- Commands for Managing a Cell on page 37

  Use the `cell` command of the cell management tool to suspend the task scheduler so that new tasks cannot be started, to check the status of active tasks, and to shut down the cell gracefully.

- Commands for Exporting Database Tables on page 38

  Use the `dbextract` command of the cell management tool to export data from the vCloud Director database.

- Commands for Replacing SSL Certificates on page 40

  Use the `certificates` command of the cell management tool to replace the cell's SSL certificates.

- Commands for Generating Self-Signed SSL Certificates on page 41

  Use the `generate-certs` command of the cell management tool to generate new self-signed SSL certificates for the cell.

- Recovering the System Administrator Password on page 42

  If you know the vCloud Director database username and password, you can use the `recover-password` command of the cell management tool to recover the vCloud Director system administrator password.

Commands for Managing a Cell

Use the `cell` command of the cell management tool to suspend the task scheduler so that new tasks cannot be started, to check the status of active tasks, and to shut down the cell gracefully.

To manage a cell, use a command line with the following form:

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

sysadmin-username Username of a vCloud Director system administrator.

sysadmin-password Password of the vCloud Director system administrator.

command `cell` subcommand.

Table 3-1. Cell Management Tool Options and Arguments, `cell` Subcommand

Command	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--quiesce` (`-q`)	`true` or `false`	Quiesces activity on the cell. The argument `true` suspends the scheduler. The argument `false` restarts the scheduler.
`--shutdown` (`-s`)	None	Shuts down vCloud Director services on the server.
`--status` (`-t`)	None	Displays information about the number of jobs running on the cell and the status of the cell.

Example: Getting Task Status

The following `cell-management-tool` command line supplies system administrator credentials and returns the count of running jobs. When the `Job count` value is `0` and the `Is Active` value is `false`, you can safely shut down the cell.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator -p Pa55w0rd cell --status
Job count = 3
Is Active = true
```

Commands for Exporting Database Tables

Use the `dbextract` command of the cell management tool to export data from the vCloud Director database.

To export database tables, use a command line with the following form:

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

Table 3-2. Cell Management Tool Options and Arguments, `dbextract` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`-categories`	A comma-separated list of table categories to export.	Optional. `NETWORKING` is the only supported category
`-dataFile`	An absolute path to a file describing the data to export.	Optional. If not supplied, the command uses `$VCLOUD_HOME/etc/data_to_export.properties`. See "Specifying Tables and Columns to Export," on page 39.
`-dumpFile`	An absolute path to a dump file.	All data will be exported to this file.
`-exportSettingsFile`	An absolute path to a data export settings properties file.	Optional. If not supplied, the command uses `$VCLOUD_HOME/etc/data_export_settings.ini`. See "Limiting and Ordering Exported Rows," on page 40.
`-properties`	An absolute path to a database connection properties file.	Optional. If not supplied, the command uses the database connection properties in `$VCLOUD_HOME/etc/global.properties`. See "Specifying a Properties File," on page 39.
`-tables`	A comma-separated list of tables.	Optional. Export all tables to see individual table names.

Specifying a Properties File

By default, the `dbextract` command extracts data from the vCloud Director database using the database connection information in the current cell's `$VCLOUD_HOME/etc/global.properties` file. To extract data from a different vCloud Director database, specify the database connection properties in a file and use the `–properties` option to provide the pathname to that file on the command line. The properties file is a UTF-8 file that has the following format.

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

username	The vCloud Director database user name.
password	The vCloud Director database password.
db_service_name	The database service name. For example, `orcl.example.com` .
db_connection_port	The database port.
db_server_ip_address	The IP address of the database server.
db_type	The database type. Must be `Oracle` or `MS_SQL` .

Specifying Tables and Columns to Export

To restrict the set of data exported, use the `–exportSettingsFile` option and create a `data_to_export.properties` file that specifies individual tables and, optionally, columns to export. This file is a UTF-8 file that contains zero or more lines of the form *TABLE_NAME*:*COLUMN_NAME*.

TABLE_NAME	The name of a table in the database. To see a list of table names, export all tables.
COLUMN_NAME	The name of a column in the specified *TABLE_NAME*.

This example `data_to_export.properties` file exports columns from the `ACL` and `ADDRESS_TRANSLATION` tables.

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

The command expects to find this file in `$VCLOUD_HOME/etc/data_to_export.properties`, but you can specify another path.

Limiting and Ordering Exported Rows

For any table, you can specify how many rows to export and how to order the exported rows. Use the –exportSettingsFile option and create a data_export_settings.ini file that specifies individual tables. This file is a UTF-8 file that contains zero or more entries of the following form:

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

TABLE_NAME The name of a table in the database. To see a list of table names, export all tables.

COLUMN_NAME The name of a column in the specified *TABLE_NAME*.

This example data_export_settings.ini restricts data exported from the AUDIT_EVENT table to the first 10000 rows and orders the rows by the value in the event_time column

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

The command expects to find this file in $VCLOUD_HOME/etc/data_export_settings.ini, but you can specify another path.

Example: Exporting All Tables From the Current vCloud Director Database.

This example exports all tables of the current vCloud Director database to the file /tmp/dbdump .

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

Commands for Replacing SSL Certificates

Use the certificates command of the cell management tool to replace the cell's SSL certificates.

The certificates command of the cell management tool automates the process of replacing a cell's existing certificates with new ones stored in a JCEKS keystore. The certificates command helps you replace self-signed certificates with signed ones. To create a JCEKS keystore containing signed certificates, see "Create and Import a Signed SSL Certificate," on page 17 .

To replace the cell's SSL certificates, use a command with the following form:

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

Table 3-3. Cell Management Tool Options and Arguments, certificates Subcommand

Option	Argument	Description
--help (-h)	None	Provides a summary of available commands in this category.
--config (-c)	full pathname to the cell's global.properties file	Defaults to $VCLOUD_HOME/etc/global.properties.
--responses (-r)	full pathname to the cell's responses.properties file	Defaults to $VCLOUD_HOME/etc/responses.properties.

Table 3-3. Cell Management Tool Options and Arguments, `certificates` Subcommand (Continued)

Option	Argument	Description
`--keystore` (-s)	*keystore-pathname*	Full pathname to a JCEKS keystore containing the signed certificates.
`--keystore-pwd` (-w)	*keystore-password*	Password for the JCEKS keystore referenced by the `--keystore` option.

Example: Replacing Certificates

You can omit the `--config` and `--responses` options unless those files were moved from their default locations. In this example, a keystore at `/tmp/new.ks` has the password `kspw`. This example replaces the cell's existing certificates with the certificates found in `/tmp/new.ks`

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

NOTE You must restart the cell after you replace the certificates.

Commands for Generating Self-Signed SSL Certificates

Use the `generate-certs` command of the cell management tool to generate new self-signed SSL certificates for the cell.

The `generate-certs` command of the cell management tool automates the procedure shown in "Create a Self-Signed SSL Certificate," on page 19.

To generate new self-signed SSL certificates and add them to a new or existing keystore, use a command line with the following form:

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

Table 3-4. Cell Management Tool Options and Arguments, `generate-certs` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`-issuer` (-i)	*name=value* [, *name=value*, ...]	X.509 distinguished name of the certificate issuer. Defaults to `CN=Unknown`. If you specify multiple attribute and value pairs, separate them with commas and enclose the entire argument in quotation marks.
`--out` (-o)	*keystore-pathname*	Full pathname to the keystore on this host.
`--key-size` (-s)	*key-size*	Size of key pair expressed as an integer number of bits. Defaults to 1024.
`--keystore-pwd` (-w)	*keystore-password*	Password for the keystore on this host.
`--expiration` (-x)	*days-until-expiration*	Number of days until the certificates expire. Defaults to 365

Example: Creating Self-Signed Certificates

Both of these examples assume a keystore at `/tmp/cell.ks` that has the password `kspw`. This keystore is created if it does not already exist.

This example creates the new certificates using the defaults. The issuer name is set to `CN=Unknown`. The certificate uses 1024-bit encryption and expires one year after creation.

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

This example creates the new certificates using custom values for key size and issuer name. The issuer name is set to `CN=Test, L=London, C=GB`. The certificate uses 2048-bit encryption and expires 90 days after creation.

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

Recovering the System Administrator Password

If you know the vCloud Director database username and password, you can use the `recover-password` command of the cell management tool to recover the vCloud Director system administrator password.

With the `recover-password` command of the cell management tool, a user who knows the vCloud Director database username and password can recover the vCloud Director system administrator password.

To recover the system administrator password, use a command line with the following form:

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

Table 3-5. Cell Management Tool Options and Arguments, `recover-password` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--dbuser`	The user name of the vCloud Director database user.	Must be supplied on the command line.
`--dbpassword`	The password of the vCloud Director database user.	Prompted for if not supplied.

Upgrade vCloud Director Software on Any Member of a Server Group

The vCloud Director installer verifies that the target server meets all upgrade prerequisites and upgrades the vCloud Director software on the server.

vCloud Director software is distributed as a Linux executable file named `vmware-vcloud-director-5.1.0-`*nnnnnn*`.bin`, where *nnnnnn* represents a build number. After the upgrade is installed on a member of a server group, you must run a tool that upgrades the vCloud Director database that the group uses before you can restart vCloud Director services on the upgraded server.

Prerequisites

- Verify that all organizations in the system that contain an organization network also contain an organization vDC. Because the upgrade process converts existing organization networks to organization vDC networks, organizations that contain organization networks but do not contain an organization vDC cannot be upgraded, and the database upgrade fails.

- Verify that you have superuser credentials for the target server.
- If you want the installer to verify the digital signature of the installation file, download and install the VMware public key on the target server. If you have already verified the digital signature of the installation file, you do not need to verify it again during installation. See "Download and Install the VMware Public Key," on page 22.
- Use the cell management tool to quiesce and shut down vCloud Director services on the server's cell.

Procedure

1 Log in to the target server as root.

2 Download the installation file to the target server.

If you purchased the software on a CD or other media, copy the installation file to a location that is accessible to all target servers.

3 Verify that the checksum of the download matches the one posted on the download page.

Values for both MD5 and SHA1 checksums are posted on the download page. Use the appropriate tool to verify that the checksum of the downloaded installation file matches the one shown on the download page. A Linux command of the following form validates the checksum for *installation-file* using the MD5 *checksum-value* copied from the download page.

```
md5sum –c checksum–value installation–file
```

4 Ensure that the installation file is executable.

The installation file requires execute permission. To be sure that it has this permission, open a console, shell, or terminal window and run the following Linux command, where *installation-file* is the full pathname to the vCloud Director installation file.

```
chmod u+x installation–file
```

5 Use the cell management tool to quiesce the cell and shut down vCloud Director services on the server.

See "Use the Cell Management Tool to Quiesce and Shut Down a Server," on page 35.

6 In a console, shell, or terminal window, run the installation file.

To run the installation file, type its full pathname, for example `./installation–file`. The file includes an installation script and an embedded RPM package.

NOTE You cannot run the installation file from a directory whose pathname includes any embedded space characters.

If the installer detects a version of vCloud Director installed on this server that is equal to or later than the version in the installation file, it displays an error message and exits. Otherwise, it prompts you to confirm that you are ready to upgrade this 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?  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 Respond to the upgrade prompt.

Option	Action
Continue the upgrade.	Type **y**.
Exit to the shell without making any changes in the current installation.	Type **n**.

After you confirm that you are ready to upgrade the server, the installer verifies that the host meets all requirements, unpacks the vCloud Director RPM package, stops vCloud Director services on the server, and upgrades the installed vCloud Director software.

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

The installer prints a warning of the following form if you did not install the VMware public key on the target server.

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

8 (Optional) Update logging properties.

After an upgrade, new logging properties are written to the file `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew`.

Option	Action
If you did not change existing logging properties	Copy this file to `/opt/vmware/vcloud-director/etc/log4j.properties`.
If you changed logging properties	Merge `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` file with the existing `/opt/vmware/vcloud-director/etc/log4j.properties`. Merging these files preserves your changes.

When the vCloud Director software upgrade is complete, the installer displays a message indicating where the old configuration files are stored, then reminds you to run the database upgrade tool.

What to do next

- If you have not already done so, upgrade the vCloud Director database that this server uses.
- If you already upgraded the vCloud Director database that this server group uses, you can restart the upgraded server. See "Start or Stop vCloud Director Services," on page 29.

Upgrade the vCloud Director Database

After you upgrade a server in your vCloud Director server group, you must upgrade the group's vCloud Director database before you restart vCloud Director services on the server.

All servers in a vCloud Director server group share the same database, so regardless of how many servers you are upgrading, you need upgrade the database only once. After the database has been upgraded, vCloud Director servers cannot connect to it until they, too, have been upgraded.

Prerequisites

IMPORTANT Back up your existing database before you upgrade it. Use the procedures that your database software vendor recommends.

- Verify that no vCloud Director servers are using the database. See "Use the Cell Management Tool to Quiesce and Shut Down a Server," on page 35

Procedure

1 Open a console, shell, or terminal window, and type the following command to run the database upgrade script.

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

IMPORTANT If the database upgrade script detects that an incompatible version of vShield manager is registered to this installation of vCloud Director, it displays this warning message and cancels the upgrade.

```
One or more vShield Manager servers registered to this vCloud
Director installation are not supported by the version of vCloud Director
you are upgrading to. Upgrade canceled, please follow the procedures in
the vShield Manager Upgrade Guide to upgrade those unsupported vShield
Manager servers to vShield Manager version 5.0 or later versions.
```

See "Upgrade vShield Manager," on page 46.

2 Respond to the database upgrade prompt.

```
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
```

Option	Action
Continue the upgrade.	Type **y**.
Exit to the shell without making any changes in the current vCloud Director database.	Type **n**.

The database upgrade tool runs and displays progress messages.

```
Examining database at URL: jdbc:oracle:thin:@10.26.50.54:1521/orcl
Applying 1 upgrade batches
Executing upgrade batch:
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:
Running 2 upgrade tasks
Successfully ran upgrade task
Successfully ran upgrade task
Applying 1 upgrade batches
Executing upgrade batch: 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: cleanup
Database upgrade complete
++++++++++++++++++++++++++++++++
```

3 (Optional) Rebuild the database indexes and update the database statistics.

These steps are optional and can lead to better database performance after the upgrade.

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


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

After the database has been upgraded, the upgrade script offers to start vCloud Director services on this host.

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

Upgrade vShield Manager

Before you can upgrade vCenter and ESX/ESXi hosts registered to vCloud Director, you must upgrade vShield Manager servers attached to the vCenter servers.

Before you upgrade a vCenter server attached to vCloud Director, upgrade the vShield Manager server associated with the upgraded vCenter server. Upgrading vShield Manager interrupts access to vShield Manager administrative functions, but does not interrupt network services.

Prerequisites

At least one upgraded cell in your vCloud Director installation must be running before you begin this upgrade. The cell is responsible for writing data about the upgraded vShield Manager to the vCloud Director database.

Procedure

1 Upgrade vShield Manager.

Follow the procedure in the *vShield Quick Start Guide*. After this upgrade completes, vShield Manager notifies vCloud Director that it has a new version. It can take several minutes before vShield Manager sends the notification and vCloud Director processes it.

2 After you have upgraded vShield manager, you must upgrade all vCenter and ESX/ESXi hosts before you upgrade the vShield Edge appliances that the upgraded vShield Manager manages.

Upgrade vCenter, ESX/ESXi Hosts, and vShield Edge Appliances

After you have upgraded vCloud Director and vShield Manager, upgrade the vCenter servers and ESX/ESXi hosts attached to your cloud, then upgrade vShield Edge appliances on upgraded vCenter servers.

Procedure

1 Upgrade the vCenter server.

See the *vSphere Installation and Setup Guide*.

2 Refresh the vCenter server's registration with vCloud Director.

a In the vCloud Director Web console, click the **Manage & Monitor** tab and click **vCenters** in the left pane.

b Right-click the vCenter Server name and select **Refresh**.

c Click **Yes**.

3 Upgrade each ESX/ESXi host that the upgraded vCenter server supports.

See the *vSphere Installation and Setup Guide*. For each host, the upgrade requires the following steps:

a In the vCloud Director Web console, disable the host.

On the **Manage and Monitor** page, click **Hosts**, then right-click the host and select **Disable Host**.

b Use vCenter to put the host into maintenance mode and allow all the virtual machines on that host to migrate to another host.

c Upgrade the host.

To ensure that you have enough upgraded host capacity to support the virtual machines in your cloud, upgrade hosts in small batches. When you do this, host agent upgrades can complete in time to allow virtual machines to migrate back to the upgraded host.

d Use vCenter to reconnect the host.

e Upgrade the vCloud Director host agent on the host.

See "Upgrade an ESX/ESXi Host Agent" in the *vCloud Director Administrator's Guide*.

f In the vCloud Director Web console, enable the host.

On the **Manage and Monitor** page, click **Hosts**, then right-click the host and select **Enable Host**.

g Use vCenter to take the host out of maintenance mode.

4 Upgrade all vShield Edge appliances managed by the vShield Manager on the upgraded vCenter server.

Use the vShield Manager user interface to manage this upgrade.

NOTE If you use the vCloud Director Web console or REST API to reset a network that vShield Edge protects, this upgrade occurs automatically. Using the vShield Manager user interface to manage the vShield Edge provides better administrative control over the upgrade process and related network downtime.

Changes to Upgraded Networks

Because of changes in the vCloud Director networking infrastructure, existing networks and services are sometimes modified by the upgrade process. While none of these modifications affect existing network connections, post-upgrade reconfiguration might be required for some network services.

Organization Networks

When you upgrade vCloud Director to this release, existing organization networks are converted to use the new vCloud Director networking infrastructure. You can expect to see the following changes in your upgraded organization networks.

- Routed organization networks become routed organization vDC networks. These networks are connected to an Edge Gateway in one of your organization vDCs. Services, such as NAT and firewall, that had been defined in the organization network are now defined in the Edge Gateway. If your organization has multiple vDCs, organization vDC networks created during an upgrade are shared across all vDCs in the organization.
- Isolated organization networks become isolated organization vDC networks.
- Directly connected organization networks are unchanged.
- New organization VDC networks use the network pool assigned to the organization VDC in which the network is created.
- NAT rules in routed organization networks are converted to Edge Gateway NAT rules. The effect of each rule remains the same, though the rule is expressed differently. See the *vCloud Director Administrator's Guide* for more about NAT rules. NAT rules in routed vApp networks are unchanged.

Edge Gateways and vApp Networks

Firewall services and firewall rules have been changed to allow greater flexibility in configuration in both Edge gateways and vApp networks.

After an upgrade, all firewall services in Edge Gateways and routed vApp networks are running in compatibility mode, which preserves the operational semantics of their firewall rules. After you convert existing firewall rules to the current format, you can upgrade your networks to remove the limitations imposed by compatibility mode. See the *vCloud Director Administrator's Guide* for more about firewall rules.

Network Limitations in Compatibility Mode

Several limitations apply while the system is in compatibility mode.

- Each EdgeGateway can support exactly one uplink and one internal interface, so there can be only one routed organization vDC network per Edge Gateway.
- Version 5.1 firewall rules cannot be created in a firewall service.

To remove these limitations, see "Reconfigure Edge Gateways and vApp Networks to Enable Normal Operation," on page 48

Reconfigure Edge Gateways and vApp Networks to Enable Normal Operation

After you convert existing firewall rules to the current format, you can reconfigure your Edge Gateways and vApp networks to enable normal operation and remove the limitations imposed by compatibility mode.

In earlier releases of vCloud Director, firewall rules specified the direction of packets subject to the rule. Beginning with this release, packet direction is derived from the source and destination IP addresses. In the **Source** or **Destination** IP address of a firewall rule, you can now use the keywords **`internal`** and **`external`** in addition to the **`any`** keyword or an IP address.

After an upgrade, all firewall services in Edge Gateways and vApp networks are running in compatibility mode, which preserves the operational semantics of their firewall rules. After you convert existing firewall rules to the current format, you can upgrade your networks to remove the limitations imposed by compatibility mode. See the *vCloud Director Administrator's Guide* for more about firewall rules.

Procedure

1 Redeploy all Edge Gateways.

   Right-click each Edge Gateway and select **Re-Deploy**.

2 Redeploy all vApp networks.

   Right-click each vApp network and select **Reset Network**.

3 Convert all Edge Gateway firewall rules to the current format.

   You can click **Convert Rules** on the **Firewall** tab of the **Gateway Services** page to automatically convert the rules. You can also convert the rules manually.

   a On the **Firewall** tab of the **Gateway Services** page, select the rule and click **Edit**.

   b Clear the **Match rule on translated IP** checkbox.

   c Wherever **`any`** is used to specify a **Source** or **Destination** IP address, use **`internal`** or **`external`** instead.

   d If the rule is intended to provide destination NAT, change the **Destination** IP address from **`internal`** to **`external`**.

4 Convert all vApp network firewall rules to the current format.

   You can click **Convert Rules** on the **Firewall** tab of the **Configure Services** page of a vApp network to automatically convert the rules. You can also convert the rules manually.

   a On the **Firewall** tab of the **Configure Services** page of a vApp network select the rule and click **Edit**.

   b Clear the **Match rule on translated IP** checkbox.

   c Wherever **`any`** is used to specify a **Source** or **Destination** IP address, use **`internal`** or **`external`** instead.

   d If the rule is intended to provide destination NAT, change the **Destination** IP address from **`internal`** to **`external`**.

5 Reconfigure all Edge Gateways to remove compatibility mode constraints.

   On the **General** tab of the Edge Gateway Properties page, select **Enable multiple interface support**.

6 Reconfigure all vApp networks to remove compatibility mode constraints.

   a Click the **My Cloud** tab and click **vApps** in the left pane.

   b Right-click a vApp and select **Open**.

   c On the **Networking** tab, select **Show networking details**.

   d Right-click the vApp network and select **Configure Services**.

   e In the **Firewall** tab, select **Match rules on original addresses only**

vCloud Director Setup 4

After you configure all servers in the vCloud Director server group and connect them to the database, you can initialize the server group's database with a license key, system administrator account, and related information. When this process is complete, you can use the vCloud Director Web Console to complete the initial provisioning of your cloud.

Before you can run the vCloud Director Web Console, you must run the Setup wizard, which gathers the information that the Web Console requires before it can start. After the wizard is finished, the Web Console starts and displays the login screen. The vCloud Director Web Console provides a set of tools for provisioning and managing a cloud. It includes a Quickstart feature that guides you through steps like attaching vCloud Director to vCenter and creating an organization.

Prerequisites

- Complete the installation of all vCloud Director servers, and verify that vCloud Director services have started on all servers.
- Verify that you have the URL that the configuration script displays when it completes.

> **NOTE** To discover the URL of the Setup wizard after the script exits, look up the fully qualified domain name associated with the IP address you specified for the HTTP service during installation of the first server and use it to construct a URL of the form https://*fully-qualified-domain-name*, for example, https://mycloud.example.com. You can connect to the wizard at that URL.

Complete the installation of all vCloud Director servers, and verify that vCloud Director services have started on all servers.

Procedure

1 Open a Web browser and connect to the URL that the configuration script displays when it completes.

2 Follow the prompts to complete the setup.

This chapter includes the following topics:

Review the License Agreement

Before you can configure a vCloud Director server group, you must review and accept the end user license agreement.

Procedure

1 Review the license agreement.

2 Accept or reject the agreement.

Option	Action
To accept the license agreement.	Click **Yes, I accept the terms in the license agreement**.
To reject the license agreement	**No, I do not accept the terms in the license agreement**.

If you reject the license agreement, you cannot proceed with vCloud Director configuration.

Enter the License Key

Each vCloud Director cluster requires a license to run. The license is specified as a product serial number. The product serial number is stored in the vCloud Director database.

The vCloud Director product serial number is not the same as the vCenter server license key. To operate a vCloud, you must have a vCloud Director product serial number and a vCenter server license key. You can obtain both types of license keys from the VMware License Portal.

Procedure

1 Obtain a vCloud Director product serial number from the VMware License Portal.

2 Type the product serial number in the **Product serial number** text box.

Create the System Administrator Account

Specify the user name, password, and contact information for the vCloud Director system administrator.

The vCloud Director system administrator has superuser privileges throughout the cloud. You create the initial system administrator account during vCloud Director setup. After installation and configuration is complete, this system administrator can create additional system administrator accounts as needed.

Procedure

1 Type the system administrator's user name.

2 Type the system administrator's password and confirm it.

3 Type the system administrator's full name.

4 Type the system administrator's email address.

Specify System Settings

You can specify the system settings that control how vCloud Director interacts with vSphere and vShield Manager.

The configuration process creates a folder in vCenter for vCloud Director to use and specifies an installation ID to use when you create MAC addresses for virtual NICs.

Procedure

1 Type a name for the vCloud Director vCenter folder in the **System name** field.

2 Use the **Installation ID** field to specify the installation ID for this installation of vCloud Director.

If a datacenter includes multiple installations of vCloud Director, each installation must specify a unique installation ID.

Ready to Log In to vCloud Director

After you provide all of the information that the Setup Wizard requires, you can confirm your settings and complete the wizard. After the wizard finishes, the login screen of the vCloud Director Web Console appears.

The Ready to Log In page lists all the settings you have provided to the wizard. Review the settings carefully.

Prerequisites

Verify that you have access to vCenter and vShield Manager. The vCloud Director Web Console requires access to the installations of vCenter and vShield Manager that you want to configure as part of this vCloud Director. These installations must be running and configured to work with each other before you finish this task. For more information, see "vCloud Director Hardware and Software Requirements," on page 9.

Procedure

- To change a setting, click **Back** until you get to the page where the setting originated.
- To confirm all settings and complete the configuration process, click **Finish**.

When you click **Finish**, the wizard applies the settings you specified, then starts the vCloud Director Web Console and displays its login screen.

What to do next

Log in to the vCloud Director Web Console using the user name and password you provided for the system administrator account. After you have logged in, the console displays a set of Quickstart steps that you must complete before you can use this cloud. When the steps are complete, the Guided Tasks are enabled, and your cloud is ready for use.

Index