Cloud Director Installation and Configuration Guide

Cloud Director 1.0.0

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-000338-01



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, 2011 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

About This Book 5

- Overview of VMware Cloud Director Installation and Configuration 7 Cloud Director Architecture 7 Configuration Planning 8 About the Cloud Director Database 9 Cloud Director Hardware and Software Requirements 10
- Creating a VMware Cloud Director Cluster 21
 Install Cloud Director Software on the First Server Host 22
 Configure Network and Database Connections 23
 Start Cloud Director Services 25
 Install Cloud Director Software on Additional Server Hosts 26
 Create a Microsoft Sysprep Deployment Package 27
 Uninstall VMware Cloud Director Software 27

3 Cloud Director Setup 29

Review the License Agreement 30 Enter the License Key 30 Create the System Administrator Account 30 Specify System Settings 31 Ready to Log In 31

Index 33

Cloud Director Installation and Configuration Guide

About This Book

The VMware Cloud Director[®] Installation and Configuration Guide provides information about installing VMware Cloud Director software and configuring it to work with vCenter to provide VMware-ready Cloud services.

Intended Audience

This book is intended for anyone who wants to install and configure VMware Cloud Director software. The information in this book is written for experienced system administrators who are familiar with Linux, Windows, IP networks, and VMware vSphere.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support	To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.
	Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.
Support Offerings	To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.
VMware Professional Services	VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting

Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

Overview of VMware Cloud Director Installation and Configuration

A VMware Cloud Director[®] cluster combines Cloud Director servers with the vSphere platform. You create a Cloud Director cluster by installing and configuring Cloud Director software on one or more server hosts, and then integrating the cluster with one or more installations of vSphere.

This chapter includes the following topics:

- "Cloud Director Architecture," on page 7
- "Configuration Planning," on page 8
- "About the Cloud Director Database," on page 9
- "Cloud Director Hardware and Software Requirements," on page 10

Cloud Director Architecture

In a Cloud, a VMware Cloud Director cluster is linked with one or more vCenter servers and vShield Manager servers, and an arbitrary number of ESX/ESXi hosts. The Cloud Director cluster and its database manage access to vCenter resources by Cloud clients.

Figure 1-1 is a schematic representation of a simple Cloud. The diagram shows a Cloud Director cluster comprising four server hosts. Each host runs a group of services called a Cloud Director cell. All hosts in the cluster share a single database. The entire cluster is connected to three vCenter servers and the ESX/ESXi hosts that they manage. Each vCenter server is connected to a vShield Manager host, which provides network services to the Cloud.





The Cloud Director installation and configuration process creates the cells, connects them to the shared database, and establishes the first connections to a vCenter server, ESX/ESXi hosts, and vShield Manager. After installation and configuration is complete, a system administrator can connect additional vCenter servers, vShield Manager servers, and ESX/ESXi hosts to the Cloud Director cluster at any time.

Configuration Planning

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

Configuration requirements depend on many factors, including the number of organization in a 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 Cloud Director server host (cell) for each vCenter server that you want to include in your cloud.
- Be sure that all Cloud Director server hosts meet at least the minimum requirements for memory, CPU, and storage detailed in "Cloud Director Hardware and Software Requirements," on page 10.
- Configure the Cloud Director database as described in "About the Cloud Director Database," on page 9.

About the Cloud Director Database

Cells in a Cloud Director cluster use a database to store shared information. This database must exist before you can complete installation and configuration of Cloud Director software.

Database Configuration Parameters

The database must be configured to allow at least 75 connections per Cloud Director cell plus about 50 for Oracle's own use. There is one cell for each server host in a Cloud Director cluster. Table 1-1 shows how to obtain values for other configuration parameters based on the number of connections, where *C* represents the number of cells in your Cloud Director cluster.

Oracle Configuration ParameterValue for C CellsCONNECTIONS75*C+50PROCESSES= CONNECTIONSSESSIONS= PROCESSES*1.1+5TRANSACTIONS= SESSIONS*1.1OPEN_CURSORS= SESSIONS

Table 1-1. Oracle Database Configuration Parameters

Database Creation Best Practices

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;

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

Create user \$vclouduser identified by \$vcloudpass default tablespace CLOUD_DATA;

Database User Account and Required System Privileges

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

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

National Character Set

The database must be configured to use the AL16UTF16 character set.

Database Server Configuration

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

Cloud Director Hardware and Software Requirements

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

Supported vCenter, ESX/ESXi, and vShield Manager Versions

vCenter servers intended for use with Cloud Director must meet specific configuration requirements

- vCenter networks intended for use as Cloud Director external networks or network pools must be available to all hosts in any cluster intended for use by Cloud Director. Making these networks available to all hosts in the datacenter simplifies the task of adding new hosts to Cloud Director.
- DVS must be used for cross-host fencing and network pool allocation.
- vCenter clusters used with Cloud 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 hosts.

Table 1-2 lists the vCenter server versions that are compatible with this version of Cloud Director.

Table 1-2. Supported vCenter Versions

vCenter Version	Build Number	Required Patches
4.0 Update 2	264050	None
4.1	259021	None
4.1 vSphere Client	258902	None

Table 1-3 lists the ESX versions that are compatible with this version of Cloud Director.

Table 1-3. Supported ESX and ESXi Versions

ESX or ESXi Version	Build Number	Required Patches	
4.0 Update 2	261974	None	
4.1	260247	None	

Table 1-4 lists the vShield Manager versions that are compatible with this version of Cloud Director.

Table 1-4. Supported vShield Manager Versions

vShield Manager	Build Number	Required Patches
4.1	287872	None

Supported VMware Cloud Director Server Host Platforms

Table 1-5 lists the server operating systems that are compatible with this version of Cloud Director.

Table 1-5. Supported VMwa	re Cloud Director Server Host Platforms
---------------------------	---

Operating System			
Red Hat Enterprise Linux 5 (64 bit), Update 4			
Red Hat Enterprise Linux 5 (64 bit), Update 5			

Table 1-6 lists additional software that must be installed on each Cloud Director server host. These packages are typically installed by default with the operating system software. If any are missing, the installer fails with a diagnostic message.

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

Table 1-6. Required Software Packages

Supported Cloud Director Databases

Table 1-7 lists the database software products that are compatible with this version of Cloud Director.

Table 1-7.	Supported	Cloud Director	Database	Software

Database Software	Required Patches
Oracle 10g Standard Edition Release 2 (10.2.0.x)	None
Oracle 10g Enterprise Edition Release 2 (10.2.0.x)	None
Oracle 11g Standard Edition (11.1.0.x)	None
Oracle 11g Enterprise Edition (11.1.0.x)	None

Disk Space Requirements

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

Memory Requirements

Each Cloud Director server host must have at least 1GB of memory (2GB recommended).

Network Requirements

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

IP addresses	Each Cloud Director support two differe for the console prop of IP aliases or mul address using the L	or server host requires tw ent SSL connections: one ay service. You can creat tiple network interfaces. inux ip addr add comm	to IP addresses, so that it can for the HTTP service and another the these addresses through the use You cannot create the second and.	
Network Time Service	You must use a net all Cloud Director s maximum allowab seconds.	work time service such a server hosts, including th e drift between the clock	s NTP to synchronize the clocks of a database server host. The as of synchronized hosts is 2	
Hostname Resolution	All host names spe installation and cor reverse lookup of th hostname. For exan following comman	cified during Cloud Dire afiguration must be resol ne fully-qualified domain nple, for a host named m ds must succeed on a Clo	ctor and vShield Manager vable by DNS using forward and n name or the unqualified cycloud.example.com, both of the oud Director host:	
	nslookup mycloud nslookup mycloud.	example.com		
	In addition, if the h following comman	ost mycloud.example.com d must return mycloud.e	has the IP address 192.168.1.1, the xample.com:	
	nslookup 192.168.1.1			
Transfer Server Storage	torage To provide temporary storage for uploads and downloads, share must be accessible to all hosts in a Cloud Director cluster. The tra- storage volume must have write permission for root. Each host n this storage at \$VCLOUD_HOME/data/transfer (typically /opt/vmware/cloud-director/data/transfer). Uploads downloads occupy this storage for a short time (a few hours to a because transferred images can be large, allocate at least several gigabytes to this volume.			
Network Security	Connect all Cloud I Cloud Director net	Director services to a netw work connections have s	ork that is secured and monitored. everal additional requirements:	
	Do not connect protect Cloud I (HTTPS) must Cloud Director for incoming c public network used for incom	Cloud Director directly Director network connect be open to incoming cor cluster. Ports 22 (SSH) a connections if needed. All a must be rejected by the ing connections within a	to the Public Internet. Always tions with a firewall. Only port 443 nections from hosts outside the and 80 (HTTP) can also be opened other incoming traffic from a firewall. Table 1-8 lists the ports a Cloud Director cluster.	
	Table 1-8.PoDirector Hosts	rts That Must Allow Inco	ning Packets From Cloud	
	Port	Protocol	Comments	
	111	TCP, UDP	NFS portmapper used by transfer service	
	920	TCP, UDP	NFS rpc.statd used by transfer	

service

- - -

Port	Protocol	Comments
61611	TCP	ActiveMQ
61616	ТСР	ActiveMQ

Table 1-8. Ports That Must Allow Incoming Packets From Cloud Director Hosts (Continued)

 Table 1-9 lists the ports used for outgoing connections. Do not connect these ports to the public network.

l able 1-9.	Ports	That Must Allow	Outgoing	Packets I	From Cloud
Director Ho	sts				

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	ТСР	vCenter and ESX connections	
514	UDP	Optional. Enables syslog use	
902	TCP	vCenter and ESX connections	
903	ТСР	vCenter and ESX connections	
920	TCP, UDP	NFS rpc.statd used by transfer service	
1521	TCP	Default Oracle database port	
61611	TCP	ActiveMQ	
61616	ТСР	ActiveMQ	

- Do not connect physical hosts to physical networks that are uplinks for vNetwork distributed switches that back Cloud Director network pools.
- Traffic between Cloud Director hosts and the Cloud Director database server should be routed over a dedicated private network if possible.

Supported Browsers

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

"YES" means the browser version and OS platform are compatible, "No" means they are not compatible.

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

Browsers Supported on Microsoft Windows Platforms

Table 1-10 summarizes browser support on Microsoft Windows Platforms.

Virtual Switch IsolationVirtual 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.

Platform	Internet Explorer 7.*	Internet Explorer 8.*	Firefox 3.*
Windows XP Pro 32-bit	YES	YES	YES
Windows XP Pro 64-bit	YES	YES	YES
Windows Server 2003 Enterprise Edition 32-bit	YES	YES	YES
Windows Server 2003 Enterprise Edition 64-bit	YES	YES	YES
Windows Server 2003 Standard Edition 32-bit	YES	YES	YES
Windows Server 2003 Standard Edition 64-bit	YES	YES	YES
Windows Server 2008 32-bit	YES	YES	YES
Windows Server 2008 R2 32- bit	YES	YES	YES
Windows Vista 32-bit	YES	YES	YES
Windows Vista 64-bit	YES	YES	YES
Windows 7 32-bit	No	YES	YES
Windows 7 64-bit	No	YES	YES

Table 1-10. Browser Support on Microsoft Windows Platforms

Browsers Supported on Red Hat Enterprise Linux Platforms

Table 1-11 summarizes the browser support on Red Hat Enterprise Linux Platforms.

Table 1-11.	Browser Suppo	rt on Red Hat	Enterprise Linux	Platforms
-------------	---------------	---------------	------------------	-----------

Platform	Firefox 3.*
Red Hat Enterprise Linux 4 (32 bit)	YES
Red Hat Enterprise Linux 5 (32 bit), Update 4	YES
Red Hat Enterprise Linux 5 (32 bit), Update 5	YES

Browsers Supported on SUSE Linux Platforms

Table 1-12 summarizes the browser support on SUSE Linux Platforms.

Table 1-12. Browser Support on SUSE Linux Platforms

Platform	Firefox 3.*
SLES 11 32-bit	YES

Supported Versions of Adobe Flash Player

The Cloud Director Web Console requires Adobe Flash Player version 10.1 or later.

Supported TLS and SSL Protocol Versions and Cipher Suites

Cloud 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.

Installing and Configuring vShield Manager

Each Cloud Director cluster requires access to a vShield Manager host, which provides network services to the Cloud. Install and configure vShield Manager before you begin installing Cloud Director.

You must have a unique instance of vShield Manager for each vCenter Server you add to Cloud Director. For information about the network requirements and supported versions of vShield Manager, see "Cloud Director Hardware and Software Requirements," on page 10.

Procedure

- 1 Use the vSphere Client to log in to your vCenter Server.
- 2 From the File menu, select Deploy OVF Template.
- 3 Browse to the location of vShield Manager.ovf and follow the rest of the wizard steps to deploy the OVF.
- 4 After the OVF 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.

At the Password: prompt, type **default** to enable setup mode. When setup mode is enabled, the promote string changes to manager#.

- 7 At the manager# prompt, type **setup** to begin the setup procedure.
- 8 Enter the IP address, subnet mask, and default gateway for the vShield Manager virtual machine.

You will need this information later when you attach a vCenter Server to Cloud Director.

- 9 Type **exit** to log out.
- 10 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 using vShield Manager with Cloud Director.

Creating SSL Certificates

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

Each Cloud Director host requires two SSL certificates, one for each of its IP addresses. You must execute this procedure for each host that you intend to use in your Cloud Director cluster.

Procedure

1 List the IP addresses for this host.

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

2 For each IP address, run the following command and note the fully-qualified domain name.

nslookup ip-address

3 Make a note of each IP address, the fully-qualified domain name associated with it, and whether you want Cloud Director to use the address for the HTTP service or the Console Proxy service on this host.

You will need the hostnames when creating the certificates, and the IP addresses when configuring network and database connections. Recording the information in a form like the one shown in Table 1-13 can make it easier to create the certificates and, later, configure network and database connections.

Table 1-13. SSL Certificate Info	ormation
----------------------------------	----------

Service Name	IP Address	Hostname (FQDN)
HTTP	10.100.101.19	foo.example.com
Console Proxy	10.100.101.20	bar.example.com

4 Create the certificates.

You can use signed certificates (signed by a trusted certification authority) or self-signed certificates. Signed certificates provide the highest level of trust.

- To create signed certificates, see "Create and Import a Signed SSL Certificate," on page 16.
- To create self-signed certificates, see "Create a Self-Signed SSL Certificate," on page 18.

Create and Import a Signed SSL Certificate

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

Each Cloud Director host requires two SSL certificates, one for each of its IP addresses, in a Java keystore file. You must execute this procedure for each host that you intend to use in your Cloud Director cluster. You can use signed 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 18.

Prerequisites

- Follow the procedure in "Creating SSL Certificates," on page 15 to generate a list of fully-qualified domain names and their associated IP addresses on this host, along with a service choice for each domain name.
- You must have access to a computer that has a Java 6 runtime environment, so that you can use the keytool command to create the certificate. The Cloud Director installer places a copy of keytool in /opt/vmware/cloud-director/jre/bin/keytool, but you can perform this procedure on any computer that has a Java runtime environment installed. Creating and importing the certificates before you install and configure Cloud Director software simplifies the installation and configuration process. The 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 host.

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

In response to the keytool question:

What is your first and last name?

enter the fully qualified domain name of the HTTP service host. 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):

2 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

3 Create an untrusted certificate for the console proxy service host.

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

In response to the keytool question:

What is your first and last name?

enter the fully qualified domain name of the console proxy service host. For the remaining questions, provide answers appropriate for your organization and location, as shown in the example in Step 1.

4 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

- 5 Send the certificate signing requests to your Certification Authority.
- 6 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 a file named root.cer into the keystore file certificates.ks.

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

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

This command imports intermediate certificates from a file named intermediate.cer into the keystore file certificates.ks.

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

c Import the host-specific certificate for the HTTP service.

This command imports the certificate from a file named http.cer into the keystore file certificates.ks.

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

d Import the host-specific certificate for the console proxy service.

This command imports the certificate from a file named consoleproxy.cer into the keystore file certificates.ks.

keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias consoleproxy -file consoleproxy.cer 7 To verify that all the certificates have been imported, list the contents of the keystore file.

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

8 Repeat this procedure to create certificates for each additional Cloud Director host.

What to do next

If you created the keystore file (certificates.ks) on a host other than the one on which you generated the list of fully-qualified domain names and their associated IP addresses, copy the keystore file to that host now. You will need the keystore path name when you run the configuration script. (See "Configure Network and Database Connections," on page 23.)

NOTE Because the Cloud 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 Cloud Director in environments where trust concerns are minimal.

Each server host in a Cloud Director cluster must have two IP addresses, one for the HTTP service and one for the console proxy service, and be capable of establishing an SSL connection at each. This requires each host to have two SSL certificates, one for each IP address, in a Java keystore file. You can use signed 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 16.

Prerequisites

- Follow the procedure in "Creating SSL Certificates," on page 15 to generate a list of fully-qualified domain names and their associated IP addresses on this host, along with a service choice for each domain name.
- You must have access to a computer that has a Java 6 runtime environment, so that you can use the keytool command to create the certificate. The Cloud Director installer places a copy of keytool in /opt/vmware/cloud-director/jre/bin/keytool, but you can perform this procedure on any computer that has a Java runtime environment installed. Creating and importing the certificates before you install and configure Cloud Director software simplifies the installation and configuration process. The 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 host.

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

In response to the keytool question:

What is your first and last name?

enter the fully qualified domain name of the HTTP service host. 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):

2 Create an untrusted certificate for the console proxy service host.

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

In response to the keytool question:

What is your first and last name?

enter the fully qualified domain name of the console proxy service host. For the remaining questions, provide answers appropriate for your organization and location, as shown in the example in Step 1.

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

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

4 Repeat this procedure to create certificates for each additional Cloud Director host.

What to do next

If you created the keystore file (certificates.ks) on a host other than the one on which you generated the list of fully-qualified domain names and their associated IP addresses, copy the keystore file to that host now. You will need the keystore path name when you run the configuration script. (See "Configure Network and Database Connections," on page 23.)

NOTE Because the Cloud 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.

Cloud Director Installation and Configuration Guide

2

Creating a VMware Cloud Director Cluster

A Cloud Director cluster consists of one or more server hosts. Each host in the cluster runs a group of services called a Cloud Director cell. To create a cluster, you install Cloud Director software on each server host and connect the host to a shared database.

Prerequisites

Before you begin installing and configuring Cloud Director, be sure that all of the following tasks have been completed:

- 1 A supported vCenter server must be running and properly configured for use with Cloud Director. See "Supported vCenter, ESX/ESXi, and vShield Manager Versions," on page 10 for supported versions and configuration requirements.
- 2 A supported vShield Manager server must be running and properly configured for use with Cloud Director. See "Supported vCenter, ESX/ESXi, and vShield Manager Versions," on page 10 for supported versions. See "Installing and Configuring vShield Manager," on page 15 for installation and configuration details.
- 3 At least one supported Cloud Director host platform must be running and configured with an appropriate amount of memory and storage. See "Supported VMware Cloud Director Server Host Platforms," on page 10 for supported platforms and configuration requirements.
 - Each host must have two IP addresses.
 - Each host must have two SSL certificates: one for each IP address. See "Creating SSL Certificates," on page 15.
 - Each host must mount the shared transfer server storage at \$VCLOUD_HOME/data/transfer (typically /opt/vmware/cloud-director/data/transfer). This volume must have write permission for root.
 - Each host should have access to a Microsoft Sysprep deployment package.
- 4 The database for this cluster must exist and be accessible to all hosts in the cluster. See "Supported Cloud Director Databases," on page 11 for a list of supported database software.
 - An account for the Cloud Director database user must exist and be granted the required system privileges. For more information, see "About the Cloud Director Database," on page 9.
 - Verify that the database service starts automatically when the database server is rebooted.
- 5 All Cloud Director server hosts, the database server, and all vCenter and vShield Manger serves must be able to resolve each others names as described in "Network Requirements," on page 12.
- 6 All Cloud Director server hosts and the database server host must be synchronized to a network time server.

- 7 If you plan to import users or groups from an LDAP service, the LDAP server host must be accessible to each Cloud Director server host.
- 8 Firewall ports must be opened as shown on Table 1-8 and Table 1-9. It is especially important that port 443 be open between Cloud Director and vCenter servers.

This chapter includes the following topics:

- "Install Cloud Director Software on the First Server Host," on page 22
- "Configure Network and Database Connections," on page 23
- "Start Cloud Director Services," on page 25
- "Install Cloud Director Software on Additional Server Hosts," on page 26
- "Create a Microsoft Sysprep Deployment Package," on page 27
- "Uninstall VMware Cloud Director Software," on page 27

Install Cloud Director Software on the First Server Host

The Cloud Director installer verifies that the target host meets all prerequisites and installs Cloud Director software on the host.

VMware Cloud Director software is distributed as a Linux executable file named vmware-clouddirector-1.0.0-*nnnnn*.bin, where *nnnnn* represents the build number of this version. Running this file requires superuser (root) privileges. After the software is installed on the target host, you can run a configuration script that lets you specify network and database connection details for the cluster.

Prerequisites

Target hosts and the network that connects them must meet the requirements specified in "Cloud Director Hardware and Software Requirements," on page 10. If you intend to create a Cloud Director cluster that includes multiple hosts, each host must mount the shared transfer service storage at \$VCLOUD_HOME/data/transfer.

Procedure

- 1 Log in to the target host as root.
- 2 Download the installation file to the target host.

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

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 command:

chmod u+x installation-file

where installation-file is the full pathname to the VMware Cloud Director installation file.

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

To run the installation file, you must type its full pathname (for example *./installation_file*). The installation file includes an installation script and an embedded RPM package.

The installer verifies that the host meets all requirements, unpacks the VMware Cloud Director RPM package, and installs the software.

What to do next

After the software is installed, the installer prompts you to run the configuration script.

- To run the configuration script now, type y and press Enter.
- To 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 23.

Configure Network and Database Connections

After Cloud Director software is installed on the host, the installer prompts you to run a script that configures network and database connection details.

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

/opt/vmware/cloud-director/bin/configure

The configuration script creates network and database connections for a single Cloud Director server host. 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 Cloud Director server host. For more information, see "About the Cloud Director Database," on page 9 and "Cloud Director Hardware and Software Requirements," on page 10.
- Have the following information available:
 - Location and password of the keystore file that includes the SSL certificates for this host. See "Create and Import a Signed SSL Certificate," on page 16. 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.
 - The hostname or IP address of the database server host.
 - The database name and connection port.
 - Database user credentials (user name and password). The database user you specify must have specific rights in the database. See "About the Cloud Director Database," on page 9.

Procedure

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

Each member of a cluster 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]: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 Enter the keystore and certificate passwords.

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

- 4 Services in each Cloud Director cell log audit messages to the Cloud Director database, where they are preserved for 90 days. If you want to preserve audit messages for longer, you can configure Cloud Director services to send audit messages to the syslog utility in addition to the Cloud Director database.
 - To log audit messages to both syslog and the Cloud Director database., enter the syslog host name or IP address.
 - To log audit messages only to the Cloud 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 Cloud 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 listens on the specified host. 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 Type the hostname or IP address of the database server host.

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

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

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

8 Type the database name, or press Enter to accept the default value.

Enter the database name [default=vcloud]: Using default value "vcloud" for database name.

9 Type the database service name, or press Enter to accept the default value.

Enter the database service name [default=oracle]: Using default value "oracle" for database service name.

10 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 host to it.
- 2 It offers to start Cloud Director services on this host.
- 3 It displays a URL at which you can connect to the Cloud Director Setup wizard after Cloud Director service have started.

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 Cloud Director server has been started you will be able to
access the first-time setup wizard at this URL:
http://mycloud.example.com
```

Would you like to start the Cloud 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 Cloud 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.

Cloud Director configuration is now complete. Exiting...

What to do next

To add more hosts to this cluster, see "Install Cloud Director Software on Additional Server Hosts," on page 26.

Note Database connection information and other reusable responses you supplied during configuration are preserved in a file located at /opt/vmware/cloud-director/etc/responses.properties on this server host. Save a copy of the file in a location that is accessible to all target hosts. When you configure additional server hosts for this cluster, you must use the response file to supply configuration parameters that all host share. If you move or copy the file, be sure that the file name, permissions, and ownership do not change. It must be owned by vcloud.vcloud and have read and write permission for the owner or it cannot be used by the configuration script.

After Cloud Director services are running on all server hosts, you can open the Cloud Director Setup wizard at the URL displayed when the script completes. See Chapter 3, "Cloud Director Setup," on page 29.

Start Cloud Director Services

After you complete installation and database connection setup on a server host, you can start the Cloud Director services on that host.

The configuration script prompts you to start Cloud Director services. If you choose not to have the script start these services, or if you stopped the services and want to restart them without rebooting the host, you can start them yourself any time after the configuration script finishes. These services must be running before you can complete and initialize the installation.

Cloud Director services start automatically whenever a server host is rebooted.

Procedure

- 1 Log in to the target host as root.
- 2 Open a console, shell, or terminal window and run the service command.

service vmware-vcd start

Install Cloud Director Software on Additional Server Hosts

After you install and configure Cloud Director software on the first server host, you can add more server hosts to the cluster. All server hosts in a cluster must be configured with the same database connection details. To ensure that this requirement is met, use the response file created by the first server installation to supply this information during installation of the remaining hosts in the cluster.

Prerequisites

All additional server hosts must be able to access the response file. This file is saved in /opt/vmware/clouddirector/etc/responses.properties on the first server host that you install. Save a copy of this file in a location that is accessible to all target hosts, so that you can use it whenever you add a host to the cluster.

Procedure

- 1 Log in to the target host as root.
- 2 Download the installation file to the target host.

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

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 command:

chmod u+x installation-file

where installation-file is the full pathname to the VMware Cloud Director installation file.

4 Run the installation file, supplying the pathname of the response file that you saved after you installed the first server host.

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 server hosts that you want to add to this cluster.

The installer prompts for 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 on and Cloud Director services are running on all server hosts, you can open the Cloud Director Setup wizard at the URL that appears when the script completes. See Chapter 3, "Cloud Director Setup," on page 29.

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
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/cloud-director/deploymentPackageCreator/createSysprepPackage.sh SysprepBinariesDirectory command.

For example, /opt/vmware/clouddirector/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/cloud-director/guestcustomization/vcloud_sysprep.properties
/opt/vmware/cloud-director/guestcustomization/windows_deployment_package_sysprep.cab
root@next_cell_IP:/opt/vmware/cloud-director/guestcustomization

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

Uninstall VMware Cloud Director Software

Use the Linux rpm command to uninstall Cloud Director software from an individual server host.

Procedure

- 1 Log in to the target host as root.
- 2 Unmount the transfer service storage, typically mounted at /opt/vmware/clouddirector/data/transfer.

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

rpm -e vmware-cloud-director

Cloud Director Setup

After all hosts in the Cloud Director cluster are installed and connected to the database, you can use the Cloud Director Setup wizard to initialize the cluster's database with a license key, system administrator account, and related information. After this wizard completes, you can use the Cloud Director Web Console to complete the initial provisioning of your Cloud.

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

Prerequisites

Complete the installation of all Cloud Director hosts, and verify that Cloud Director services have started on all hosts.

Procedure

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

NOTE To discover the URL of the Cloud Director Setup wizard after the script has exited, look up the fully qualified domain name associated with the IP address you specified for the HTTP service during installation of the first server host 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.

- 2 Navigate through the Wizard pages, providing the information requested.
 - Click Next to save your choices and go to the next page.
 - Click **Previous** to save your choices and go to the previous page.

This chapter includes the following topics:

- "Review the License Agreement," on page 30
- "Enter the License Key," on page 30
- "Create the System Administrator Account," on page 30
- "Specify System Settings," on page 31
- "Ready to Log In," on page 31

Review the License Agreement

Before you can configure this Cloud Director cluster, you must review and accept the end user license agreement.

Procedure

- 1 Review the license agreement.
- 2 Accept or reject the agreement.
 - To accept the license agreement, click Yes, I accept the terms in the license agreement.
 - To reject the license agreement, click No, I do not accept the terms in the license agreement.

If you reject the license agreement, you cannot proceed with the wizard.

3 Click **Next** to save your choices and go to the next page.

Enter the License Key

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

The Cloud Director product serial number is not the same as your vCenter server license key. To operate a Cloud, you need a Cloud 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 VMware Cloud Director product serial number from the VMware License Portal.
- 2 Type the product serial number in the **Product serial number** text box.
- 3 Click **Next** to save your choices and go to the next page.

Create the System Administrator Account

Specify the user name, password, and contact information of the user to designate as the Cloud Director system administrator.

The Cloud Director system administrator has superuser privileges throughout the Cloud. You create the initial system administrator account during Cloud 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.
- 5 Click **Next** to save your choices and go to the next page.

Specify System Settings

Specify the system settings that control how this Cloud Director installation interacts with vSphere and vShield Manager.

During the configuration process, the wizard creates a folder in vCenter for Cloud Director to use and specifies an installation ID for the supporting vShield Manager to use when creating MAC addresses for virtual NICs.

Procedure

- 1 Enter a name for this Cloud Director installation vCenter folder in the **System name** field.
- 2 (Optional) If more than one installation of vShield Manager is connected to this network, select a unique installation ID for the vShield Manager configured to work with this Cloud Director installation using the **Installation ID** control.
- 3 Click **Next** to save your choices and go to the next page.

Ready to Log In

After you provide all of the information that the installation wizard requires, you can confirm your settings and complete the wizard. After the wizard finishes, the login screen of the Cloud 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

The Cloud Director Web Console requires access to the installations of vCenter and vShield Manager that you want to configure as part of this Cloud Director. These installations should be running and configured to work with each other before you finish this task. For more information, see "Cloud Director Hardware and Software Requirements," on page 10.

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 setting information you provided, then starts the Cloud Director Web Console and displays its login screen.

What to do next

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

Cloud Director Installation and Configuration Guide

Index

В

browsers, supported 13

С

certificate self-signed **18** signed **16** cluster, to create **21** configuration, confirm settings and complete **31**

D

database about 9 connection details 23 supported platforms 10

G

guest customization, preparing 27

I

installation of first host 22 of more hosts 26 to configure 29 uninstalling 27 Installation and capacity planning 8 architecture diagram 7 overview of 7 Installation ID, to specify 31

Κ

keystore 15

L

license agreement 30

Μ

Microsoft Sysprep 27

Ρ

product serial number to enter **30** to obtain **30**

S

services, to start **25** System Administrator account, to create **30** System Name, to specify 31

Т

Technical Support, to obtain 5

V

vCenter, supported releases vShield Manager installing and configuring supported releases Cloud Director Installation and Configuration Guide