



# CloudPlatform

(powered by Apache CloudStack)

# Installation Guide

For CloudPlatform Version 3.0.3 - 3.0.5

Revised October 23, 2012 1:56 PM Pacific

© 2011, 2012 Citrix Systems, Inc. All rights reserved. Specifications are subject to change without notice. Citrix Systems, Inc., the Citrix logo, Citrix XenServer, Citrix XenCenter, and CloudPlatform are trademarks or registered trademarks of Citrix Systems, Inc. All other brands or products are trademarks or registered trademarks of their respective holders.

# Contents

---

What's In This Guide .....	11
What Is CloudPlatform? .....	12
What Can CloudPlatform Do? .....	13
Deployment Architecture Overview .....	14
Management Server Overview .....	14
Cloud Infrastructure Overview .....	16
Networking Overview .....	16
Overview of Installation Steps .....	18
System Requirements .....	19
Management Server, Database, and Storage System Requirements .....	19
Host/Hypervisor System Requirements .....	19
Management Server Single-Node Installation .....	21
Prepare the Operating System .....	21
Install the Management Server .....	23
Install and Configure the Database .....	23
About Password and Key Encryption .....	25
Prepare NFS Shares .....	26
Using a Separate NFS Server .....	26
Using the Management Server as the NFS Server .....	27
Prepare the System VM Template .....	29
Single-Node Installation Complete! Next Steps .....	30
Management Server Multi-Node Installation .....	31
Prepare the Operating System .....	31
Install the First Management Server .....	32
Install and Configure the Database .....	34

About Password and Key Encryption .....	36
Prepare NFS Shares.....	36
Using a Separate NFS Server .....	37
Using the Management Server as the NFS Server .....	37
Prepare and Start Additional Management Servers .....	39
Prepare the System VM Template .....	40
Multi-Node Installation Complete! Next Steps .....	41
Log In to the CloudPlatform UI .....	42
End User's UI Overview.....	42
Root Administrator's UI Overview .....	42
Logging In as the Root Administrator .....	42
Provision Your Cloud Infrastructure .....	44
Change the Root Password .....	45
Add a Zone .....	46
About Zones.....	46
About Physical Networks .....	47
Configurable Characteristics of Physical Networks.....	47
Basic Zone Network Traffic Types.....	48
Basic Zone Guest IP Addresses .....	48
Advanced Zone Network Traffic Types .....	48
Advanced Zone Guest IP Addresses.....	49
Advanced Zone Public IP Addresses .....	49
System Reserved IP Addresses .....	49
Using Security Groups to Control Traffic to VMs .....	50
About Security Groups.....	50
Enabling Security Groups .....	51
Working With Security Groups .....	51

Adding a Zone .....	51
Basic Zone Configuration .....	52
Advanced Zone Configuration .....	56
Add More Pods (Optional) .....	61
About Pods.....	61
Adding a Pod.....	61
Add More Clusters (Optional) .....	63
About Clusters .....	63
Add Cluster: KVM or XenServer .....	63
Add Cluster: OVM .....	64
Add Cluster: vSphere .....	64
Add More Hosts (Optional) .....	67
About Hosts .....	67
Install Hypervisor Software on Hosts.....	67
Add Hosts to CloudPlatform (XenServer, KVM, or OVM) .....	68
Requirements for XenServer, KVM, and OVM Hosts .....	68
Adding a XenServer, KVM, or OVM Host .....	69
Add Hosts (vSphere) .....	70
Add Primary Storage.....	71
About Primary Storage .....	71
System Requirements for Primary Storage.....	71
Adding Primary Storage .....	71
Add Secondary Storage.....	73
About Secondary Storage .....	73
System Requirements for Secondary Storage .....	73
Adding Secondary Storage .....	73
Initialization and Testing.....	75

Citrix XenServer Installation for CloudPlatform .....	76
System Requirements for XenServer Hosts .....	76
XenServer Installation Steps .....	76
Configure XenServer dom0 Memory .....	77
Username and Password .....	77
Time Synchronization .....	77
Licensing .....	78
Getting and Deploying a License.....	78
Install CloudPlatform XenServer Support Package (CSP) .....	78
Primary Storage Setup for XenServer .....	79
iSCSI Multipath Setup for XenServer (Optional) .....	80
Physical Networking Setup for XenServer .....	80
Configuring Public Network with a Dedicated NIC for XenServer (Optional) .....	81
Configuring Multiple Guest Networks for XenServer (Optional) .....	81
Separate Storage Network for XenServer (Optional) .....	82
NIC Bonding for XenServer (Optional) .....	82
Upgrading XenServer Versions .....	84
VMware vSphere Installation and Configuration .....	87
System Requirements for vSphere Hosts .....	87
Preparation Checklist for VMware.....	88
vCenter Checklist .....	89
Networking Checklist for VMware .....	89
vSphere Installation Steps .....	90
ESXi Host setup .....	90
Physical Host Networking .....	91
Configure Virtual Switch .....	91
Configure vCenter Management Network .....	93

Extend Port Range for CloudPlatform Console Proxy .....	95
Configure NIC Bonding for vSphere .....	95
Configuring a vSphere Cluster with Nexus 1000v Virtual Switch .....	95
About Cisco Nexus 1000v Distributed Virtual Switch .....	95
Prerequisites and Guidelines .....	96
Nexus 1000v Virtual Switch Preconfiguration .....	96
Enabling Nexus Virtual Switch in CloudPlatform .....	100
Configuring Nexus 1000v Virtual Switch in CloudPlatform .....	101
Removing Nexus Virtual Switch .....	102
Storage Preparation for vSphere (iSCSI only) .....	103
Enable iSCSI initiator for ESXi hosts .....	103
Add iSCSI target .....	105
Create an iSCSI datastore .....	106
Multipathing for vSphere (Optional) .....	106
Add Hosts or Configure Clusters (vSphere) .....	107
KVM Installation and Configuration .....	108
Supported Operating Systems .....	108
System Requirements for KVM Hosts .....	108
KVM Installation Steps .....	109
Installing the CloudPlatform Agent on a KVM Host .....	109
Physical Network Configuration for KVM .....	110
Time Synchronization .....	111
Primary Storage Setup for KVM (Optional) .....	111
Oracle VM (OVM) Installation and Configuration .....	112
System Requirements for OVM Hosts .....	112
OVM Installation Overview .....	112
Installing OVM on the Host(s) .....	112

Primary Storage Setup for OVM .....	113
Set Up Host(s) for System VMs .....	113
Choosing a Deployment Architecture .....	114
Small-Scale Deployment .....	114
Large-Scale Redundant Setup .....	115
Separate Storage Network .....	116
Multi-Node Management Server .....	116
Multi-Site Deployment .....	117
Choosing a Hypervisor: Supported Features .....	121
Network Setup .....	123
Basic and Advanced Networking .....	123
VLAN Allocation Example .....	124
Example Hardware Configuration .....	125
Dell 62xx .....	125
Cisco 3750 .....	125
Layer-2 Switch .....	126
Hardware Firewall .....	127
Generic Firewall Provisions .....	127
External Guest Firewall Integration for Juniper SRX (Optional) .....	127
Management Server Load Balancing .....	130
Topology Requirements .....	131
Security Requirements .....	131
Runtime Internal Communications Requirements .....	131
Storage Network Topology Requirements .....	131
External Firewall Topology Requirements .....	131
Advanced Zone Topology Requirements .....	131
XenServer Topology Requirements .....	132

---

VMware Topology Requirements .....	132
KVM Topology Requirements .....	132
External Guest Load Balancer Integration (Optional) .....	132
Guest Network Usage Integration for Traffic Sentinel .....	133
Setting Zone VLAN and Running VM Maximums .....	134
Storage Setup.....	135
Small-Scale Setup.....	135
Secondary Storage .....	135
Example Configurations .....	135
Additional Installation Options .....	139
Edit the Global Configuration Settings (Optional) .....	139
Installing the Usage Server (Optional) .....	140
Requirements for Installing the Usage Server .....	140
Steps to Install the Usage Server .....	141
SSL (Optional).....	141
Database Replication (Optional) .....	141
Failover .....	143
Amazon Web Services API Compatibility (Optional).....	143
System Requirements for AWS API Compatibility .....	144
Enabling AWS API Compatibility .....	144
AWS API User Setup.....	145
Ensuring AWS API Command Completion: Timeouts .....	145
Supported AWS API Commands and Parameters .....	146
Best Practices.....	153
Process Best Practices.....	153
Setup Best Practices.....	153
Maintenance Best Practices.....	153

---

Troubleshooting.....	155
Checking the Management Server Log .....	155
Troubleshooting the Secondary Storage VM .....	155
Running a Diagnostic Script .....	155
Checking the Log Files.....	156
Troubleshooting AWS API Compatibility .....	156
VLAN Issues.....	156
Console Proxy VM Issues .....	156
Binary Logging Error when Upgrading Database .....	157
Can't Add Host .....	157
Preparation Checklists .....	158
Management Server Checklist .....	158
Database Checklist.....	159
Storage Checklist.....	160
Contacting Support .....	161

## What's In This Guide

---

This Guide is for those who have already gone through a design phase and planned a more sophisticated CloudPlatform deployment, or those who are ready to start scaling up a trial cloud that was set up earlier using the Basic Installation Wizard and Trial Installation Guide.

With the procedures in this Installation Guide, you can start using the more powerful features of CloudPlatform, such as advanced VLAN networking, high availability, additional network elements such as load balancers and firewalls, and support for multiple hypervisors including Citrix XenServer, KVM, and VMware vSphere.

# What Is CloudPlatform?

CloudPlatform™ is an open source software platform that pools computing resources to build public, private, and hybrid Infrastructure as a Service (IaaS) clouds. CloudPlatform manages the network, storage, and compute nodes that make up a cloud infrastructure. Use CloudPlatform to deploy, manage, and configure cloud computing environments.

Typical users are service providers and enterprises. With CloudPlatform, you can:

- Set up an on-demand, elastic cloud computing service. Service providers can sell self-service virtual machine instances, storage volumes, and networking configurations over the Internet.
- Set up an on-premise private cloud for use by employees. Rather than managing virtual machines in the same way as physical machines, with CloudPlatform an enterprise can offer self-service virtual machines to users without involving IT departments.

## Who Should Read This

If you are new to CloudPlatform or you want to learn more about concepts before installing and running it, read this overview.

If you just want to get started, you can skip to Overview of Installation Steps on page 18.



# What Can CloudPlatform Do?

---

## Multiple Hypervisor Support

CloudPlatform works with a variety of hypervisors. A single cloud deployment can contain multiple hypervisor implementations. You have the complete freedom to choose the right hypervisor for your workload. CloudPlatform is designed to work with open source Xen and KVM hypervisors as well as enterprise-grade hypervisors such as Citrix XenServer, VMware vSphere, and Oracle VM (OVM).

## Massively Scalable Infrastructure Management

CloudPlatform can manage tens of thousands of servers installed in multiple geographically distributed datacenters. The centralized management server scales linearly, eliminating the need for intermediate cluster-level management servers. No single component failure can cause cloud-wide outage. Periodic maintenance of the management server can be performed without affecting the functioning of virtual machines running in the cloud.

## Automatic Configuration Management

CloudPlatform automatically configures each guest virtual machine's networking and storage settings.

CloudPlatform internally manages a pool of virtual appliances to support the cloud itself. These appliances offer services such as firewalling, routing, DHCP, VPN access, console proxy, storage access, and storage replication. The extensive use of virtual appliances simplifies the installation, configuration, and ongoing management of a cloud deployment.

## Graphical User Interface

CloudPlatform offers an administrator's Web interface, used for provisioning and managing the cloud, as well as an end-user's Web interface, used for running VMs and managing VM templates. The UI can be customized to reflect the desired service provider or enterprise look and feel.

## API and Extensibility

CloudPlatform provides an API that gives programmatic access to all the management features available in the UI. The API is maintained and documented. This API enables the creation of command line tools and new user interfaces to suit particular needs. See the Developer's Guide and API Reference, both available at <http://support.citrix.com/product/cs>.

The CloudPlatform platform pluggable allocation architecture allows the creation of new types of allocators for the selection of storage and Hosts. See the Allocator Implementation Guide ([http://docs.cloudstack.org/CloudStack\\_Documentation/Allocator\\_Implementation\\_Guide](http://docs.cloudstack.org/CloudStack_Documentation/Allocator_Implementation_Guide)).

## High Availability

The CloudPlatform platform has a number of features to increase the availability of the system. The Management Server itself may be deployed in a multi-node installation where the servers are load balanced. MySQL may be configured to use replication to provide for a manual failover in the event of database loss. For the Hosts, the

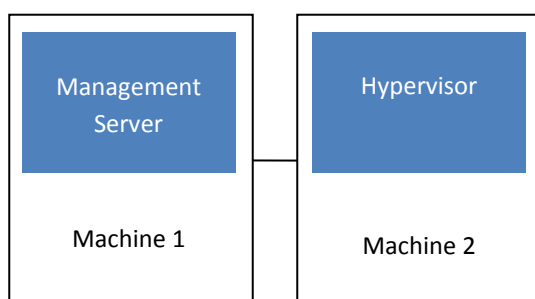
CloudPlatform platform supports NIC bonding and the use of separate networks for storage as well as iSCSI Multipath.

## Deployment Architecture Overview

---

A CloudPlatform installation consists of two parts: the Management Server and the cloud infrastructure that it manages. When you set up and manage a CloudPlatform cloud, you provision resources such as hosts, storage devices, and IP addresses into the Management Server, and the Management Server manages those resources.

The minimum installation consists of one machine running the CloudPlatform Management Server and another machine to act as the cloud infrastructure (in this case, a very simple infrastructure consisting of one host running hypervisor software).



**Simplified view of a basic deployment**

A more full-featured installation consists of a highly-available multi-node Management Server installation and up to thousands of hosts using any of several advanced networking setups. For information about deployment options, see [Choosing a Deployment Architecture](#) on page 114.

## Management Server Overview

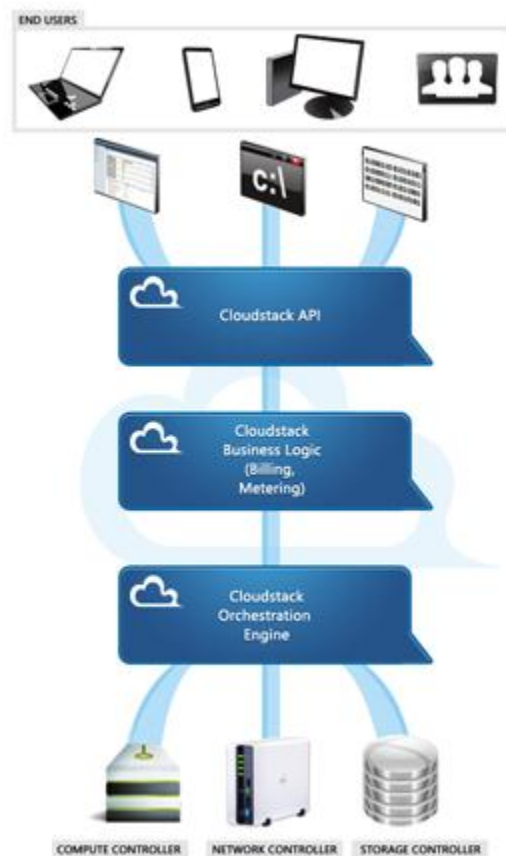
The Management Server is the CloudPlatform software that manages cloud resources. By interacting with the Management Server through its UI or API, you can configure and manage your cloud infrastructure.

The Management Server runs on a dedicated server or VM. It controls allocation of virtual machines to hosts and assigns storage and IP addresses to the virtual machine instances. The CloudPlatform Management Server runs in a Tomcat container and requires a MySQL database for persistence.

The machine must meet the system requirements described in [System Requirements](#) on page 19.

#### The Management Server:

- Provides the web user interface for the administrator and a reference user interface for end users.
- Provides the APIs for the CloudPlatform platform.
- Manages the assignment of guest VMs to particular hosts.
- Manages the assignment of public and private IP addresses to particular accounts.
- Manages the allocation of storage to guests as virtual disks.
- Manages snapshots, templates, and ISO images, possibly replicating them across data centers.
- Provides a single point of configuration for the cloud.



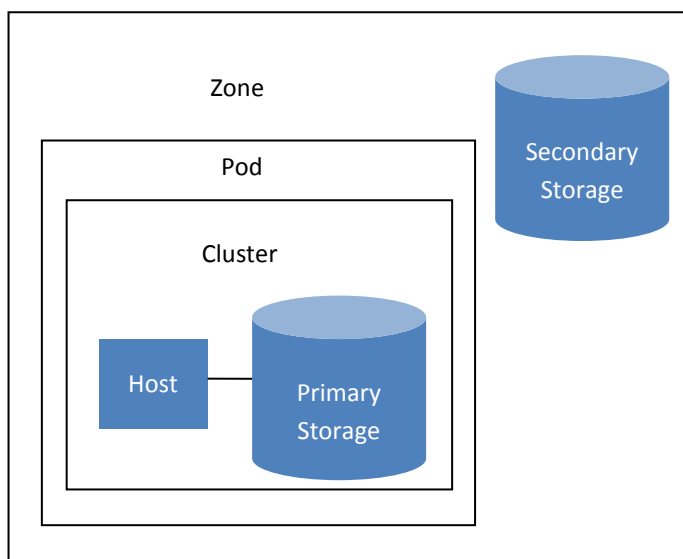
#### Management Server Components

For additional options, including how to set up a multi-node management server installation, see [Choosing a Deployment Architecture](#) on page 114.

## Cloud Infrastructure Overview

The Management Server manages one or more zones (typically, datacenters) containing host computers where guest virtual machines will run. The cloud infrastructure is organized as follows:

- **Zone:** Typically, a zone is equivalent to a single datacenter. A zone consists of one or more pods and secondary storage. See About Zones on page 46.
- **Pod:** A pod is usually one rack of hardware that includes a layer-2 switch and one or more clusters. See About Pods on page 61.
- **Cluster:** A cluster consists of one or more hosts and primary storage. See About Clusters on page 63.
- **Host:** A single compute node within a cluster. The hosts are where the actual cloud services run in the form of guest virtual machines. See About Hosts on page 67.
- **Primary storage** is associated with a cluster, and it stores the disk volumes for all the VMs running on hosts in that cluster. See About Primary Storage on page 71.
- **Secondary storage** is associated with a zone, and it stores templates, ISO images, and disk volume snapshots. See About Secondary Storage on page 73.



**Nested organization of a zone**

## Networking Overview

CloudPlatform offers two types of networking scenario:

- **Basic.** For AWS-style networking. Provides a single network where guest isolation can be provided through layer-3 means such as security groups (IP address source filtering).
- **Advanced.** For more sophisticated network topologies. This network model provides the most flexibility in defining guest networks.

For more details, see Network Setup on page 123.

# Overview of Installation Steps

---

## Prepare

1. Make sure you have the required hardware ready (p. 19)
2. (Optional) Fill out the preparation checklists (p. 158)

## Install the CloudPlatform software

3. Install the CloudPlatform Management Server (single-node, p. 21, or multi-node, p. 31)
4. Log in to the CloudPlatform UI (p. 42)

## Provision your cloud infrastructure

5. Add a zone. Includes the first pod, cluster, and host (p. 46)
6. Add more pods (p. 61)
7. Add more clusters (p. 63)
8. Add more hosts (p. 67)
9. Add more primary storage (p. 71)
10. Add more secondary storage (p. 73)

## Try using the cloud

11. Initialization and testing (p. 75)

For anything more than a simple trial installation, you will need guidance for a variety of configuration choices. It is strongly recommended that you read the following:

- Choosing a Deployment Architecture on page 114
- Choosing a Hypervisor: Supported Features on page 121
- Network Setup on page 123
- Storage Setup on page 135
- Best Practices on page 153

# System Requirements

---

## Management Server, Database, and Storage System Requirements

---

The machine or machines that will run the Management Server and MySQL database must meet the following requirements. The same machines can also be used to provide primary and secondary storage, such as via localdisk or NFS. The Management Server may be placed on a virtual machine.

- Operating system:
  - Preferred: RHEL 6.2+ 64-bit (<https://access.redhat.com/downloads>) or CentOS 6.2+ 64-bit ([http://isoredirect.centos.org/centos/6/isos/x86\\_64/](http://isoredirect.centos.org/centos/6/isos/x86_64/))
  - Also supported (v3.0.3 and greater): RHEL and CentOS 5.4-5.x 64-bit
  - It is highly recommended that you purchase a RHEL support license. Citrix support can not be responsible for helping fix issues with the underlying OS.
- 64-bit x86 CPU (more cores results in better performance)
- 4 GB of memory
- 250 GB of local disk (more results in better capability; 500 GB recommended)
- At least 1 NIC
- Statically allocated IP address
- Fully qualified domain name as returned by the hostname command

## Host/Hypervisor System Requirements

---

The hypervisor is where the cloud services run in the form of guest virtual machines. For a small-scale setup, you need only one machine that meets the following requirements. In the smallest possible setup, this can be the same machine where you are running the Management Server. More commonly, in a production cloud, the hypervisor software does not run on the same machine with the Management Server.

- Must be 64-bit and must support HVM (Intel-VT or AMD-V enabled).
- 64-bit x86 CPU (more cores results in better performance)
- Hardware virtualization support required
- 4 GB of memory
- 36 GB of local disk
- At least 1 NIC
- Statically allocated IP Address
- Latest hotfixes applied to hypervisor software

- When you deploy CloudPlatform, the hypervisor host must not have any VMs already running

Hosts have additional requirements depending on the hypervisor. See the requirements in the Installation section for your chosen hypervisor:

- Citrix XenServer Installation for CloudPlatform on page 76
- VMware vSphere Installation and Configuration on page 87
- KVM Installation and Configuration on page 108
- Oracle VM (OVM) Installation and Configuration on page 112

**WARNING**

Be sure you fulfill the additional hypervisor requirements and installation steps provided in this Guide. Hypervisor hosts must be properly prepared to work with CloudPlatform.

# Management Server Single-Node Installation

---

This section describes installing a single Management Server and installing MySQL on the same node. The machine must meet the system requirements described in System Requirements on page 19.

If you prefer to set up a Management Server with multiple nodes for high availability, see Management Server Multi-Node Installation on page 31.

The procedure for the installation is:

1. Prepare the Operating System
2. Install the Management Server
3. Install and Configure the Database
4. Prepare NFS Shares
5. Prepare the System VM Template

## WARNING

For the sake of security, be sure the public Internet can not access port 8096 or port 8250 on the Management Server.

## Prepare the Operating System

---

The OS must be prepared to host the Management Server using the following steps.

1. Log in to your OS as root.
2. Check for a fully qualified hostname.

```
# hostname --fqdn
```

This should return a fully qualified hostname such as "kvm1.lab.example.org". If it does not, edit /etc/hosts so that it does.

3. Set SELinux to be permissive by default.
  - a. Check to see whether SELinux is installed on your machine. If not, you can skip to step 4.  
In RHEL or CentOS, SELinux are installed and enabled by default. You can verify this with:

```
# rpm -qa | grep selinux
```

- b. Set the SELINUX variable in /etc/selinux/config to "permissive". This ensures that the permissive setting will be maintained after a system reboot.

```
# vi /etc/selinux/config
```

- c. Then set SELinux to permissive starting immediately, without requiring a system reboot.

In CentOS:

```
# setenforce permissive
```

In RHEL:

```
# setenforce 0
```

4. Make sure that the machine can reach the Internet.

```
# ping www.google.com
```

5. (CentOS) If you are installing everything on a single machine (Management Server, database, KVM hypervisor, etc.), be sure to configure the network and put the network configuration file into `/etc/sysconfig/network-scripts/ifcfg-<yourPhysicalDeviceName>`. Without this configuration, CloudPlatform will not be able to create the bridge.

NOTE: This single-machine style of installation is recommended only for a trial installation.

6. (RHEL 6.2) If you do not have a Red Hat Network account, you need to prepare a local Yum repository.
  - a. If you are working with a physical host, insert the RHEL 6.2 installation CD. If you are using a VM, attach the RHEL6 ISO.
  - b. Mount the CDROM to `/media`.
  - c. Create a repo file at `/etc/yum.repos.d/rhel6.repo`. In the file, insert the following lines:

```
[rhel]
name=rhel6
baseurl=file:///media
enabled=1
gpgcheck=0
```

7. Turn on NTP for time synchronization.

- a. Install NTP.

```
# yum install ntp
```

- b. Edit the NTP configuration file to point to your NTP server.

```
# vi /etc/ntp.conf
```

Add one or more server lines in this file with the names of the NTP servers you want to use. For example:

```
server 0.xenserver.pool.ntp.org
server 1.xenserver.pool.ntp.org
server 2.xenserver.pool.ntp.org
server 3.xenserver.pool.ntp.org
```

- c. Restart the NTP client.

```
# service ntpd restart
```

- d. Make sure NTP will start again upon reboot.

```
# chkconfig ntpd on
```

**TIP**

NTP is required to synchronize the clocks of the servers in your cloud.

## Install the Management Server

This section describes the procedure for performing a single node install where the Management Server and MySQL are on a single, shared OS instance. If you have multiple Management Servers or if you want to have MySQL on a separate server, see Management Server Multi-Node Install on page 31.

1. Download the CloudPlatform Management Server onto the host where it will run from the following link. If your operating system is CentOS, use the download file for RHEL.

<https://www.citrix.com/English/ss/downloads/>

You will need a [MyCitrix account](#).

2. Install the CloudPlatform packages. You should have a file in the form of "CloudStack-VERSION-N-OSVERSION.tar.gz". Untar the file and then run the install.sh script inside it. Replace the file and directory names below with those you are using:

```
# tar xzf CloudStack-VERSION-N-OSVERSION.tar.gz
# cd CloudStack-VERSION-N-OSVERSION
# ./install.sh
```

You should see a few messages as the installer prepares, followed by a list of choices.

3. Choose M to install the Management Server software.

```
> M
```

Wait for a message like "Complete! Done."

4. When the installation is finished, run the following commands to start essential services (the commands might be different depending on your OS).

```
# service rpcbind start
# service nfs start
# chkconfig nfs on
# chkconfig rpcbind on
```

5. Continue with Install and Configure the Database on page 23.

## Install and Configure the Database

1. If you already have a version of MySQL installed on the Management Server node, make one of the following choices, depending on what version of MySQL it is. The most recent version tested with CloudPlatform is 5.1.58.
  - If you already have installed MySQL version 5.1.58 or later, skip to step 4.
  - If you have installed a version of MySQL earlier than 5.1.58, you can either skip to step 4 or uninstall MySQL and proceed to step 2 to install a more recent version.

### WARNING

It is important that you make the right choice of database version. Never downgrade an existing MySQL installation that is being used with CloudPlatform.

2. On the same computer where you installed the CloudPlatform Management Server, re-run install.sh.

```
# ./install.sh
```

You should see a few messages as the installer prepares, followed by a list of choices.

3. Choose D to install the MySQL server from the distribution's repo.

```
> D
```

Troubleshooting: If you do not see the D option, you already have MySQL installed. Please go back to step 1.

4. Edit the MySQL configuration (/etc/my.cnf or /etc/mysql/my.cnf, depending on your OS) and insert the following lines in the [mysqld] section. You can put these lines below the datadir line. The max\_connections parameter should be set to 350 multiplied by the number of Management Servers you are deploying. This example assumes one Management Server.

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=350
log-bin=mysql-bin
binlog-format = 'ROW'
```

**NOTE:** The binlog-format variable is supported in MySQL versions 5.1 and greater. It is not supported in MySQL 5.0. In some versions of MySQL, an underscore character is used in place of the hyphen in the variable name. For the exact syntax and spelling of each variable, consult the documentation for your version of MySQL.

5. Restart the MySQL service, then invoke MySQL as the root user.

```
# service mysqld restart
# mysql -u root
```

6. Best Practice: On RHEL and CentOS, MySQL does not set a root password by default. It is very strongly recommended that you set a root password as a security precaution. Run the following commands, and substitute your own desired root password.

```
mysql> SET PASSWORD = PASSWORD('password');
```

From now on, start MySQL with `mysql -p` so it will prompt you for the password.

7. To grant access privileges to remote users, perform the following steps.

- a. Run the following commands from the mysql prompt:

```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' WITH GRANT OPTION;
mysql> exit
```

- b. Restart the MySQL service.

```
# service mysqld restart
```

- c. Open the MySQL server port (3306) in the firewall to allow remote clients to connect.

```
# iptables -I INPUT -p tcp --dport 3306 -j ACCEPT
```

- d. Edit the `/etc/sysconfig/iptables` file and add the following line at the beginning of the INPUT chain.

```
-A INPUT -p tcp --dport 3306 -j ACCEPT
```

8. Set up the database. The following command creates the cloud user on the database.

- In `dbpassword`, specify the password to be assigned to the cloud user. You can choose to provide no password.
- In `deploy-as`, specify the username and password of the user deploying the database. In the following command, it is assumed the root user is deploying the database and creating the cloud user.
- (Optional) For `encryption_type`, use `file` or `web` to indicate the technique used to pass in the database encryption password. Default: `file`. See About Password and Key Encryption on page 25.
- (Optional) For `management_server_key`, substitute the default key that is used to encrypt confidential parameters in the CloudPlatform properties file. Default: `password`. It is highly recommended that you replace this with a more secure value. See About Password and Key Encryption on page 25.
- (Optional) For `database_key`, substitute the default key that is used to encrypt confidential parameters in the CloudPlatform database. Default: `password`. It is highly recommended that you replace this with a more secure value. See About Password and Key Encryption on page 25.

```
# cloud-setup-databases cloud:<dbpassword>@localhost --deploy-as=root:<password> -e  
<encryption_type> -m <management_server_key> -k <database_key>
```

When this script is finished, you should see a message like “CloudPlatform has successfully initialized the database.”

9. If you are running the KVM hypervisor on the same machine with the Management Server, edit `/etc/sudoers` and add the following line:

```
Defaults:cloud !requiretty
```

NOTE: This type of single-machine setup is recommended only for a trial installation.

10. Now that the database is set up, you can finish configuring the OS for the Management Server. This command will set up iptables, sudoers, and start the Management Server.

```
# cloud-setup-management
```

You should see the message “CloudPlatform Management Server setup is done.”

11. Continue to Prepare NFS Shares on page 26.

## About Password and Key Encryption

CloudPlatform stores several sensitive passwords and secret keys that are used to provide security. These values are always automatically encrypted:

- Database secret key
- Database password
- SSH keys
- Compute node root password
- VPN password
- User API secret key

➤ VNC password

CloudPlatform uses the Java Simplified Encryption (JASYPT) library. The data values are encrypted and decrypted using a database secret key, which is stored in one of CloudPlatform's internal properties files along with the database password. The other encrypted values listed above (SSH keys, etc.) are in the CloudPlatform internal database.

Of course, the database secret key itself can not be stored in the open – it must be encrypted. How then does CloudPlatform read it? A second secret key must be provided from an external source during Management Server startup. This key can be provided in one of two ways: loaded from a file or provided by the CloudPlatform administrator. The CloudPlatform database has a new configuration setting that lets it know which of these methods will be used. If the encryption type is set to “file,” the key must be in a file in a known location. If the encryption type is set to “web,” the administrator runs the utility `com.cloud.utils.crypt.EncryptionSecretKeySender`, which relays the key to the Management Server over a known port.

The encryption type, database secret key, and Management Server secret key are set during CloudPlatform installation. They are all parameters to the CloudPlatform database setup script (`cloud-setup-databases`). The default values are file, password, and password. It is, of course, highly recommended that you change these to more secure keys.

## Prepare NFS Shares

---

CloudPlatform needs a place to keep primary and secondary storage (see Cloud Infrastructure Overview on page 16). Both of these can be NFS shares. This section tells how to set up the NFS shares before adding the storage to CloudPlatform. A production installation typically uses a separate NFS server, but you can also use the Management Server node as the NFS server.

For primary storage, you can use iSCSI instead.

The requirements for primary and secondary storage are described in:

- About Primary Storage on page 71
- About Secondary Storage on page 73

## Using a Separate NFS Server

This section tells how to set up NFS shares for primary and secondary storage on an NFS server running on a separate node from the Management Server.

The exact commands for the following steps may vary depending on your operating system version.

1. On the storage server, create an NFS share for secondary storage.
2. Export it with `rw,async,no_root_squash`. For example:

```
# vi /etc/exports
```

**WARNING**

(KVM only) Ensure that no volume is already mounted at your NFS mount point.

Insert the following line.

```
/export *(rw,async,no_root_squash)
```

3. Export the /export directory.

```
# exportfs -a
```

4. On the management server, create a mount point. For example:

```
# mkdir -p /mnt/secondary
```

5. Mount the secondary storage on your Management Server. Replace the example NFS server name and NFS share paths below with your own.

```
# mount -t nfs nfsservername:/nfs/share/secondary /mnt/secondary
```

6. If you are using NFS for primary storage as well, repeat these steps with a different NFS share and mount point.
7. Continue with Prepare the System VM Template on page 29.

## Using the Management Server as the NFS Server

This section tells how to set up NFS shares for primary and secondary storage on the same node with the Management Server. It is assumed that you will have less than 16TB of storage on the host.

The exact commands for the following steps may vary depending on your operating system version.

1. On the Management Server host, create two directories that you will use for primary and secondary storage.

For example:

```
# mkdir -p /export/primary
# mkdir -p /export/secondary
```

2. To configure the new directories as NFS exports, edit /etc/exports.

```
# vi /etc/exports
```

Insert the following line.

```
/export *(rw,async,no_root_squash)
```

3. Export the /export directory.

```
# exportfs -a
```

4. Edit the /etc/sysconfig/nfs file and uncomment the following lines.

```
LOCKD_TCP_PORT=32803
LOCKD_UDP_PORT=32769
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=662
STATD_OUTGOING_PORT=2020
```

5. Edit the `/etc/sysconfig/iptables` file and add the following lines at the beginning of the INPUT chain.

```
-A INPUT -m state --state NEW -p udp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 2049 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 32803 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 32769 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 662 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 662 -j ACCEPT
```

6. Run the following commands:

```
# service iptables restart
# service iptables save
```

7. If NFS v4 communication is used between client and server, add your domain to `/etc/ldapd.conf` on both the hypervisor host and Management Server.

```
# vi /etc/ldapd.conf
```

Remove the character `#` from the beginning of the Domain line in `ldapd.conf` and replace the value in the file with your own domain. In the example below, the domain is `company.com`.

```
Domain = company.com
```

8. Reboot the Management Server host.

Two NFS shares called `/export/primary` and `/export/secondary` are now set up.

9. It is recommended that you test to be sure the previous steps have been successful.

- a. Log in to the hypervisor host.
- b. Be sure NFS and `rpcbind` are running. The commands might be different depending on your OS. For example (substitute your own management server name):

```
# service rpcbind start
# service nfs start
# chkconfig nfs on
# chkconfig rpcbind on
# reboot
```

- c. Log back in to the hypervisor host and try to mount the `/export` directories. For example (substitute your own management server name):

```
# mkdir /primarymount
# mount -t nfs <management-server-name>:/export/primary /primarymount
# umount /primarymount
# mkdir /secondarymount
# mount -t nfs <management-server-name>:/export/secondary /secondarymount
# umount /secondarymount
```

10. Continue with Prepare the System VM Template on page 29.

## Prepare the System VM Template

Secondary storage must be seeded with a template that is used for CloudPlatform system VMs.

When copying and pasting a command, be sure the command has pasted as a single line before executing. Some document viewers may introduce unwanted line breaks in copied text.

1. On the Management Server, run one or more of the following `cloud-install-sys-tmplt` commands to retrieve and decompress the system VM template. Run the command for each hypervisor type that you expect end users to run in this Zone.

If your secondary storage mount point is not named `/mnt/secondary`, substitute your own mount point name.

If you set the CloudPlatform database encryption type to "web" when you set up the database, you must use the parameter `-s <management-server-secret-key>`. See About Password and Key Encryption on page 36.

This process will require approximately 5 GB of free space on the local file system and up to 30 minutes each time it runs.

- For vSphere, with CloudPlatform v3.0.5:

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt -m
/mnt/secondary -u http://download.cloud.com/templates/burbank/burbank-systemvm-
08012012.ova -h vmware -s <optional-management-server-secret-key> -F
```

- For vSphere, with CloudPlatform v3.0.0-3.0.4:

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt -m
/mnt/secondary -u http://download.cloud.com/templates/acton/acton-systemvm-
02062012.ova -h vmware -s <optional-management-server-secret-key> -F
```

- For KVM:

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt -m
/mnt/secondary -u http://download.cloud.com/templates/acton/acton-systemvm-
02062012.qcow2.bz2 -h kvm -s <optional-management-server-secret-key> -F
```

- For XenServer:

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt -m
/mnt/secondary -u http://download.cloud.com/templates/acton/acton-systemvm-
02062012.vhd.bz2 -h xenserver -s <optional-management-server-secret-key> -F
```

2. When the script has finished, unmount secondary storage and remove the created directory.

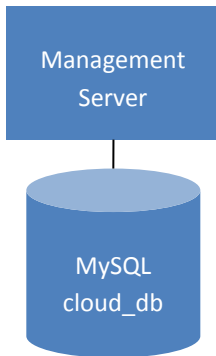
```
# umount /mnt/secondary
# rmdir /mnt/secondary
```

3. Repeat these steps for each secondary storage server.

## Single-Node Installation Complete! Next Steps

---

Congratulations! You have now installed CloudPlatform Management Server and the database it uses to persist system data.



What should you do next?

- Even without adding any cloud infrastructure, you can run the UI to get a feel for what's offered and how you will interact with CloudPlatform on an ongoing basis. See [Log In to the CloudPlatform UI](#) on page 42.
- When you're ready, add the cloud infrastructure and try running some virtual machines on it, so you can watch how CloudPlatform manages the infrastructure. See [Provision Your Cloud Infrastructure](#) on page 44.
- If desired, you can scale up by adding more Management Server nodes. See [Management Server Multi-Node Installation](#) on page 31.

# Management Server Multi-Node Installation

---

This section describes installing multiple Management Servers and installing MySQL on a node separate from the Management Servers. The machines must meet the system requirements described in System Requirements on page 19.

The procedure for a multi-node installation is:

1. Prepare the Operating System
2. Install the First Management Server
3. Install and Configure the Database
4. Prepare NFS Shares
5. Prepare and Start Additional Management Servers
6. Prepare the System VM Template

**WARNING**

For the sake of security, be sure the public Internet can not access port 8096 or port 8250 on the Management Server.

## Prepare the Operating System

---

The OS must be prepared to host the Management Server using the following steps. These steps must be performed on each Management Server node.

1. Log in to your OS as root.
2. Check for a fully qualified hostname.

```
# hostname --fqdn
```

This should return a fully qualified hostname such as "kvm1.lab.example.org". If it does not, edit /etc/hosts so that it does.

3. Set SELinux to be permissive by default.
  - a. Check to see whether SELinux is installed on your machine. If not, you can skip to step 4.  
In RHEL or CentOS, SELinux are installed and enabled by default. You can verify this with:

```
# rpm -qa | grep selinux
```

- b. Set the SELINUX variable in /etc/selinux/config to "permissive". This ensures that the permissive setting will be maintained after a system reboot.

```
# vi /etc/selinux/config
```

- c. Then set SELinux to permissive starting immediately, without requiring a system reboot.

In CentOS:

```
# setenforce permissive
```

In RHEL:

```
# setenforce 0
```

4. Make sure that the Management Server can reach the Internet.

```
# ping www.google.com
```

5. (RHEL 6.2) If you do not have a Red Hat Network account, you need to prepare a local Yum repository.
  - a. If you are working with a physical host, insert the RHEL 6.2 installation CD. If you are using a VM, attach the RHEL6 ISO.
  - b. Mount the CDROM to /media.
  - c. Create a repo file at /etc/yum.repos.d/rhel6.repo. In the file, insert the following lines:

```
[rhel]
name=rhel6
baseurl=file:///media
enabled=1
gpgcheck=0
```

6. Turn on NTP for time synchronization.

- a. Install NTP.

```
# yum install ntp
```

- b. Edit the NTP configuration file to point to your NTP server.

```
# vi /etc/ntp.conf
```

Add one or more server lines in this file with the names of the NTP servers you want to use. For example:

```
server 0.xenserver.pool.ntp.org
server 1.xenserver.pool.ntp.org
server 2.xenserver.pool.ntp.org
server 3.xenserver.pool.ntp.org
```

- c. Restart the NTP client.

```
# service ntpd restart
```

- d. Make sure NTP will start again upon reboot.

```
# chkconfig ntpd on
```

**TIP**

NTP is required to synchronize the clocks of the servers in your cloud.

---

## Install the First Management Server

---

1. Download the CloudPlatform Management Server onto the host where it will run from the following link. If your operating system is CentOS, use the download file for RHEL.

<https://www.citrix.com/English/ss/downloads/>

You will need a [MyCitrix account](#).

2. Install the CloudPlatform packages. You should have a file in the form of “CloudStack-VERSION-N-OSVERSION.tar.gz”. Untar the file and then run the install.sh script inside it. Replace the file and directory names below with those you are using:

```
# tar xzf CloudStack-VERSION-N-OSVERSION.tar.gz
# cd CloudStack-VERSION-N-OSVERSION
# ./install.sh
```

You should see a few messages as the installer prepares, followed by a list of choices.

3. Choose M to install the Management Server software.

```
> M
```

4. Wait for a message like “Complete! Done,” which indicates that the software was installed successfully.
5. When the installation is finished, run the following commands to start essential services (the commands might be different depending on your OS):

```
# service rpcbind start
# service nfs start
# chkconfig nfs on
# chkconfig rpcbind on
```

6. Continue to Install and Configure the Database on page 34.

## Install and Configure the Database

1. If you already have a version of MySQL installed, make one of the following choices, depending on what version of MySQL it is. The most recent version tested with CloudPlatform is 5.1.58.

- If you already have installed MySQL version 5.1.58 or later, skip to step 3.
- If you have installed a version of MySQL earlier than 5.1.58, you can either skip to step 3 or uninstall MySQL and proceed to step 2 to install a more recent version.

**WARNING**

It is important that you choose the right database version. Never downgrade a MySQL installation that is used with CloudPlatform.

2. Log in as root to your Database Node and run the following commands. If you are going to install a replica database, then log in to the master.

```
# yum install mysql-server
# chkconfig --level 35 mysqld on
```

3. Edit the MySQL configuration (/etc/my.cnf or /etc/mysql/my.cnf, depending on your OS) and insert the following lines in the [mysqld] section. You can put these lines below the datadir line. The max\_connections parameter should be set to 350 multiplied by the number of Management Servers you are deploying. This example assumes two Management Servers.

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=700
log-bin=mysql-bin
binlog-format = 'ROW'
```

**NOTE:** The binlog-format variable is supported in MySQL versions 5.1 and greater. It is not supported in MySQL 5.0. In some versions of MySQL, an underscore character is used in place of the hyphen in the variable name. For the exact syntax and spelling of each variable, consult the documentation for your version of MySQL.

4. Start the MySQL service, then invoke MySQL as the root user.

```
# service mysqld restart
# mysql -u root
```

5. Best Practice: On RHEL and CentOS, MySQL does not set a root password by default. It is very strongly recommended that you set a root password as a security precaution. Run the following command, and substitute your own desired root password for <password>.

```
mysql> SET PASSWORD = PASSWORD('password');
```

From now on, start MySQL with `mysql -p` so it will prompt you for the password.

6. To grant access privileges to remote users, perform the following steps.
  - a. Run the following command from the mysql prompt:

```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' WITH GRANT OPTION;
mysql> exit
```

- b. Restart the MySQL service.

```
# service mysqld restart
```

- c. Open the MySQL server port (3306) in the firewall to allow remote clients to connect.

```
# iptables -I INPUT -p tcp --dport 3306 -j ACCEPT
```

- d. Edit the `/etc/sysconfig/iptables` file and add the following lines at the beginning of the INPUT chain.

```
-A INPUT -p tcp --dport 3306 -j ACCEPT
```

7. Return to the root shell on your first Management Server.

8. Set up the database. The following command creates the cloud user on the database.

- In `dbpassword`, specify the password to be assigned to the cloud user. You can choose to provide no password.
- In `dbhost`, provide the hostname of the database node.
- In `deploy-as`, specify the username and password of the user deploying the database. For example, if you originally installed MySQL with user “root” and password “password”, provide `--deploy-as=root:password`.
- (Optional) For `encryption_type`, use file or web to indicate the technique used to pass in the database encryption password. Default: file. See About Password and Key Encryption on page 36.
- (Optional) For `management_server_key`, substitute the default key that is used to encrypt confidential parameters in the CloudPlatform properties file. Default: password. It is highly recommended that you replace this with a more secure value. See About Password and Key Encryption on page 36.
- (Optional) For `database_key`, substitute the default key that is used to encrypt confidential parameters in the CloudPlatform database. Default: password. It is highly recommended that you replace this with a more secure value. See About Password and Key Encryption on page 36.

```
# cloud-setup-databases cloud:<dbpassword>@<dbhost> --deploy-as=root:<password> -e  
<encryption_type> -m <management_server_key> -k <database_key>
```

9. If you are running the hypervisor on the same machine with the Management Server, edit `/etc/sudoers` and add the following line:

```
Defaults:cloud !requiretty
```

10. Now run a script that will set up iptables rules and SELinux for use by the Management Server. It will also chkconfig off and start the Management Server.

```
# cloud-setup-management
```

You should see the message “CloudPlatform Management Server setup is done.”

11. Continue to Prepare NFS Shares on page 36.

## About Password and Key Encryption

CloudPlatform stores several sensitive passwords and secret keys that are used to provide security. These values are always automatically encrypted:

- Database secret key
- Database password
- SSH keys
- Compute node root password
- VPN password
- User API secret key
- VNC password

CloudPlatform uses the Java Simplified Encryption (JASYPT) library. The data values are encrypted and decrypted using a database secret key, which is stored in one of CloudPlatform's internal properties files along with the database password. The other encrypted values listed above (SSH keys, etc.) are in the CloudPlatform internal database.

Of course, the database secret key itself can not be stored in the open – it must be encrypted. How then does CloudPlatform read it? A second secret key must be provided from an external source during Management Server startup. This key can be provided in one of two ways: loaded from a file or provided by the CloudPlatform administrator. The CloudPlatform database has a new configuration setting that lets it know which of these methods will be used. If the encryption type is set to “file,” the key must be in a file in a known location. If the encryption type is set to “web,” the administrator runs the utility `com.cloud.utils.crypt.EncryptionSecretKeySender`, which relays the key to the Management Server over a known port.

The encryption type, database secret key, and Management Server secret key are set during CloudPlatform installation. They are all parameters to the CloudPlatform database setup script (`cloud-setup-databases`). The default values are file, password, and password. It is, of course, highly recommended that you change these to more secure keys.

## Prepare NFS Shares

---

CloudPlatform needs a place to keep primary and secondary storage (see Cloud Infrastructure Overview on page 16). Both of these can be NFS shares. This section tells how to set up the NFS shares before adding the storage to CloudPlatform. A production installation typically uses a separate NFS server, but you can also use the Management Server node as the NFS server.

For primary storage, you can use iSCSI instead.

The requirements for primary and secondary storage are described in:

- About Primary Storage on page 71
- About Secondary Storage on page 73

## Using a Separate NFS Server

This section tells how to set up NFS shares for secondary and (optionally) primary storage on an NFS server running on a separate node from the Management Server.

The exact commands for the following steps may vary depending on your operating system version.

**WARNING**

(KVM only) Ensure that no volume is already mounted at your NFS mount point.

1. On the storage server, create an NFS share for secondary storage and, if you are using NFS for primary storage as well, create a second NFS share.

```
# mkdir -p /export/primary
# mkdir -p /export/secondary
```

2. Export the NFS shares with `rw,async,no_root_squash`. For example:

```
# vi /etc/exports
```

Insert the following line.

```
/export *(rw,async,no_root_squash)
```

3. Export the `/export` directory.

```
# exportfs -a
```

4. On the management server, create a mount point for secondary storage. For example:

```
# mkdir -p /mnt/secondary
```

5. Mount the secondary storage on your Management Server. Replace the example NFS server name and NFS share paths below with your own.

```
# mount -t nfs nfsservername:/nfs/share/secondary /mnt/secondary
```

6. Continue with Prepare and Start Additional Management Servers on page 39.

## Using the Management Server as the NFS Server

This section tells how to set up NFS shares for secondary and (optionally) primary storage on the same node with the Management Server. It is assumed that you will have less than 16TB of storage on the host.

The exact commands for the following steps may vary depending on your operating system version.

1. On the Management Server host, create an NFS share for secondary storage and, if you are using NFS for primary storage as well, create a second NFS share.

```
# mkdir -p /export/primary
# mkdir -p /export/secondary
```

2. To configure the new directories as NFS exports, edit `/etc/exports`.

```
# vi /etc/exports
```

Insert the following line.

```
/export *(rw,async,no_root_squash)
```

3. Export the `/export` directory.

```
# exportfs -a
```

4. Edit the `/etc/sysconfig/nfs` file and uncomment the following lines.

```
LOCKD_TCPDPORT=32803
LOCKD_UDPSPORT=32769
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=662
STATD_OUTGOING_PORT=2020
```

5. Edit the `/etc/sysconfig/iptables` file and add the following lines at the beginning of the INPUT chain.

```
-A INPUT -m state --state NEW -p udp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 2049 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 32803 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 32769 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 662 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 662 -j ACCEPT
```

6. Run the following commands:

```
# service iptables restart
# service iptables save
```

7. If NFS v4 communication is used between client and server, add your domain to `/etc/idmapd.conf` on both the hypervisor host and Management Server.

```
# vi /etc/idmapd.conf
```

Remove the character `#` from the beginning of the Domain line in `idmapd.conf` and replace the value in the file with your own domain. In the example below, the domain is `company.com`.

```
Domain = company.com
```

8. Reboot the Management Server host.

Two NFS shares called `/export/primary` and `/export/secondary` are now set up.

9. It is recommended that you also test to be sure the previous steps have been successful.
  - a. Log in to the hypervisor host.
  - b. Be sure NFS and rpcbind are running. The commands might be different depending on your OS. For example (substitute your own management server name):

```
# service rpcbind start
# service nfs start
# chkconfig nfs on
# chkconfig rpcbind on
# reboot
```

- c. Log back in to the hypervisor host and try to mount the /export directories. For example (substitute your own management server name):

```
# mkdir /primarymount
# mount -t nfs <management-server-name>:/export/primary /primarymount
# umount /primarymount
# mkdir /secondarymount
# mount -t nfs <management-server-name>:/export/secondary /secondarymount
# umount /secondarymount
```

10. Continue with Prepare and Start Additional Management Servers on page 39.

## Prepare and Start Additional Management Servers

---

For your second and subsequent Management Servers, you will install CloudPlatform, connect it to the database, and set up the OS for the Management Server.

1. Perform the steps in Prepare the Operating System on page 31.
2. Download the CloudPlatform Management Server onto the additional host where it will run from the following link. If your operating system is CentOS, use the download file for RHEL.

<https://www.citrix.com/English/ss/downloads/>

You will need a [MyCitrix account](#).

3. Install the CloudPlatform packages. Replace the file and directory names below with those you are using:

```
# tar xzf CloudStack-VERSION-1-OSVERSION.tar.gz
# cd CloudStack-VERSION-1-OSVERSION
# ./install.sh
```

You should see a few messages as the installer prepares, followed by a list of choices.

4. Choose “M” to install the Management Server.
5. When the installation is finished, run the following commands to start essential services (the commands might be different depending on your OS):

```
# service rpcbind start
# service nfs start
# chkconfig nfs on
# chkconfig rpcbind on
```

6. Configure the database client. Note the absence of the `--deploy-as` argument in this case.

```
# cloud-setup-databases cloud:<dbpassword>@<dbhost> -e <encryption_type> -m
<management_server_key> -k <database_key>
```

7. If you are running the hypervisor on the same machine with the Management Server, edit `/etc/sudoers` and add the following line:

```
Defaults:cloud !requiretty
```

8. Configure the OS and start the Management Server:

```
# cloud-setup-management
```

The Management Server on this node should now be running.

9. Repeat these steps on each additional Management Server.
10. Be sure to configure a load balancer for the Management Servers. See [Management Server Load Balancing](#) on page 130.
11. Continue with [Prepare the System VM Template](#) on page 40.

## Prepare the System VM Template

Secondary storage must be seeded with a template that is used for CloudPlatform system VMs.

1. On the Management Server, run one or more of the following `cloud-install-sys-tpmt` commands to retrieve and decompress the system VM template. Run the command for each hypervisor type that you expect end users to run in this Zone.

When copying and pasting a command, be sure the command has pasted as a single line before executing. Some document viewers may introduce unwanted line breaks in copied text.

If your secondary storage mount point is not named `/mnt/secondary`, substitute your own mount point name.

If you set the CloudPlatform database encryption type to "web" when you set up the database, you must now add the parameter `-s <management-server-secret-key>`. See [About Password and Key Encryption](#) on page 36.

This process will require approximately 5 GB of free space on the local file system and up to 30 minutes each time it runs.

- For vSphere, with CloudPlatform v3.0.5:

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tpmt -m
/mnt/secondary -u http://download.cloud.com/templates/burbank/burbank-systemvm-
08012012.ova -h vmware -s <optional-management-server-secret-key> -F
```

- For vSphere, with CloudPlatform v3.0.0-3.0.4:

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tpmt -m
/mnt/secondary -u http://download.cloud.com/templates/acton/acton-systemvm-02062012.ova
-h vmware -s <optional-management-server-secret-key> -F
```

➤ For KVM:

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmpl -m
/mnt/secondary -u http://download.cloud.com/templates/acton/acton-systemvm-
02062012.qcow2.bz2 -h kvm -s <optional-management-server-secret-key> -F
```

➤ For XenServer:

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmpl -m
/mnt/secondary -u http://download.cloud.com/templates/acton/acton-systemvm-
02062012.vhd.bz2 -h xenserver -s <optional-management-server-secret-key> -F
```

2. If you are using a separate NFS server, perform this step. If you are using the Management Server as the NFS server, you **MUST NOT** perform this step.

When the script has finished, unmount secondary storage and remove the created directory.

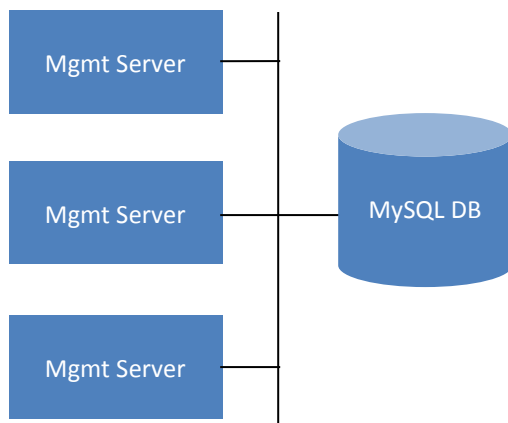
```
# umount /mnt/secondary
# rmdir /mnt/secondary
```

3. Repeat these steps for each secondary storage server.

## Multi-Node Installation Complete! Next Steps

---

Congratulations! You have now installed CloudPlatform Management Server and the database it uses to persist system data in a multi-node configuration.



What should you do next?

- Even without adding any cloud infrastructure, you can run the UI to get a feel for what's offered and how you will interact with CloudPlatform on an ongoing basis. See [Log In to the CloudPlatform UI](#) on page 42.
- When you're ready, add the cloud infrastructure and try running some virtual machines on it, so you can watch how CloudPlatform manages the infrastructure. See [Provision Your Cloud Infrastructure](#) on page 44.

# Log In to the CloudPlatform UI

---

CloudPlatform provides a web-based UI that can be used by both administrators and end users. The appropriate version of the UI is displayed depending on the credentials used to log in. The UI is available in popular browsers including IE7, IE8, IE9, Firefox 3.5+, Firefox 4, Safari 4, and Safari 5. The URL is: (substitute your own management server IP address)

```
http://<management-server-ip-address>:8080/client
```

For more guidance about the choices that appear when you log in to this UI, see [Logging In as the Root Administrator](#) on page 42.

## End User's UI Overview

---

The CloudPlatform UI helps users of cloud infrastructure to view and use their cloud resources, including virtual machines, templates and ISOs, data volumes and snapshots, guest networks, and IP addresses. If the user is a member or administrator of one or more CloudPlatform projects, the UI can provide a project-oriented view.

## Root Administrator's UI Overview

---

The CloudPlatform UI helps the CloudPlatform administrator provision, view, and manage the cloud infrastructure, domains, user accounts, projects, and configuration settings. The first time you start the UI after a fresh Management Server installation, you can choose to follow a guided tour to provision your cloud infrastructure. On subsequent logins, the dashboard of the logged-in user appears. The various links in this screen and the navigation bar on the left provide access to a variety of administrative functions. The root administrator can also use the UI to perform all the same tasks that are present in the end-user's UI.

## Logging In as the Root Administrator

---

After the Management Server software is installed and running, you can run the CloudPlatform user interface. This UI is there to help you provision, view, and manage your cloud infrastructure.

1. Open your favorite Web browser and go to this URL. Substitute the IP address of your own Management Server:

```
http://<management-server-ip-address>:8080/client
```

On a fresh Management Server installation, a guided tour splash screen appears. On later visits, you'll see a login screen where you can enter a user ID and password and proceed to your Dashboard.

2. If you see the first-time splash screen, choose one of the following.
  - **Continue with basic setup.** Choose this if you're just trying CloudPlatform, and you want a guided walkthrough of the simplest possible configuration so that you can get started using CloudPlatform right away. We'll help you set up a cloud with the following features: a single machine that runs CloudPlatform software and uses NFS to provide storage; a single machine running VMs under the XenServer hypervisor; and a shared public network.

The prompts in this guided tour should give you all the information you need, but if you want just a bit more detail, you can follow along in the CloudPlatform Trial Installation Guide.

- **I have used CloudPlatform before.** Choose this if you have already gone through a design phase and planned a more sophisticated deployment, or you are ready to start scaling up a trial cloud that you set up earlier with the basic setup screens. In the Administrator UI, you can start using the more powerful features of CloudPlatform, such as advanced VLAN networking, high availability, additional network elements such as load balancers and firewalls, and support for multiple hypervisors including Citrix XenServer, KVM, and VMware vSphere.

The root administrator Dashboard appears.

3. You should set a new root administrator password. If you chose basic setup, you'll be prompted to create a new password right away. If you chose experienced user, use the steps in Change the Root Password on page 45.

You are logging in as the root administrator. This account manages the CloudPlatform deployment, including physical infrastructure. The root administrator can modify configuration settings to change basic functionality, create or delete user accounts, and take many actions that should be performed only by an authorized person. Please change the default password to a new, unique password.

# Provision Your Cloud Infrastructure

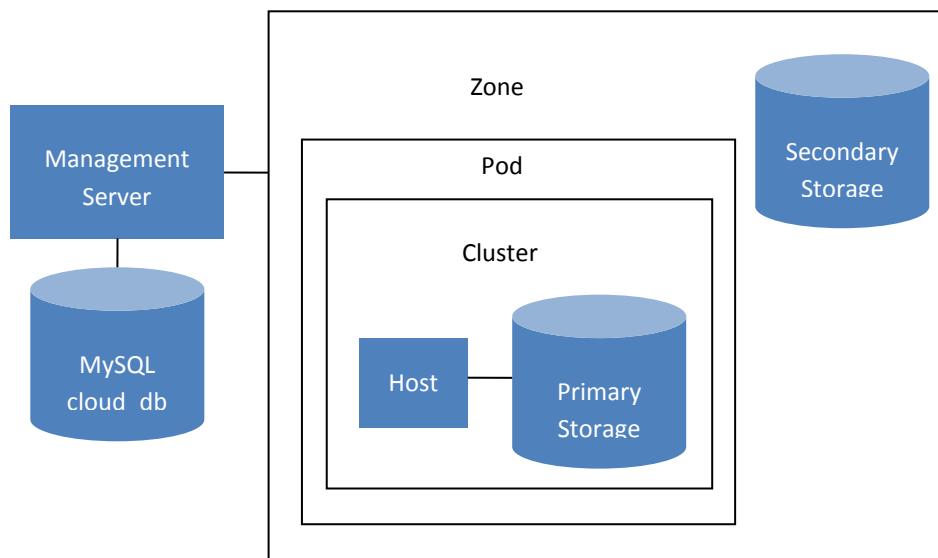
---

After the Management Server is installed and running, you can add the compute resources for it to manage. For an overview of how a CloudPlatform cloud infrastructure is organized, see [Cloud Infrastructure Overview](#) on page 16.

To provision the cloud infrastructure, or to scale it up at any time, follow these procedures:

1. Change the Root Password on page 45
2. Add a Zone on page 46
3. Add More Pods (Optional) on page 61
4. Add More Cluster on page 63
5. Add More Hosts (Optional) on page 67
6. Add Primary Storage on page 71
7. Add Secondary Storage on page 73
8. Initialization and Testing on page 75

When you have finished these steps, you will have a deployment with the following basic structure:




Conceptual view of a basic deployment

Your actual deployment can have multiple management servers and zones.

# Change the Root Password

---

During CloudPlatform installation, you are logging in as the root administrator. This account manages the CloudPlatform deployment, including physical infrastructure. The root administrator can modify configuration settings to change basic functionality, create or delete user accounts, and take many actions that should be performed only by an authorized person. Please change the default password (which is “password”) to a new, unique value.

1. Log in to the CloudPlatform UI using the current root user ID and password. The default is admin, password.
2. Click Accounts.
3. Click the admin account name.
4. Click View Users.
5. Click the admin user name.
6. Click the Change Password button. 
7. Type the new password, and click OK.

# Add a Zone

---

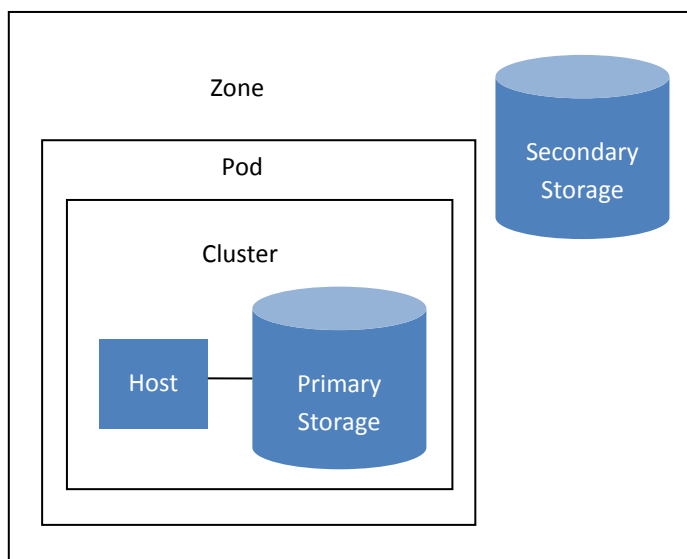
## About Zones

---

A zone is the largest organizational unit within a CloudPlatform deployment. A zone typically corresponds to a single datacenter, although it is permissible to have multiple zones in a datacenter. The benefit of organizing infrastructure into zones is to provide physical isolation and redundancy. For example, each zone can have its own power supply and network uplink, and the zones can be widely separated geographically (though this is not required).

A zone consists of:

- One or more pods. Each pod contains one or more clusters of hosts and one or more primary storage servers.
- Secondary storage, which is shared by all the pods in the zone.



**A simple zone**

Zones are visible to the end user. When a user starts a guest VM, the user must select a zone for their guest. Users might also be required to copy their private templates to additional zones to enable creation of guest VMs using their templates in those zones.

Zones can be public or private. Public zones are visible to all users. This means that any user may create a guest in that zone. Private zones are reserved for a specific domain. Only users in that domain or its subdomains may create guests in that zone.

Hosts in the same zone are directly accessible to each other without having to go through a firewall. Hosts in different zones can access each other through statically configured VPN tunnels.

For each zone, the administrator must decide the following.

- How many pods to place in a zone.
- How many clusters to place in each pod.
- How many hosts to place in each cluster.
- How many primary storage servers to place in each cluster and total capacity for the storage servers.
- How much secondary storage to deploy in a zone.

When you add a new zone, you will be prompted to configure the zone's physical network and add the first pod, cluster, host, primary storage, and secondary storage.

## About Physical Networks

---

Part of adding a zone is setting up the physical network. One or (in an advanced zone) more physical networks can be associated with each zone. The network corresponds to a NIC on the hypervisor host. Each physical network can carry one or more types of network traffic. The choices of traffic type for each network vary depending on whether you are creating a zone with basic networking or advanced networking.

A physical network is the actual network hardware and wiring in a zone. A zone can have multiple physical networks. An administrator can:

- Add/Remove/Update physical networks in a zone
- Configure VLANs on the physical network
- Configure a name so the network can be recognized by hypervisors
- Configure the service providers (firewalls, load balancers, etc.) available on a physical network
- Configure the IP addresses trunked to a physical network
- Specify what type of traffic is carried on the physical network, as well as other properties like network speed

## Configurable Characteristics of Physical Networks

CloudPlatform provides configuration settings you can use to set up a physical network in a zone, including:

- What type of network traffic it carries (guest, public, management, storage)
- VLANs
- Unique name that the hypervisor can use to find that particular network
- Enabled or disabled. When a network is first set up, it is disabled – not in use yet. The administrator sets the physical network to enabled, and it begins to be used. The administrator can later disable the network again, which prevents any new virtual networks from being created on that physical network; the existing network traffic continues even though the state is disabled.

- Speed
- Tags, so network offerings can be matched to physical networks
- Isolation method

## Basic Zone Network Traffic Types

When basic networking is used, there can be only one physical network in the zone. That physical network carries three traffic types:

We strongly recommend the use of separate NICs for management traffic and guest traffic.

- **Guest.** When end users run VMs, they generate guest traffic. The guest VMs communicate with each other over a network that can be referred to as the guest network. Each pod in a basic zone is a broadcast domain, and therefore each pod has a different IP range for the guest network. The administrator must configure the IP range for each pod.
- **Management.** When CloudPlatform's internal resources communicate with each other, they generate management traffic. This includes communication between hosts, system VMs (VMs used by CloudPlatform to perform various tasks in the cloud), and any other component that communicates directly with the CloudPlatform Management Server. You must configure the IP range for the system VMs to use.
- **Storage.** Traffic such as VM templates and snapshots, which is sent between the secondary storage VM and secondary storage servers. CloudPlatform uses a separate Network Interface Controller (NIC) named storage NIC for storage network traffic. Use of a storage NIC that always operates on a high bandwidth network allows fast template and snapshot copying. You must configure the IP range to use for the storage network.
- **Public.** Public traffic is generated when VMs in the cloud access the Internet. Publicly accessible IPs must be allocated for this purpose. End users can use the CloudPlatform UI to acquire these IPs to implement NAT between their guest network and the public network, as described in "Acquiring a New IP Address" in the Administration Guide.

In a basic network, configuring the physical network is fairly straightforward. In most cases, you only need to configure one guest network to carry traffic that is generated by guest VMs. If you use a NetScaler load balancer and enable its elastic IP and elastic load balancing (EIP and ELB) features, you must also configure a network to carry public traffic. CloudPlatform takes care of presenting the necessary network configuration steps to you in the UI when you add a new zone.

## Basic Zone Guest IP Addresses

When basic networking is used, CloudPlatform will assign IP addresses in the CIDR of the pod to the guests in that pod. The administrator must add a Direct IP range on the pod for this purpose. These IPs are in the same VLAN as the hosts.

## Advanced Zone Network Traffic Types

When advanced networking is used, there can be multiple physical networks in the zone. Each physical network can carry one or more traffic types, and you need to let CloudPlatform know which type of network traffic you want each network to carry. The traffic types in an advanced zone are:

- **Guest.** When end users run VMs, they generate guest traffic. The guest VMs communicate with each other over a network that can be referred to as the guest network. This network can be isolated or shared. In an isolated guest network, the administrator needs to reserve VLAN ranges to provide isolation for each CloudPlatform account's network (potentially a large number of VLANs). In a shared guest network, all guest VMs share a single network.

- **Management.** When CloudPlatform's internal resources communicate with each other, they generate management traffic. This includes communication between hosts, system VMs (VMs used by CloudPlatform to perform various tasks in the cloud), and any other component that communicates directly with the CloudPlatform Management Server. You must configure the IP range for the system VMs to use.
- **Public.** Public traffic is generated when VMs in the cloud access the Internet. Publicly accessible IPs must be allocated for this purpose. End users can use the CloudPlatform UI to acquire these IPs to implement NAT between their guest network and the public network, as described in "Acquiring a New IP Address" in the Administration Guide.
- **Storage.** Traffic such as VM templates and snapshots, which is sent between the secondary storage VM and secondary storage servers. CloudPlatform uses a separate Network Interface Controller (NIC) named storage NIC for storage network traffic. Use of a storage NIC that always operates on a high bandwidth network allows fast template and snapshot copying. You must configure the IP range to use for the storage network.

These traffic types can each be on a separate physical network, or they can be combined with certain restrictions. When you use the Add Zone wizard in the UI to create a new zone, you are guided into making only valid choices.

## Advanced Zone Guest IP Addresses

When advanced networking is used, the administrator can create additional networks for use by the guests. These networks can span the zone and be available to all accounts, or they can be scoped to a single account, in which case only the named account may create guests that attach to these networks. The networks are defined by a VLAN ID, IP range, and gateway. The administrator may provision thousands of these networks if desired.

## Advanced Zone Public IP Addresses

CloudPlatform provisions one public IP address per account for use as the source NAT IP address. If a Juniper SRX firewall is used, CloudPlatform can instead use a single public IP address as an interface NAT IP for all accounts, reducing the number of IP addresses consumed. Users may request additional public IP addresses. The administrator must configure one or more ranges of public IP addresses for use by CloudPlatform. These IP addresses could be RFC1918 addresses in private clouds.

## System Reserved IP Addresses

In each zone, you need to configure a range of reserved IP addresses for the management network. This network carries communication between the CloudPlatform Management Server and various system VMs, such as Secondary Storage VMs, Console Proxy VMs, and DHCP.

The reserved IP addresses must be unique across the cloud. You cannot, for example, have a host in one zone which has the same private IP address as a host in another zone.

The hosts in a pod are assigned private IP addresses. These are typically RFC1918 addresses. The Console Proxy and Secondary Storage system VMs are also allocated private IP addresses in the CIDR of the pod that they are created in.

Make sure computing servers and Management Servers use IP addresses outside of the System Reserved IP range. For example, suppose the System Reserved IP range starts at 192.168.154.2 and ends at 192.168.154.7. CloudPlatform can use .2 to .7 for System VMs. This leaves the rest of the pod CIDR, from .8 to .254, for the Management Server and hypervisor hosts.

**In all zones:**

Provide private IPs for the system in each pod and provision them in CloudPlatform.

For KVM and XenServer, the recommended number of private IPs per pod is one per host. If you expect a pod to grow, add enough private IPs now to accommodate the growth.

**In a zone that uses advanced networking:**

For vSphere with advanced networking, we recommend provisioning enough private IPs for your total number of customers, plus enough for the required CloudPlatform System VMs. Typically, about 10 additional IPs are required for the System VMs. For more information about System VMs, see *Working with System Virtual Machines* in the Administrator's Guide.

When advanced networking is being used, the number of private IP addresses available in each pod varies depending on which hypervisor is running on the nodes in that pod. Citrix XenServer and KVM use link-local addresses, which in theory provide more than 65,000 private IP addresses within the address block. As the pod grows over time, this should be more than enough for any reasonable number of hosts as well as IP addresses for guest virtual routers. VMWare ESXi, by contrast uses any administrator-specified subnetting scheme, and the typical administrator provides only 255 IPs per pod. Since these are shared by physical machines, the guest virtual router, and other entities, it is possible to run out of private IPs when scaling up a pod whose nodes are running ESXi.

To ensure adequate headroom to scale private IP space in an ESXi pod that uses advanced networking, use one or more of the following techniques:

- Specify a larger CIDR block for the subnet. A subnet mask with a /20 suffix will provide more than 4,000 IP addresses.
- Create multiple pods, each with its own subnet. For example, if you create 10 pods and each pod has 255 IPs, this will provide 2,550 IP addresses.

---

## Using Security Groups to Control Traffic to VMs

---

### About Security Groups

Security groups provide a way to isolate traffic to VMs. A security group is a group of VMs that filter their incoming and outgoing traffic according to a set of rules, called ingress and egress rules. These rules filter network traffic according to the IP address that is attempting to communicate with the VM. Security groups are particularly useful in zones that use basic networking, because there is a single guest network for all guest VMs. In CloudPlatform 3.0.3 - 3.0.5, security groups are supported only in zones that use basic networking.

In a zone that uses advanced networking, you can instead define multiple guest networks to isolate traffic to VMs.

Each CloudPlatform account comes with a default security group that denies all inbound traffic and allows all outbound traffic. The default security group can be modified so that all new VMs inherit some other desired set of rules.

Any CloudPlatform user can set up any number of additional security groups. When a new VM is launched, it is assigned to the default security group unless another user-defined security group is specified. A VM can be a member of any number of

security groups. Once a VM is assigned to a security group, it remains in that group for its entire lifetime; you can not move a running VM from one security group to another.

You can modify a security group by deleting or adding any number of ingress and egress rules. When you do, the new rules apply to all VMs in the group, whether running or stopped.

If no ingress rules are specified, then no traffic will be allowed in, except for responses to any traffic that has been allowed out through an egress rule.

## Enabling Security Groups

In order for security groups to function in a zone, the security groups feature must first be enabled for the zone. The administrator can do this when creating a new zone, by selecting a network offering that includes security groups. The procedure is described in Basic Zone Configuration on page 52.

## Working With Security Groups

For information about adding security groups and defining ingress and egress rules, see the Administrator's Guide.

## Adding a Zone

---

These steps assume you have already logged in to the CloudPlatform UI (see page 42).

1. (Optional) If you are going to use Swift for cloud-wide secondary storage, you need to add it to CloudPlatform before you add zones.
  - a. Log in to the CloudPlatform UI as administrator.
  - b. If this is your first time visiting the UI, you will see the guided tour splash screen. Choose "Experienced user." The Dashboard appears.
  - c. In the left navigation bar, click Global Settings.
  - d. In the search box, type `swift.enable` and click the search button.

e. Click the edit button and set `swift.enable` to true.



f. Restart the Management Server.

```
# service cloud-management restart
```

- g. Refresh the CloudPlatform UI browser tab and log back in.
2. In the left navigation, choose Infrastructure. On Zones, click View More.
3. (Optional) If you are using Swift storage, click Enable Swift. Provide the following:
  - **URL.** The Swift URL.
  - **Account.** The Swift account.
  - **Username.** The Swift account's username.

- **Key.** The Swift key.
4. Click Add Zone. The Zone creation wizard will appear.
  5. Choose one of the following network types:
    - **Basic.** For AWS-style networking. Provides a single network where each VM instance is assigned an IP directly from the network. Guest isolation can be provided through layer-3 means such as security groups (IP address source filtering).
    - **Advanced.** For more sophisticated network topologies. This network model provides the most flexibility in defining guest networks and providing custom network offerings such as firewall, VPN, or load balancer support.For more information about the network types, see Network Setup on page 123.
  6. The rest of the steps differ depending on whether you chose Basic or Advanced. Continue with the steps that apply to you:
    - Basic Zone Configuration on page 52
    - Advanced Zone Configuration on page 56

## Basic Zone Configuration

1. After you select Basic in the Add Zone wizard and click Next, you will be asked to enter the following details. Then click Next.
  - **Name.** A name for the zone.
  - **DNS 1 and 2.** These are DNS servers for use by guest VMs in the zone. These DNS servers will be accessed via the public network you will add later. The public IP addresses for the zone must have a route to the DNS server named here.
  - **Internal DNS 1 and Internal DNS 2.** These are DNS servers for use by system VMs in the zone (these are VMs used by CloudPlatform itself, such as virtual routers, console proxies, and Secondary Storage VMs.) These DNS servers will be accessed via the management traffic network interface of the System VMs. The private IP address you provide for the pods must have a route to the internal DNS server named here.
  - **Hypervisor.** (Introduced in version 3.0.1) Choose the hypervisor for the first cluster in the zone. You can add clusters with different hypervisors later, after you finish adding the zone.
  - **Network Offering.** Your choice here determines what network services will be available on the network for guest VMs.

DefaultSharedNetworkOfferingWithSGService	If you want to enable security groups for guest traffic isolation, choose this. (See Using Security Groups to Control Traffic to VMs on page 50.)
DefaultSharedNetworkOffering	If you do not need security groups, choose this.
DefaultSharedNetscalerEIPandELBNetworkOffering	If you have installed a Citrix NetScaler appliance as part of your zone network, and you will be using its Elastic IP and Elastic Load Balancing features, choose this. With the EIP and ELB features, a basic zone with

	security groups enabled can offer 1:1 static NAT and load balancing.
--	--

- **Network Domain:** (Optional) If you want to assign a special domain name to the guest VM network, specify the DNS suffix.
- **Public.** A public zone is available to all users. A zone that is not public will be assigned to a particular domain. Only users in that domain will be allowed to create guest VMs in this zone.

2. Choose which traffic types will be carried by the physical network.

The traffic types are management, public, guest, and storage traffic. For more information about the types, roll over the icons to display their tool tips, or see Basic Zone Network Traffic Types on page 48. This screen starts out with some traffic types already assigned. To add more, drag and drop traffic types onto the network. You can also change the network name if desired.

3. (Introduced in version 3.0.1) Assign a network traffic label to each traffic type on the physical network. These labels must match the labels you have already defined on the hypervisor host. To assign each label, click the Edit button under the traffic type icon. A popup dialog appears where you can type the label, then click OK.

These traffic labels will be defined only for the hypervisor selected for the first cluster. For all other hypervisors, the labels can be configured after the zone is created.

(VMware only) If you have enabled Nexus dvSwitch in the environment, you must specify the corresponding Ethernet port profile names as network traffic label for each traffic type on the physical network. For more information on Nexus dvSwitch, see Configuring a vSphere Cluster with Nexus 1000v Virtual Switch on page 95.

4. Click Next.

5. (NetScaler only) If you chose the network offering for NetScaler, you have an additional screen to fill out. Provide the requested details to set up the NetScaler, then click Next.

- **IP address.** The NSIP (NetScaler IP) address of the NetScaler device.
- **Username/Password.** The authentication credentials to access the device. CloudPlatform uses these credentials to access the device.
- **Type.** NetScaler device type that is being added. It could be NetScaler VPX, NetScaler MPX, or NetScaler SDX. For a comparison of the types, see the CloudPlatform Administration Guide.
- **Public interface.** Interface of NetScaler that is configured to be part of the public network.
- **Private interface.** Interface of NetScaler that is configured to be part of the private network.
- **Number of retries.** Number of times to attempt a command on the device before considering the operation failed. Default is 2.
- **Capacity.** Number of guest networks/accounts that will share this NetScaler device.
- **Dedicated.** When marked as dedicated, this device will be dedicated to a single account. When Dedicated is checked, the value in the Capacity field has no significance – implicitly, its value is 1.

6. (NetScaler only) Configure the IP range for public traffic. The IPs in this range will be used for the static NAT capability which you enabled by selecting the network offering for NetScaler with EIP and ELB. Enter the following details, then click Add. If desired, you can repeat this step to add more IP ranges. When done, click Next.

- **Gateway.** The gateway in use for these IP addresses.
- **Netmask.** The netmask associated with this IP range.
- **VLAN.** The VLAN that will be used for public traffic.

- **Start IP/End IP.** A range of IP addresses that are assumed to be accessible from the Internet and will be allocated for access to guest VMs.

7. In a new zone, CloudPlatform adds the first pod for you. You can always add more pods later. For an overview of what a pod is, see About Pods on page 61.

To configure the first pod, enter the following, then click Next:

- **Pod Name.** A name for the pod.
- **Reserved system gateway.** The gateway for the hosts in that pod.
- **Reserved system netmask.** The network prefix that defines the pod's subnet. Use CIDR notation.
- **Start/End Reserved System IP.** The IP range in the management network that CloudPlatform uses to manage various system VMs, such as Secondary Storage VMs, Console Proxy VMs, and DHCP. For more information, see System Reserved IP Addresses on page 49.

8. Configure the network for guest traffic. Provide the following, then click Next:

- **Guest gateway:** The gateway that the guests should use.
- **Guest netmask:** The netmask in use on the subnet the guests will use.
- **Guest start IP/End IP:** Enter the first and last IP addresses that define a range that CloudPlatform can assign to guests.
  - We strongly recommend the use of multiple NICs. If multiple NICs are used, they may be in a different subnet.
  - If one NIC is used, these IPs should be in the same CIDR as the pod CIDR.

9. In a new pod, CloudPlatform adds the first cluster for you. You can always add more clusters later. For an overview of what a cluster is, see About Clusters on page 63.

To configure the first cluster, enter the following, then click Next:

- **Hypervisor.** (Version 3.0.0 only; in 3.0.1, this field is read only) Choose the type of hypervisor software that all hosts in this cluster will run. If you choose VMware, additional fields appear so you can give information about a vSphere cluster. For vSphere servers, we recommend creating the cluster of hosts in vCenter and then adding the entire cluster to CloudPlatform. See Add Cluster: vSphere on page 64.
- **Cluster name.** Enter a name for the cluster. This can be text of your choosing and is not used by CloudPlatform.

10. In a new cluster, CloudPlatform adds the first host for you. You can always add more hosts later. For an overview of what a host is, see About Hosts on page 67.

Before you can configure the host, you need to install the hypervisor software on the host. You will need to know which version of the hypervisor software version is supported by CloudPlatform and what additional configuration is required to ensure the host will work with CloudPlatform. To find these installation details, see:

- Citrix XenServer Installation for CloudPlatform on page 76
- VMware vSphere Installation and Configuration on page 87
- KVM Installation and Configuration on page 108
- Oracle VM (OVM) Installation and Configuration on page 112

When you deploy CloudPlatform, the hypervisor host must not have any VMs already running.

To configure the first host, enter the following, then click Next:

- **Host Name.** The DNS name or IP address of the host.

- **Username.** Usually root.
- **Password.** This is the password for the user named above (from your XenServer or KVM install).
- **Host Tags.** (Optional) Any labels that you use to categorize hosts for ease of maintenance. For example, you can set this to the cloud's HA tag (set in the ha.tag global configuration parameter) if you want this host to be used only for VMs with the "high availability" feature enabled. For more information, see HA-Enabled Virtual Machines as well as HA for Hosts, both in the Administration Guide.

**11.** In a new cluster, CloudPlatform adds the first primary storage server for you. You can always add more servers later. For an overview of what primary storage is, see About Primary Storage on page 71.

To configure the first primary storage server, enter the following, then click Next:

- **Name.** The name of the storage device.
- **Protocol.** For XenServer, choose either NFS, iSCSI, or PreSetup. For KVM, choose NFS or SharedMountPoint. For vSphere choose either VMFS (iSCSI or FiberChannel) or NFS. The remaining fields in the screen vary depending on what you choose here.

NFS	<ul style="list-style-type: none"> <li>• <b>Server.</b> The IP address or DNS name of the storage device.</li> <li>• <b>Path.</b> The exported path from the server.</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> <li>• The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</li> </ul>
iSCSI	<ul style="list-style-type: none"> <li>• <b>Server.</b> The IP address or DNS name of the storage device.</li> <li>• <b>Target IQN.</b> The IQN of the target. Example: iqn.1986-03.com.sun:02:01ec9bb549-1271378984</li> <li>• <b>Lun #.</b> The LUN number. Example: 3.</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> <li>• The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</li> </ul>
PreSetup	<ul style="list-style-type: none"> <li>• <b>Server.</b> The IP address or DNS name of the storage device.</li> <li>• <b>SR Name-Label.</b> Name-label of an SR that has been set up outside CloudPlatform.</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> <li>• The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</li> </ul>

SharedMountPoint	<ul style="list-style-type: none"> <li>• <b>Path.</b> The path on each host where primary storage is mounted. Example: <code>"/mnt/primary"</code>.</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> <li>• The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</li> </ul>
VMFS	<ul style="list-style-type: none"> <li>• <b>Server.</b> The IP address or DNS name of the vCenter server.</li> <li>• <b>Path.</b> The datacenter and datastore as <code>"/datacenter name/datastore name"</code>. Example: <code>"/cloud.dc.VM/cluster1datastore"</code>.</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> <li>• The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</li> </ul>

12. In a new zone, CloudPlatform adds the first secondary storage server for you. For an overview of what secondary storage is, see About Secondary Storage on page 73.

Before you can fill out this screen, you need to prepare the secondary storage by setting up NFS shares and installing the latest CloudPlatform System VM template. See Adding Secondary Storage on page 73.

To configure the first secondary storage server, enter the following, then click Next:

- **NFS Server.** The IP address of the server.
- **Path.** The exported path from the server.

13. Click Launch.

## Advanced Zone Configuration

1. After you select Advanced in the Add Zone wizard and click Next, you will be asked to enter the following details. Then click Next.
  - **Name.** A name for the zone.
  - **DNS 1 and 2.** These are DNS servers for use by guest VMs in the zone. These DNS servers will be accessed via the public network you will add later. The public IP addresses for the zone must have a route to the DNS server named here.
  - **Internal DNS 1 and Internal DNS 2.** These are DNS servers for use by system VMs in the zone (these are VMs used by CloudPlatform itself, such as virtual routers, console proxies, and Secondary Storage VMs.) These DNS servers will be accessed via the management traffic network interface of the System VMs. The private IP address you provide for the pods must have a route to the internal DNS server named here.
  - **Network Domain.** (Optional) If you want to assign a special domain name to the guest VM network, specify the DNS suffix.

- **Guest CIDR.** This is the CIDR that describes the IP addresses in use in the guest virtual networks in this zone. For example, 10.1.1.0/24. As a matter of good practice you should set different CIDRs for different zones. This will make it easier to set up VPNs between networks in different zones.
- **Hypervisor.** (Introduced in version 3.0.1) Choose the hypervisor for the first cluster in the zone. You can add clusters with different hypervisors later, after you finish adding the zone.
- **Public.** A public zone is available to all users. A zone that is not public will be assigned to a particular domain. Only users in that domain will be allowed to create guest VMs in this zone.

2. Choose which traffic types will be carried by each physical network.

The traffic types are management, public, guest, and storage traffic. For more information about the types, roll over the icons to display their tool tips, or see *Advanced Zone Network Traffic Types* on page 48. This screen starts out with one network already configured. If you have multiple physical networks, you need to add more. Drag and drop traffic types onto a greyed-out network and it will become active. You can move the traffic icons from one network to another; for example, if the default traffic types shown for Network 1 do not match your actual setup, you can move them down. You can also change the network names if desired.

3. (Introduced in version 3.0.1) Assign a network traffic label to each traffic type on each physical network. These labels must match the labels you have already defined on the hypervisor host. To assign each label, click the Edit button under the traffic type icon within each physical network. A popup dialog appears where you can type the label, then click OK.

These traffic labels will be defined only for the hypervisor selected for the first cluster. For all other hypervisors, the labels can be configured after the zone is created.

(VMware only) If you have enabled Nexus dvSwitch in the environment, you must specify the corresponding Ethernet port profile names as network traffic label for each traffic type on the physical network. For more information on Nexus dvSwitch, see *Configuring a vSphere Cluster with Nexus 1000v Virtual Switch* on page 95.

4. Click Next.

5. Configure the IP range for public Internet traffic. Enter the following details, then click Add. If desired, you can repeat this step to add more public Internet IP ranges. When done, click Next.

- **Gateway.** The gateway in use for these IP addresses.
- **Netmask.** The netmask associated with this IP range.
- **VLAN.** The VLAN that will be used for public traffic.
- **Start IP/End IP.** A range of IP addresses that are assumed to be accessible from the Internet and will be allocated for access to guest networks.

6. In a new zone, CloudPlatform adds the first pod for you. You can always add more pods later. For an overview of what a pod is, see *About Pods* on page 61.

To configure the first pod, enter the following, then click Next:

- **Pod Name.** A name for the pod.
- **Reserved system gateway.** The gateway for the hosts in that pod.
- **Reserved system netmask.** The network prefix that defines the pod's subnet. Use CIDR notation.
- **Start/End Reserved System IP.** The IP range in the management network that CloudPlatform uses to manage various system VMs, such as Secondary Storage VMs, Console Proxy VMs, and DHCP. For more information, see *System Reserved IP Addresses* on page 49.

7. Specify a range of VLAN IDs to carry guest traffic for each physical network (see VLAN Allocation Example on page 124), then click Next.
8. In a new pod, CloudPlatform adds the first cluster for you. You can always add more clusters later. For an overview of what a cluster is, see About Clusters on page 63.

To configure the first cluster, enter the following, then click Next:

- **Hypervisor.** (Version 3.0.0 only; in 3.0.1, this field is read only) Choose the type of hypervisor software that all hosts in this cluster will run. If you choose VMware, additional fields appear so you can give information about a vSphere cluster. For vSphere servers, we recommend creating the cluster of hosts in vCenter and then adding the entire cluster to CloudPlatform. See Add Cluster: vSphere on page 64.
  - **Cluster name.** Enter a name for the cluster. This can be text of your choosing and is not used by CloudPlatform.
9. In a new cluster, CloudPlatform adds the first host for you. You can always add more hosts later. For an overview of what a host is, see About Hosts on page 67.

Before you can configure the host, you need to install the hypervisor software on the host. You will need to know which version of the hypervisor software version is supported by CloudPlatform and what additional configuration is required to ensure the host will work with CloudPlatform. To find these installation details, see:

When you deploy CloudPlatform, the hypervisor host must not have any VMs already running.

- Citrix XenServer Installation for CloudPlatform on page 76
- VMware vSphere Installation and Configuration on page 87
- KVM Installation and Configuration on page 108
- Oracle VM (OVM) Installation and Configuration on page 112

To configure the first host, enter the following, then click Next:

- **Host Name.** The DNS name or IP address of the host.
  - **Username.** Usually root.
  - **Password.** This is the password for the user named above (from your XenServer or KVM install).
  - **Host Tags.** (Optional) Any labels that you use to categorize hosts for ease of maintenance. For example, you can set to the cloud's HA tag (set in the ha.tag global configuration parameter) if you want this host to be used only for VMs with the "high availability" feature enabled. For more information, see HA-Enabled Virtual Machines as well as HA for Hosts, both in the Administration Guide.
10. In a new cluster, CloudPlatform adds the first primary storage server for you. You can always add more servers later. For an overview of what primary storage is, see About Primary Storage on page 71.

To configure the first primary storage server, enter the following, then click Next:

- **Name.** The name of the storage device.
- **Protocol.** For XenServer, choose either NFS, iSCSI, or PreSetup. For KVM, choose NFS or SharedMountPoint. For vSphere choose either VMFS (iSCSI or FiberChannel) or NFS. The remaining fields in the screen vary depending on what you choose here.

NFS	<ul style="list-style-type: none"> <li>• <b>Server.</b> The IP address or DNS name of the storage device.</li> <li>• <b>Path.</b> The exported path from the server.</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> </ul> <p>The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</p>
iSCSI	<ul style="list-style-type: none"> <li>• <b>Server.</b> The IP address or DNS name of the storage device.</li> <li>• <b>Target IQN.</b> The IQN of the target. For example, iqn.1986-03.com.sun:02:01ec9bb549-1271378984</li> <li>• <b>Lun #.</b> The LUN number. For example, 3.</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> </ul> <p>The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</p>
PreSetup	<ul style="list-style-type: none"> <li>• <b>Server.</b> The IP address or DNS name of the storage device.</li> <li>• <b>SR Name-Label.</b> Enter the name-label of the SR that has been set up outside CloudPlatform.</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> </ul> <p>The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</p>
SharedMountPoint	<ul style="list-style-type: none"> <li>• <b>Path.</b> The path on each host that is where this primary storage is mounted. For example, "/mnt/primary".</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> </ul> <p>The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</p>
VMFS	<ul style="list-style-type: none"> <li>• <b>Server.</b> The IP address or DNS name of the vCenter server.</li> <li>• <b>Path.</b> A combination of the datacenter name and the datastore name. The format is "/" datacenter name "/" datastore name. For example, "/cloud.dc.VM/cluster1datastore".</li> <li>• <b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</li> </ul> <p>The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other</p>

	clusters in the Zone must also provide primary storage that has tags T1 and T2.
--	---

- 11.** In a new zone, CloudPlatform adds the first secondary storage server for you. You can always add more servers later. For an overview of what secondary storage is, see [About Secondary Storage](#) on page 73.

Before you can fill out this screen, you need to prepare the secondary storage by setting up NFS shares and installing the latest CloudPlatform System VM template. See [Adding Secondary Storage](#) on page 73.

To configure the first secondary storage server, enter the following, then click Next:

- **NFS Server.** The IP address of the server.
- **Path.** The exported path from the server.

- 12.** Click Launch.

## Add More Pods (Optional)

---

When you created a new zone, CloudPlatform adds the first pod for you. You can add more pods at any time using the procedure in this section.

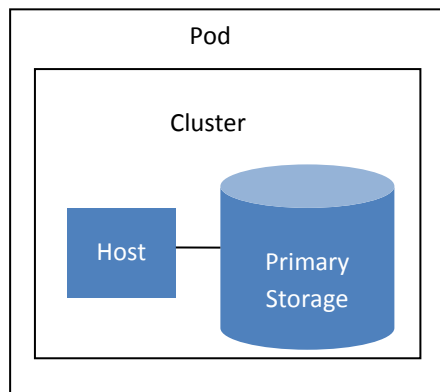
### About Pods

---

A pod often represents a single rack. Hosts in the same pod are in the same subnet.

A pod is the second-largest organizational unit within a CloudPlatform deployment. Pods are contained within zones. Each zone can contain one or more pods.

A pod consists of one or more clusters of hosts and one or more primary storage servers.



**A simple pod**

Pods are not visible to the end user.

### Adding a Pod

---

These steps assume you have already logged in to the CloudPlatform UI (see page 42).

1. In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone to which you want to add a pod.
2. Click the Compute and Storage tab. In the Pods node of the diagram, click View All.
3. Click Add Pod.

4. Enter the following details in the dialog.
  - **Name.** The name of the pod.
  - **Gateway.** The gateway for the hosts in that pod.
  - **Netmask.** The network prefix that defines the pod's subnet. Use CIDR notation.
  - **Start/End Reserved System IP.** The IP range in the management network that CloudPlatform uses to manage various system VMs, such as Secondary Storage VMs, Console Proxy VMs, and DHCP. For more information, see System Reserved IP Addresses on page 49.
5. Click OK.

## Add More Clusters (Optional)

---

You need to tell CloudPlatform about the hosts that it will manage. Hosts exist inside clusters, so before you begin adding hosts to the cloud, you must add at least one cluster.

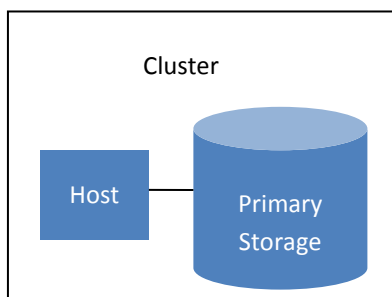
### About Clusters

---

A cluster provides a way to group hosts. To be precise, a cluster is a XenServer server pool, a set of KVM servers, a set of OVM hosts, or a VMware cluster preconfigured in vCenter. The hosts in a cluster all have identical hardware, run the same hypervisor, are on the same subnet, and access the same shared primary storage. Virtual machine instances (VMs) can be live-migrated from one host to another within the same cluster, without interrupting service to the user.

A cluster is the third-largest organizational unit within a CloudPlatform deployment. Clusters are contained within pods, and pods are contained within zones. Size of the cluster is limited by the underlying hypervisor, although the CloudPlatform recommends less in most cases; see Best Practices on page 153.

A cluster consists of one or more hosts and one or more primary storage servers.



**A simple cluster**

CloudPlatform allows multiple clusters in a cloud deployment.

Every VMware cluster is managed by a vCenter server. Administrator must register the vCenter server with CloudPlatform. There may be multiple vCenter servers per zone. Each vCenter server may manage multiple VMware clusters.

Even when local storage is used, clusters are still required. There is just one host per cluster.

### Add Cluster: KVM or XenServer

---

These steps assume you have already installed the hypervisor on the hosts (see Citrix XenServer Installation for CloudPlatform on page 76 or KVM Installation and Configuration on page 108 for essential configuration requirements) and logged in to the CloudPlatform UI (see page 42).

To add a cluster of hosts that run KVM or XenServer:

1. In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone in which you want to add the cluster.
2. Click the Compute tab.
3. In the Clusters node of the diagram, click View All.
4. Click Add Cluster.
5. Choose the hypervisor type for this cluster.
6. Choose the pod in which you want to create the cluster.
7. Enter a name for the cluster. This can be text of your choosing and is not used by CloudPlatform.
8. Click OK.

## Add Cluster: OVM

---

To add a Cluster of hosts that run Oracle VM (OVM):

1. Add a companion non-OVM cluster to the Pod. This cluster provides an environment where the CloudPlatform System VMs can run. You should have already installed a non-OVM hypervisor on at least one Host to prepare for this step. Depending on which hypervisor you used:
  - For VMWare, follow the steps in Add Cluster: vSphere on page 64. When finished, return here and continue with the next step.
  - For KVM or XenServer, follow the steps in Add Cluster: KVM or XenServer on page 63. When finished, return here and continue with the next step.
2. In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone in which you want to add the cluster.
3. Click the Compute tab. In the Pods node, click View All. Select the same pod you used in step 1.
4. Click View Clusters, then click Add Cluster.
5. The Add Cluster dialog will appear.
6. In Hypervisor, choose OVM.
7. In Cluster, enter a name for the cluster.
8. Click Add.

## Add Cluster: vSphere

---

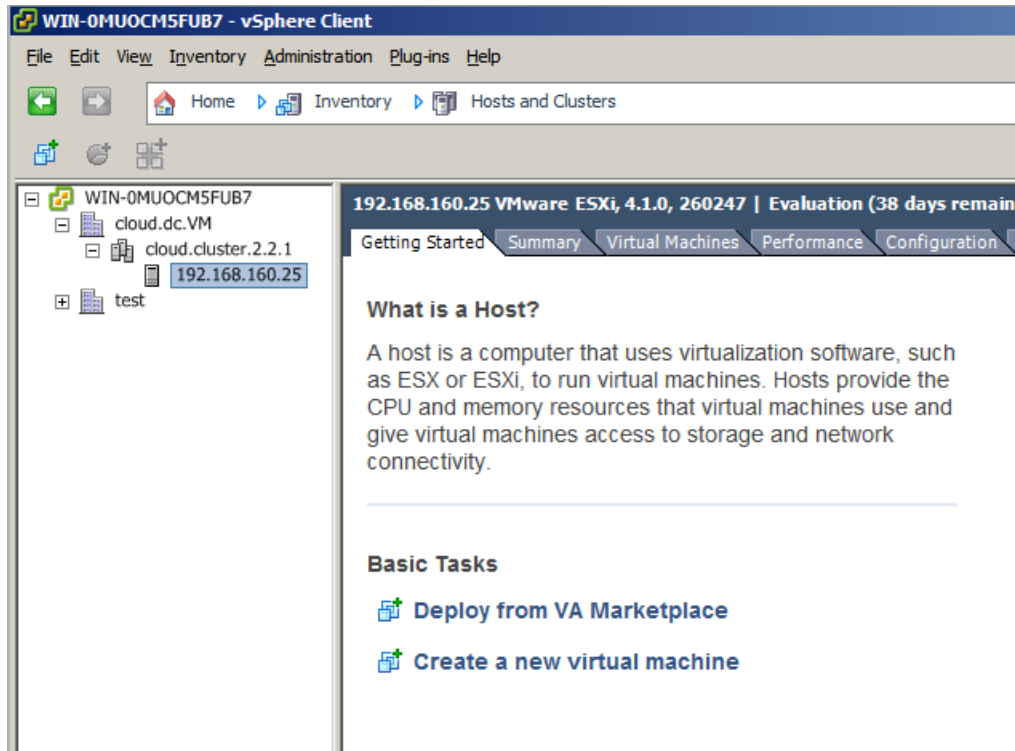
Host management for vSphere is done through a combination of vCenter and the CloudPlatform admin UI. CloudPlatform requires that all hosts be in a CloudPlatform cluster, but the cluster may consist of a single host. As an administrator you must decide if you would like to use clusters of one host or of multiple hosts. Clusters of multiple hosts allow for features like live migration. Clusters also require shared storage such as NFS or iSCSI.

For vSphere servers, we recommend creating the cluster of hosts in vCenter and then adding the entire cluster to CloudPlatform. Follow these requirements:

- Do not put more than 8 hosts in a vSphere cluster.
- Make sure the hypervisor hosts do not have any VMs already running before you add them to CloudPlatform.

To add a vSphere cluster to CloudPlatform:

1. Create the cluster of hosts in vCenter. Follow the vCenter instructions to do this. You will create a cluster that looks something like this in vCenter.



2. Log in to the UI (see page 42).
3. In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone in which you want to add the cluster.
4. Click the Compute tab, and click View All on Pods. Choose the pod to which you want to add the cluster.
5. Click View Clusters.
6. Click Add Cluster.
7. In Hypervisor, choose VMware.
8. Provide the following information in the dialog. The fields below make reference to values from vCenter.
  - **Cluster Name.** Enter the name of the cluster you created in vCenter. For example, "cloud.cluster.2.2.1"
  - **vCenter Host.** Enter the hostname or IP address of the vCenter server.
  - **vCenter Username.** Enter the username that CloudPlatform should use to connect to vCenter. This user must have all administrative privileges.

- **vCenter Password.** Enter the password for the user named above.
- **vCenter Datacenter.** Enter the vCenter datacenter that the cluster is in. For example, "cloud.dc.VM".

If you have enabled Nexus dvSwitch in the environment, the following parameters for dvSwitch configuration are displayed:

- Nexus dvSwitch IP Address: The IP address of the Nexus VSM appliance.
- Nexus dvSwitch Username: The username required to access the Nexus VSM appliance.
- Nexus dvSwitch Password: The password associated with the username specified above.

The screenshot shows a dialog box titled "Add Cluster". It contains the following fields and values:

- \* Zone: ZONE-NEXUS-ADV (dropdown)
- Hypervisor: VMware (dropdown)
- Pod: POD-1 (dropdown)
- \* Cluster Name: doc-cluster
- \* vCenter Host: host-cs-vcenter (highlighted with a yellow border)
- \* vCenter Username: admin
- \* vCenter Password: [masked with dots]
- \* vCenter Datacenter: doc-datacenter
- \* Nexus dvSwitch IP Address: 10.10.105.10
- \* Nexus dvSwitch Username: dv-admin
- \* Nexus dvSwitch Password: [masked with dots]

At the bottom of the dialog are two buttons: "Cancel" and "OK".

For more information on Nexus dvSwitch, see [Configuring a vSphere Cluster with Nexus dvSwitch 1000v](#).

There might be a slight delay while the cluster is provisioned. It will automatically display in the UI.

# Add More Hosts (Optional)

---

After adding at least one cluster to your CloudPlatform configuration, you can start adding hosts.

## About Hosts

---

A host is a single computer. Hosts provide the computing resources that run the guest virtual machines. Each host has hypervisor software installed on it to manage the guest VMs. For example, a Linux KVM-enabled server, a Citrix XenServer server, and an ESXi server are hosts.

The host is the smallest organizational unit within a CloudPlatform deployment. Hosts are contained within clusters, clusters are contained within pods, and pods are contained within zones.

Hosts in a CloudPlatform deployment:

- Provide the CPU, memory, storage, and networking resources needed to host the virtual machines
- Interconnect using a high bandwidth TCP/IP network and connect to the Internet
- May reside in multiple data centers across different geographic locations
- May have different capacities (different CPU speeds, different amounts of RAM, etc.), although the hosts within a cluster must all be homogeneous

Additional hosts can be added at any time to provide more capacity for guest VMs.

CloudPlatform automatically detects the amount of CPU and memory resources provided by the Hosts.

Hosts are not visible to the end user. An end user cannot determine which host their guest has been assigned to.

For a host to function in CloudPlatform, you must do the following:

- Install hypervisor software on the host
- Assign an IP address to the host
- Ensure the host is connected to the CloudPlatform Management Server

## Install Hypervisor Software on Hosts

---

Before adding a host to the CloudPlatform configuration, you must first install your chosen hypervisor on the host. CloudPlatform can manage hosts running VMs under a variety of hypervisors. For a comparison of CloudPlatform supported features for each hypervisor, see [Choosing a Hypervisor: Supported Features](#) on page 121.

For information about which version of your chosen hypervisor is supported, as well as crucial additional steps to configure the hosts for use with CloudPlatform, see the appropriate section:

- [Citrix XenServer Installation for CloudPlatform](#) on page 76

Be sure you have performed the additional CloudPlatform-specific configuration steps described in the hypervisor installation sections. Follow the link for your particular hypervisor.

- VMware vSphere Installation and Configuration on page 87
- KVM Installation and Configuration on page 108
- Oracle VM (OVM) Installation and Configuration on page 112

## Add Hosts to CloudPlatform (XenServer, KVM, or OVM)

---

XenServer, KVM, and Oracle VM (OVM) hosts can be added to a cluster at any time.

### Requirements for XenServer, KVM, and OVM Hosts

Configuration requirements:

- Each cluster must contain only hosts with the identical hypervisor.
- For XenServer, do not put more than 8 hosts in a cluster.
- For KVM, do not put more than 16 hosts in a cluster.

Make sure the hypervisor host does not have any VMs already running before you add it to CloudPlatform.

For hardware requirements, see the appropriate section:

- Citrix XenServer Installation for CloudPlatform on page 76
- KVM Installation and Configuration on page 108
- Oracle VM (OVM) Installation and Configuration on page 112

### XenServer Host Additional Requirements

If network bonding is in use, the administrator must cable the new host identically to other hosts in the cluster.

For all additional hosts to be added to the cluster, run the following command. This will cause the host to join the master in a XenServer pool.

```
# xe pool-join master-address=[master IP] master-username=root master-password=[your password]
```

With all hosts added to the XenServer pool, run the cloud-setup-bond script. This script will complete the configuration and setup of the bonds on the new hosts in the cluster.

1. Copy the script from the Management Server in `/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/cloud-setup-bonding.sh` to the master host and ensure it is executable.
2. Run the script:

```
# ./cloud-setup-bonding.sh
```

When copying and pasting a command, be sure the command has pasted as a single line before executing. Some document viewers may introduce unwanted line breaks in copied text.

## KVM Host Additional Requirements

- If shared mountpoint storage is in use, the administrator should ensure that the new host has all the same mountpoints (with storage mounted) as the other hosts in the cluster.
- Make sure the new host has the same network configuration (guest, private, and public network) as other hosts in the cluster.

## OVM Host Additional Requirements

Before adding a used host in CloudPlatform, as part of the cleanup procedure on the host, be sure to remove `/etc/ovs-agent/db/`.

## Adding a XenServer, KVM, or OVM Host

To add a host, follow these steps:

1. If you have not already done so, install the hypervisor software on the host. You will need to know which version of the hypervisor software version is supported by CloudPlatform and what additional configuration is required to ensure the host will work with CloudPlatform. To find these installation details, see:
  - Citrix XenServer Installation for CloudPlatform on page 76
  - KVM Installation and Configuration on page 108
  - Oracle VM (OVM) Installation and Configuration on page 112
2. Log in to the CloudPlatform UI (see page 42).
3. In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone in which you want to add the host.
4. Click the Compute tab. In the Clusters node, click View All.
5. Click the cluster where you want to add the host.
6. Click View Hosts.
7. Click Add Host.
8. Provide the following information.
  - **Host Name.** The DNS name or IP address of the host.
  - **Username.** Usually root.
  - **Password.** This is the password for the user named above (from your XenServer or KVM install).
  - **Host Tags (Optional).** Any labels that you use to categorize hosts for ease of maintenance. For example, you can set to the cloud's HA tag (set in the `ha.tag` global configuration parameter) if you want this host to be used only for VMs with the "high availability" feature enabled. For more information, see HA-Enabled Virtual Machines as well as HA for Hosts, both in the Administration Guide.

There may be a slight delay while the host is provisioned. It should automatically display in the UI.

9. Repeat for additional hosts.

## Add Hosts (vSphere)

---

For vSphere servers, we recommend creating the cluster of hosts in vCenter and then adding the entire cluster to CloudPlatform. See [Add Cluster: vSphere](#) on page 64.

# Add Primary Storage

---

## About Primary Storage

---

Primary storage is associated with a cluster, and it stores the disk volumes for all the VMs running on hosts in that cluster. You can add multiple primary storage servers to a cluster. At least one is required. It is typically located close to the hosts for increased performance.

The CloudPlatform platform is designed to work with all standards-compliant iSCSI and NFS servers that are supported by the underlying hypervisor, including, for example:

- Dell EqualLogic™ for iSCSI
- Network Appliances filers for NFS and iSCSI
- Scale Computing for NFS

If you intend to use only local disk for your installation, you can skip to Add Secondary Storage on page 72.

## System Requirements for Primary Storage

---

Hardware requirements:

- Any standards-compliant iSCSI or NFS server that is supported by the underlying hypervisor.
- The storage server should be a machine with a large number of disks. The disks should ideally be managed by a hardware RAID controller.
- Minimum required capacity depends on your needs.

When setting up primary storage, follow these restrictions:

- Primary storage cannot be added until a host has been added to the cluster.
- If you do not provision shared storage for primary storage, you will not be able to create additional volumes.
- If you do not provision shared primary storage, you must set the global configuration parameter `system.vm.local.storage.required` to `true`, or else you will not be able to start VMs.

## Adding Primary Storage

---

When you create a new zone, the first primary storage is added as part of that procedure. You can add primary storage servers at any time, such as when adding a new cluster or adding more servers to an existing cluster.

1. Log in to the CloudPlatform UI (see page 42).

### WARNING

Be sure there is nothing stored on the server. Adding the server to CloudPlatform will destroy any existing data.

2. In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone in which you want to add the primary storage.
3. Click the Compute tab.
4. In the Primary Storage node of the diagram, click View All.
5. Click Add Primary Storage.
6. Provide the following information in the dialog. The information required varies depending on your choice in Protocol.
  - **Pod.** The pod for the storage device.
  - **Cluster.** The cluster for the storage device.
  - **Name.** The name of the storage device.
  - **Protocol.** For XenServer, choose either NFS, iSCSI, or PreSetup. For KVM, choose NFS or SharedMountPoint. For vSphere choose either VMFS (iSCSI or FiberChannel) or NFS.
  - **Server (for NFS, iSCSI, or PreSetup).** The IP address or DNS name of the storage device.
  - **Server (for VMFS).** The IP address or DNS name of the vCenter server.
  - **Path (for NFS).** In NFS this is the exported path from the server.
  - **Path (for VMFS).** In vSphere this is a combination of the datacenter name and the datastore name. The format is "/" datacenter name "/" datastore name. For example, "/cloud.dc.VM/cluster1datastore".
  - **Path (for SharedMountPoint).** With KVM this is the path on each host that is where this primary storage is mounted. For example, "/mnt/primary".
  - **SR Name-Label (for PreSetup).** Enter the name-label of the SR that has been set up outside CloudPlatform.
  - **Target IQN (for iSCSI).** In iSCSI this is the IQN of the target. For example, iqn.1986-03.com.sun:02:01ec9bb549-1271378984
  - **Lun # (for iSCSI).** In iSCSI this is the LUN number. For example, 3.
  - **Tags (optional).** The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.

The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.

7. Click OK.

# Add Secondary Storage

---

## About Secondary Storage

---

Secondary storage is associated with a zone, and it stores the following:

- Templates – OS images that can be used to boot VMs and can include additional configuration information, such as installed applications
- ISO images – disc images containing data or bootable media for operating systems
- Disk volume snapshots – saved copies of VM data which can be used for data recovery or to create new templates

The items in zone-based NFS secondary storage are available to all hosts in the zone. CloudPlatform manages the allocation of guest virtual disks to particular primary storage devices.

To make items in secondary storage available to all hosts throughout the cloud, you can add OpenStack Object Storage (Swift, <http://swift.openstack.org>) in addition to the zone-based NFS secondary storage. When using Swift, you configure Swift storage for the entire CloudPlatform, then set up NFS secondary storage for each zone as usual. The NFS storage in each zone acts as a staging area through which all templates and other secondary storage data pass before being forwarded to Swift. The Swift storage acts as a cloud-wide resource, making templates and other data available to any zone in the cloud. There is no hierarchy in the Swift storage, just one Swift container per storage object. Any secondary storage in the whole cloud can pull a container from Swift at need. It is not necessary to copy templates and snapshots from one zone to another, as would be required when using zone NFS alone. Everything is available everywhere.

## System Requirements for Secondary Storage

---

- NFS storage appliance or Linux NFS server
- (Optional) OpenStack Object Storage (Swift) (see <http://swift.openstack.org>)
- 100GB minimum capacity
- A secondary storage device must be located in the same zone as the guest VMs it serves.
- Each Secondary Storage server must be available to all hosts in the zone.

## Adding Secondary Storage

---

When you create a new zone, the first secondary storage is added as part of that procedure. You can add secondary storage servers at any time to add more servers to an existing zone.

1. If you are going to use Swift for cloud-wide secondary storage, you must add the Swift storage to CloudPlatform before you add the local zone secondary storage servers. See Adding a Zone on page 51.

### WARNING

Be sure there is nothing stored on the server. Adding the server to CloudPlatform will destroy any existing data.

2. To prepare for local zone secondary storage, you should have created and mounted an NFS share during Management Server installation. See [Prepare NFS Shares](#) on page 26.
3. Make sure you prepared the system VM template during Management Server installation. See [Prepare the System VM Template](#) on page 29.
4. Now that the secondary storage server for per-zone storage is prepared, add it to CloudPlatform. Secondary storage is added as part of the procedure for adding a new zone. See [Add a Zone](#) on page 46.

# Initialization and Testing

---

After everything is configured, CloudPlatform will perform its initialization. This can take 30 minutes or more, depending on the speed of your network. When the initialization has completed successfully, the administrator's Dashboard should be displayed in the CloudPlatform UI.

1. Verify that the system is ready. In the left navigation bar, select Templates. Click on the CentOS 5.5 (64bit) no Gui (KVM) template. Check to be sure that the status is "Download Complete." Do not proceed to the next step until this status is displayed.
2. Go to the Instances tab, and filter by My Instances.
3. Click Add Instance and follow the steps in the wizard.
  - a. Choose the zone you just added.
  - b. In the template selection, choose the template to use in the VM. If this is a fresh installation, likely only the provided CentOS template is available.
  - c. Select a service offering. Be sure that the hardware you have allows starting the selected service offering.
  - d. In data disk offering, if desired, add another data disk. This is a second volume that will be available to but not mounted in the guest. For example, in Linux on XenServer you will see /dev/xvdb in the guest after rebooting the VM. A reboot is not required if you have a PV-enabled OS kernel in use.
  - e. In default network, choose the primary network for the guest. In a trial installation, you would have only one option here.
  - f. Optionally give your VM a name and a group. Use any descriptive text you would like.
  - g. Click Launch VM. Your VM will be created and started. It might take some time to download the template and complete the VM startup. You can watch the VM's progress in the Instances screen.

4. To use the VM, click the View Console button.



For more information about using VMs, including instructions for how to allow incoming network traffic to the VM, start, stop, and delete VMs, and move a VM from one host to another, see [Working With Virtual Machines](#) in the Administrator's Guide.

Congratulations! You have successfully completed a CloudPlatform Installation.

If you decide to grow your deployment, you can add more hosts, primary storage, zones, pods, and clusters.

# Citrix XenServer Installation for CloudPlatform

---

If you want to use the Citrix XenServer hypervisor to run guest virtual machines, install XenServer 6.0 (for CloudStack 3.0.0) or XenServer 6.0.2 (for CloudStack 3.0.1) on the host(s) in your cloud. For an initial installation, follow the steps below. If you have previously installed XenServer and want to upgrade to another version, see [Upgrading XenServer Versions](#) on page 84.

## System Requirements for XenServer Hosts

---

- The host must be certified as compatible with XenServer 5.6 SP2 or 6.0.2. See the Citrix Hardware Compatibility Guide: <http://hcl.xensource.com>
- All hosts must be 64-bit and must support HVM (Intel-VT or AMD-V enabled in BIOS).
- All hosts within a cluster must be homogenous. That means the CPUs must be of the same type, count, and feature flags.
- You must re-install Citrix XenServer if you are going to re-use a host from a previous install.
- 64-bit x86 CPU (more cores results in better performance)
- Hardware virtualization support required
- 4 GB of memory
- 36 GB of local disk
- At least 1 NIC
- Statically allocated IP Address
- Be sure all the hotfixes provided by the hypervisor vendor are applied. Track the release of hypervisor patches through your hypervisor vendor's support channel, and apply patches as soon as possible after they are released. CloudPlatform will not track or notify you of required hypervisor patches. It is essential that your hosts are completely up to date with the provided hypervisor patches. The hypervisor vendor is likely to refuse to support any system that is not up to date with patches. For more information, see [Highly Recommended Hotfixes for XenServer](#) in the CloudPlatform Knowledge Base.

**WARNING**

The lack of up-to-date hotfixes can lead to data corruption and lost VMs.

## XenServer Installation Steps

---

1. From <https://www.citrix.com/English/ss/downloads/>, download the appropriate version of XenServer for your CloudPlatform version (see System Requirements for XenServer Hosts on page 76). Install it using the Citrix XenServer Installation Guide.

2. After installation, perform the following configuration steps, which are described in the next few sections:

Required	Optional
Configure XenServer dom0 Memory (p. 77)	Install CSP package (p. 78)
Username and password (p. 77)	Set up SR if not using NFS, iSCSI, or local disk for primary storage (p. 79)
Time synchronization (p. 77)	iSCSI multipath setup (p. 80)
Licensing (p. 78)	Physical networking setup, including NIC bonding (p. 80)

---

## Configure XenServer dom0 Memory

Configure the XenServer dom0 settings to allocate more memory to dom0. This can enable XenServer to handle larger numbers of virtual machines. We recommend 2940 MB of RAM for XenServer dom0. For instructions on how to do this, see <http://support.citrix.com/article/CTX126531>. The article refers to XenServer 5.6, but the same information applies to XenServer 6.0.

---

## Username and Password

All XenServers in a cluster must have the same username and password as configured in CloudPlatform.

---

## Time Synchronization

The host must be set to use NTP. All hosts in a pod must have the same time.

1. Install NTP.

```
# yum install ntp
```

2. Edit the NTP configuration file to point to your NTP server.

```
# vi /etc/ntp.conf
```

Add one or more server lines in this file with the names of the NTP servers you want to use. For example:

```
server 0.xenserver.pool.ntp.org
server 1.xenserver.pool.ntp.org
server 2.xenserver.pool.ntp.org
server 3.xenserver.pool.ntp.org
```

3. Restart the NTP client.

```
# service ntpd restart
```

4. Make sure NTP will start again upon reboot.

```
# chkconfig ntpd on
```

## Licensing

---

Citrix XenServer Free version provides 30 days usage without a license. Following the 30 day trial, XenServer requires a free activation and license. You can choose to install a license now or skip this step. If you skip this step, you will need to install a license when you activate and license the XenServer.

### Getting and Deploying a License

If you choose to install a license now you will need to use the XenCenter to activate and get a license.

1. In XenCenter, click Tools > License manager.
2. Select your XenServer and select Activate Free XenServer.
3. Request a license.

You can install the license with XenCenter or using the xe command line tool.

## Install CloudPlatform XenServer Support Package (CSP)

---

(Optional)

To enable security groups, elastic load balancing, and elastic IP on XenServer, download and install the CloudPlatform XenServer Support Package (CSP). After installing XenServer, perform the following additional steps on each XenServer host.

1. Download the CSP software onto the XenServer host from one of the following links:

For XenServer 6.0.2 (can be used with CloudPlatform 3.0.3 and greater):

<http://download.cloud.com/releases/3.0.1/XS-6.0.2/xenserver-cloud-supply.tgz>

For XenServer 5.6 SP2 (can be used with CloudStack 3.0.2 and CloudPlatform 3.0.3 - 3.0.5):

<http://download.cloud.com/releases/2.2.0/xenserver-cloud-supply.tgz>

For XenServer 6.0 (used with CloudStack 3.0.0 only):

<http://download.cloud.com/releases/3.0/xenserver-cloud-supply.tgz>

2. Extract the file:

```
# tar xf xenserver-cloud-supply.tgz
```

3. Run the following script:

```
# xe-install-supplemental-pack xenserver-cloud-supply.iso
```

4. If the XenServer host is part of a zone that uses basic networking, disable Open vSwitch (OVS):

```
# xe-switch-network-backend bridge
```

Restart the host machine when prompted.

The XenServer host is now ready to be added to CloudPlatform.

## Primary Storage Setup for XenServer

---

CloudPlatform natively supports NFS, iSCSI and local storage. If you are using one of these storage types, there is no need to create the XenServer Storage Repository ("SR").

If, however, you would like to use storage connected via some other technology, such as FiberChannel, you must set up the SR yourself. To do so, perform the following steps. If you have your hosts in a XenServer pool, perform the steps on the master node. If you are working with a single XenServer which is not part of a cluster, perform the steps on that XenServer.

1. Connect FiberChannel cable to all hosts in the cluster and to the FiberChannel storage host.
2. Rescan the SCSI bus. Either use the following command or use XenCenter to perform an HBA rescan.

```
# scsi-rescan
```

3. Repeat step 2 on every host.
4. Check to be sure you see the new SCSI disk.

```
# ls /dev/disk/by-id/scsi-360a98000503365344e6f6177615a516b -l
```

The output should look like this, although the specific file name will be different (scsi-<scsiID>):

```
lrwxrwxrwx 1 root root 9 Mar 16 13:47
/dev/disk/by-id/scsi-360a98000503365344e6f6177615a516b -> ../../sdc
```

5. Repeat step 4 on every host.
6. On the storage server, run this command to get a unique ID for the new SR.

```
# uuidgen
```

The output should look like this, although the specific ID will be different:

```
e6849e96-86c3-4f2c-8fcc-350cc711be3d
```

7. Create the FiberChannel SR. In name-label, use the unique ID you just generated.

```
# xe sr-create type=lvMohba shared=true
  device-config:SCSIId=360a98000503365344e6f6177615a516b
  name-label="e6849e96-86c3-4f2c-8fcc-350cc711be3d"
```

This command returns a unique ID for the SR, like the following example (your ID will be different):

```
7a143820-e893-6c6a-236e-472da6ee66bf
```

8. To create a human-readable description for the SR, use the following command. In `uuid`, use the SR ID returned by the previous command. In `name-description`, set whatever friendly text you prefer.

```
# xe sr-param-set uuid=7a143820-e893-6c6a-236e-472da6ee66bf
  name-description="Fiber Channel storage repository"
```

Make note of the values you will need when you add this storage to CloudPlatform later (see [Add Primary Storage](#) on page 71). In the Add Primary Storage dialog, in Protocol, you will choose PreSetup. In SR Name-Label, you will enter the name-label you set earlier (in this example, `e6849e96-86c3-4f2c-8fcc-350cc711be3d`).

9. (Optional) If you want to enable multipath I/O on a FiberChannel SAN, refer to the documentation provided by the SAN vendor.

---

## iSCSI Multipath Setup for XenServer (Optional)

---

When setting up the storage repository on a Citrix XenServer, you can enable multipath I/O, which uses redundant physical components to provide greater reliability in the connection between the server and the SAN. To enable multipathing, use a SAN solution that is supported for Citrix servers and follow the procedures in Citrix documentation. The following links provide a starting point:

- <http://support.citrix.com/article/CTX118791>
- <http://support.citrix.com/article/CTX125403>

You can also ask your SAN vendor for advice about setting up your Citrix repository for multipathing.

Make note of the values you will need when you add this storage to the CloudPlatform later (see [Add Primary Storage](#) on page 71). In the Add Primary Storage dialog, in Protocol, you will choose PreSetup. In SR Name-Label, you will enter the same name used to create the SR.

If you encounter difficulty, address the support team for the SAN provided by your vendor. If they are not able to solve your issue, see [Contacting Support](#) on page 161.

---

## Physical Networking Setup for XenServer

---

Once XenServer has been installed, you may need to do some additional network configuration. At this point in the installation, you should have a plan for what NICs the host will have and what traffic each NIC will carry. The NICs should be cabled as necessary to implement your plan.

If you plan on using NIC bonding, the NICs on all hosts in the cluster must be cabled exactly the same. For example, if `eth0` is in the private bond on one host in a cluster, then `eth0` must be in the private bond on all hosts in the cluster.

The IP address assigned for the management network interface must be static. It can be set on the host itself or obtained via static DHCP.

CloudPlatform configures network traffic of various types to use different NICs or bonds on the XenServer host. You can control this process and provide input to the Management Server through the use of XenServer network name labels. The name labels are placed on physical interfaces or bonds and configured in CloudPlatform. In some simple cases the name labels are not required.

## Configuring Public Network with a Dedicated NIC for XenServer (Optional)

CloudPlatform supports the use of a second NIC (or bonded pair of NICs, described in NIC Bonding for XenServer (Optional) on page 82) for the public network. If bonding is not used, the public network can be on any NIC and can be on different NICs on the hosts in a cluster. For example, the public network can be on eth0 on node A and eth1 on node B. However, the XenServer name-label for the public network must be identical across all hosts. The following examples set the network label to “cloud-public”. After the management server is installed and running you must configure it with the name of the chosen network label (e.g. “cloud-public”); this is discussed in Management Server on page 21.

If you are using two NICs bonded together to create a public network, see NIC Bonding.

If you are using a single dedicated NIC to provide public network access, follow this procedure on each new host that is added to CloudPlatform before adding the host.

1. Run `xe network-list` and find the public network. This is usually attached to the NIC that is public. Once you find the network make note of its UUID. Call this <UUID-Public>.
2. Run the following command.

```
# xe network-param-set name-label=cloud-public uuid=<UUID-Public>
```

## Configuring Multiple Guest Networks for XenServer (Optional)

CloudPlatform supports the use of multiple guest networks with the XenServer hypervisor. Each network is assigned a name-label in XenServer. For example, you might have two networks with the labels “cloud-guest” and “cloud-guest2”. After the management server is installed and running, you must add the networks and use these labels so that CloudPlatform is aware of the networks.

Follow this procedure on each new host before adding the host to CloudPlatform:

1. Run `xe network-list` and find one of the guest networks. Once you find the network make note of its UUID. Call this <UUID-Guest>.
2. Run the following command, substituting your own name-label and uuid values.

```
# xe network-param-set name-label=<cloud-guestN> uuid=<UUID-Guest>
```

3. Repeat these steps for each additional guest network, using a different name-label and uuid each time.

## Separate Storage Network for XenServer (Optional)

You can optionally set up a separate storage network. This should be done first on the host, before implementing the bonding steps below. This can be done using one or two available NICs. With two NICs bonding may be done as above. It is the administrator's responsibility to set up a separate storage network.

Give the storage network a different name-label than what will be given for other networks.

For the separate storage network to work correctly, it must be the only interface that can ping the primary storage device's IP address. For example, if eth0 is the management network NIC, `ping -I eth0 <primary storage device IP>` must fail. In all deployments, secondary storage devices must be pingable from the management network NIC or bond. If a secondary storage device has been placed on the storage network, it must also be pingable via the storage network NIC or bond on the hosts as well.

You can set up two separate storage networks as well. For example, if you intend to implement iSCSI multipath, dedicate two non-bonded NICs to multipath. Each of the two networks needs a unique name-label.

If no bonding is done, the administrator must set up and name-label the separate storage network on all hosts (masters and slaves).

Here is an example to set up eth5 to access a storage network on 172.16.0.0/24.

```
# xe pif-list host-name-label='hostname' device=eth5
uuid ( RO)                : ab0d3dd4-5744-8fae-9693-a022c7a3471d
                        device ( RO): eth5
# xe pif-reconfigure-ip DNS=172.16.3.3 gateway=172.16.0.1 IP=172.16.0.55 mode=static
netmask=255.255.255.0 uuid=ab0d3dd4-5744-8fae-9693-a022c7a3471d
```

## NIC Bonding for XenServer (Optional)

XenServer supports Source Level Balancing (SLB) NIC bonding. Two NICs can be bonded together to carry public, private, and guest traffic, or some combination of these. Separate storage networks are also possible. Here are some example supported configurations:

- 2 NICs on private, 2 NICs on public, 2 NICs on storage
- 2 NICs on private, 1 NIC on public, storage uses management network
- 2 NICs on private, 2 NICs on public, storage uses management network
- 1 NIC for private, public, and storage

All NIC bonding is optional.

XenServer expects all nodes in a cluster will have the same network cabling and same bonds implemented. In an installation the master will be the first host that was added to the cluster and the slave hosts will be all subsequent hosts added to the cluster. The bonds present on the master set the expectation for hosts added to the cluster later. The procedure to set up bonds on the master and slaves are different, and are described below. There are several important implications of this:

- You must set bonds on the first host added to a cluster. Then you must use xe commands as below to establish the same bonds in the second and subsequent hosts added to a cluster.
- Slave hosts in a cluster must be cabled exactly the same as the master. For example, if eth0 is in the private bond on the master, it must be in the management network for added slave hosts.

## Management Network Bonding

The administrator must bond the management network NICs prior to adding the host to CloudPlatform.

### Creating a Private Bond on the First Host in the Cluster

Use the following steps to create a bond in XenServer. These steps should be run on only the first host in a cluster. This example creates the cloud-private network with two physical NICs (eth0 and eth1) bonded into it.

1. Find the physical NICs that you want to bond together.

```
# xe pif-list host-name-label='hostname' device=eth0
# xe pif-list host-name-label='hostname' device=eth1
```

These command shows the eth0 and eth1 NICs and their UUIDs. Substitute the ethX devices of your choice. Call the UUID's returned by the above command slave1-UUID and slave2-UUID.

2. Create a new network for the bond. For example, a new network with name "cloud-private".

**This label is important. CloudPlatform looks for a network by a name you configure. You must use the same name-label for all hosts in the cloud for the management network.**

```
# xe network-create name-label=cloud-private
# xe bond-create network-uuid=[uuid of cloud-private created above]
    pif-uuids=[slave1-uuid],[slave2-uuid]
```

Now you have a bonded pair that can be recognized by CloudPlatform as the management network.

## Public Network Bonding

Bonding can be implemented on a separate, public network. The administrator is responsible for creating a bond for the public network if that network will be bonded and will be separate from the management network.

### Creating a Public Bond on the First Host in the Cluster

These steps should be run on only the first host in a cluster. This example creates the cloud-public network with two physical NICs (eth2 and eth3) bonded into it.

1. Find the physical NICs that you want to bond together.

```
# xe pif-list host-name-label='hostname' device=eth2
# xe pif-list host-name-label='hostname' device=eth3
```

These commands show the eth2 and eth3 NICs and their UUIDs. Substitute the ethX devices of your choice. Call the UUID's returned by the above command slave1-UUID and slave2-UUID.

2. Create a new network for the bond. For example, a new network with name "cloud-public".

**This label is important. CloudPlatform looks for a network by a name you configure. You must use the same name-label for all hosts in the cloud for the public network.**

```
# xe network-create name-label=cloud-public
# xe bond-create network-uuid=[uuid of cloud-public created above]
  pif-uuids=[slave1-uuid],[slave2-uuid]
```

Now you have a bonded pair that can be recognized by CloudPlatform as the public network.

## Adding More Hosts to the Cluster

With the bonds (if any) established on the master, you should add additional, slave hosts. Run the following command for all additional hosts to be added to the cluster. This will cause the host to join the master in a single XenServer pool.

```
# xe pool-join master-address=[master IP] master-username=root
  master-password=[your password]
```

## Complete the Bonding Setup Across the Cluster

With all hosts added to the pool, run the cloud-setup-bond script. This script will complete the configuration and set up of the bonds across all hosts in the cluster.

1. Copy the script from the Management Server in `/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/cloud-setup-bonding.sh` to the master host and ensure it is executable.
2. Run the script:

```
# ./cloud-setup-bonding.sh
```

Now the bonds are set up and configured properly across the cluster.

## Upgrading XenServer Versions

---

This section tells how to upgrade XenServer software on CloudPlatform hosts. The actual upgrade is described in XenServer documentation, but there are some additional steps you must perform before and after the upgrade.

### Tip

Be sure the hardware is certified compatible with the new version of XenServer.

To upgrade XenServer:

1. Upgrade the database. On the Management Server node:
  - a. Back up the database:

```
# mysqldump --user=root --databases cloud > cloud.backup.sql
# mysqldump --user=root --databases cloud_usage > cloud_usage.backup.sql
```

- b. You might need to change the OS type settings for VMs running on the upgraded hosts.

- If you upgraded from XenServer 5.6 GA to XenServer 5.6 SP2, change any VMs that have the OS type CentOS 5.5 (32-bit), Oracle Enterprise Linux 5.5 (32-bit), or Red Hat Enterprise Linux 5.5 (32-bit) to Other Linux (32-bit). Change any VMs that have the 64-bit versions of these same OS types to Other Linux (64-bit).
  - If you upgraded from XenServer 5.6 SP2 to XenServer 6.0.2, change any VMs that have the OS type CentOS 5.6 (32-bit), CentOS 5.7 (32-bit), Oracle Enterprise Linux 5.6 (32-bit), Oracle Enterprise Linux 5.7 (32-bit), Red Hat Enterprise Linux 5.6 (32-bit), or Red Hat Enterprise Linux 5.7 (32-bit) to Other Linux (32-bit). Change any VMs that have the 64-bit versions of these same OS types to Other Linux (64-bit).
  - If you upgraded from XenServer 5.6 to XenServer 6.0.2, do all of the above.
- c. Restart the Management Server and Usage Server. You only need to do this once for all clusters.

```
# service cloud-management start
# service cloud-usage start
```

## 2. Disconnect the XenServer cluster from CloudPlatform.

- Log in to the CloudPlatform UI as root.
- Navigate to the XenServer cluster, and click Actions – Unmanage.
- Watch the cluster status until it shows Unmanaged.

## 3. Log in to one of the hosts in the cluster, and run this command to clean up the VLAN:

```
# . /opt/xensource/bin/cloud-clean-vlan.sh
```

## 4. Still logged in to the host, run the upgrade preparation script:

```
# /opt/xensource/bin/cloud-prepare-upgrade.sh
```

Troubleshooting: If you see the error "can't eject CD," log in to the VM and umount the CD, then run the script again.

## 5. Upgrade the XenServer software on all hosts in the cluster. Upgrade the master first.

- Live migrate all VMs on this host to other hosts. See the instructions for live migration in the Administrator's Guide.

Troubleshooting: You might see the following error when you migrate a VM:

```
[root@xenserver-qa-2-49-4 ~]# xe vm-migrate live=true host=xenserver-qa-2-49-5 vm=i-2-8-VM
You attempted an operation on a VM which requires PV drivers to be installed but the
drivers were not detected.
vm: b6cf79c8-02ee-050b-922f-49583d9f1a14 (i-2-8-VM)
```

To solve this issue, run the following:

```
# /opt/xensource/bin/make_migratable.sh b6cf79c8-02ee-050b-922f-49583d9f1a14
```

- Reboot the host.
- Upgrade to the newer version of XenServer. Use the steps in XenServer documentation.

- d. After the upgrade is complete, copy the following files from the management server to this host, in the directory locations shown below:

Copy this Management Server file...	...to this location on the XenServer host
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/xenserver60/NFSSR.py	/opt/xensource/sm/NFSSR.py
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/setupxenserver.sh	/opt/xensource/bin/setupxenserver.sh
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/make_migratable.sh	/opt/xensource/bin/make_migratable.sh
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/cloud-clean-vlan.sh	/opt/xensource/bin/cloud-clean-vlan.sh

- e. Run the following script:

```
# /opt/xensource/bin/setupxenserver.sh
```

Troubleshooting: If you see the following error message, you can safely ignore it.

```
mv: cannot stat `/etc/cron.daily/logrotate': No such file or directory
```

- f. Plug in the storage repositories (physical block devices) to the XenServer host:

```
# for pbd in `xe pbd-list currently-attached=false | grep ^uuid | awk '{print $NF}'`; do
xe pbd-plug uuid=$pbd ; done
```

Note: If you add a host to this XenServer pool, you need to migrate all VMs on this host to other hosts, and eject this host from XenServer pool.

- Repeat these steps to upgrade every host in the cluster to the same version of XenServer.
- Run the following command on one host in the XenServer cluster to clean up the host tags:

```
# for host in $(xe host-list | grep ^uuid | awk '{print $NF}'); do xe host-param-clear
uuid=$host param-name=tags; done;
```

- Reconnect the XenServer cluster to CloudPlatform.
  - Log in to the CloudPlatform UI as root.
  - Navigate to the XenServer cluster, and click Actions – Manage.
  - Watch the status to see that all the hosts come up.
- After all hosts are up, run the following on one host in the cluster:

```
# /opt/xensource/bin/cloud-clean-vlan.sh
```

When copying and pasting a command, be sure the command has pasted as a single line before executing. Some document viewers may introduce unwanted line breaks in copied text.

# VMware vSphere Installation and Configuration

---

If you want to use the VMware vSphere hypervisor to run guest virtual machines, install vSphere on the host(s) in your cloud.

## System Requirements for vSphere Hosts

---

Software requirements:

- vSphere and vCenter, both version 4.1 or 5.0.

vSphere Standard is recommended. Note however that customers need to consider the CPU constraints in place with vSphere licensing. See [http://www.vmware.com/files/pdf/vsphere\\_pricing.pdf](http://www.vmware.com/files/pdf/vsphere_pricing.pdf) and discuss with your VMware sales representative.

vCenter Server Standard is recommended.

- Be sure all the hotfixes provided by the hypervisor vendor are applied. Track the release of hypervisor patches through your hypervisor vendor's support channel, and apply patches as soon as possible after they are released. CloudPlatform will not track or notify you of required hypervisor patches. It is essential that your hosts are completely up to date with the provided hypervisor patches. The hypervisor vendor is likely to refuse to support any system that is not up to date with patches.

### WARNING

The lack of up-to-date hotfixes can lead to data corruption and lost VMs.

Hardware requirements:

- The host must be certified as compatible with vSphere. See the VMware Hardware Compatibility Guide at <http://www.vmware.com/resources/compatibility/search.php>.
- All hosts must be 64-bit and must support HVM (Intel-VT or AMD-V enabled).
- All hosts within a cluster must be homogenous. That means the CPUs must be of the same type, count, and feature flags.
- 64-bit x86 CPU (more cores results in better performance)
- Hardware virtualization support required
- 4 GB of memory
- 36 GB of local disk
- At least 1 NIC
- Statically allocated IP Address

vCenter Server requirements:

- Processor – 2 CPUs 2.0GHz or higher Intel or AMD x86 processors. Processor may be higher if the database runs on the same machine.

- Memory – 3GB RAM. RAM requirements may be higher if your database runs on the same machine.
- Disk storage – 2GB. Disk requirements may be higher if your database runs on the same machine.
- Microsoft SQL Server 2005 Express disk requirements. The bundled database requires up to 2GB free disk space to decompress the installation archive.
- Networking – 1Gbit or 10Gbit.

For more information, see "vCenter Server and the vSphere Client Hardware Requirements" at [http://pubs.vmware.com/vsp40/wwhelp/wwhimpl/js/html/wwhelp.htm#href=install/c\\_vc\\_hw.html](http://pubs.vmware.com/vsp40/wwhelp/wwhimpl/js/html/wwhelp.htm#href=install/c_vc_hw.html).

Other requirements:

- VMware vCenter Standard Edition 4.1 or 5.0 must be installed and available to manage the vSphere hosts.
- vCenter must be configured to use the standard port 443 so that it can communicate with the CloudPlatform Management Server.
- You must re-install VMware ESXi if you are going to re-use a host from a previous install.
- CloudPlatform requires VMware vSphere 4.1 or 5.0. VMware vSphere 4.0 is not supported.
- All hosts must be 64-bit and must support HVM (Intel-VT or AMD-V enabled). All hosts within a cluster must be homogenous. That means the CPUs must be of the same type, count, and feature flags.
- The CloudPlatform management network **must not** be configured as a separate virtual network. The CloudPlatform management network is the same as the vCenter management network, and will inherit its configuration. See Configure vCenter Management Network on page 93.
- CloudPlatform requires ESXi. ESX is not supported.
- All resources used for CloudPlatform must be used for CloudPlatform only. CloudPlatform cannot share instance of ESXi or storage with other management consoles. Do not share the same storage volumes that will be used by CloudPlatform with a different set of ESXi servers that are not managed by CloudPlatform.
- Put all target ESXi hypervisors in a cluster in a separate Datacenter in vCenter.
- The cluster that will be managed by CloudPlatform should not contain any VMs. Do not run the management server, vCenter or any other VMs on the cluster that is designated for CloudPlatform use. Create a separate cluster for use of CloudPlatform and make sure that they are no VMs in this cluster.
- All the required VLANs must be trunked into all network switches that are connected to the ESXi hypervisor hosts. These would include the VLANs for Management, Storage, vMotion, and guest VLANs. The guest VLAN (used in Advanced Networking; see Network Setup on page 21) is a contiguous range of VLANs that will be managed by CloudPlatform. CloudPlatform supports Nexus 1000v virtual switch. For more information, see Configuring a vSphere Cluster with Nexus 1000v Virtual Switch on page 95.

## Preparation Checklist for VMware

---

For a smoother installation, gather the following information before you start:

- vCenter Checklist on page 89
- Networking Checklist for VMware on page 89
- In addition to the VMware-specific checklists, you should also see Preparation Checklists on page 158

## vCenter Checklist

You will need the following information about vCenter.

vCenter Requirement	Value	Notes
vCenter User		This user must have admin privileges.
vCenter User Password		Password for the above user.
vCenter Datacenter Name		Name of the datacenter.
vCenter Cluster Name		Name of the cluster.

## Networking Checklist for VMware

You will need the following information about the VLAN.

VLAN Information	Value	Notes
ESXi VLAN		VLAN on which all your ESXi hypervisors reside.
ESXi VLAN IP Address		IP Address Range in the ESXi VLAN. One address per Virtual Router is used from this range.
ESXi VLAN IP Gateway		
ESXi VLAN Netmask		
Management Server VLAN		VLAN on which the CloudPlatform Management server is installed.
Public VLAN		VLAN for the Public Network.
Public VLAN Gateway		

Public VLAN Netmask		
Public VLAN IP Address Range		Range of Public IP Addresses available for CloudPlatform use. These addresses will be used for virtual router on CloudPlatform to route private traffic to external networks.
VLAN Range for Customer use		A contiguous range of non-routable VLANs. One VLAN will be assigned for each customer.

---

## vSphere Installation Steps

---

1. Download and purchase vSphere from the VMware Website (<https://www.vmware.com/tryvmware/index.php?p=vmware-vsphere&lp=1>) and install it by following the VMware vSphere Installation Guide.
2. Following installation, perform the following configuration, which are described in the next few sections:

Required	Optional
ESXi host setup	NIC bonding
Configure host physical networking, virtual switch, vCenter Management Network, and extended port range	Multipath storage
Prepare storage for iSCSI	
Configure clusters in vCenter and add hosts to them, or add hosts without clusters to vCenter	

---

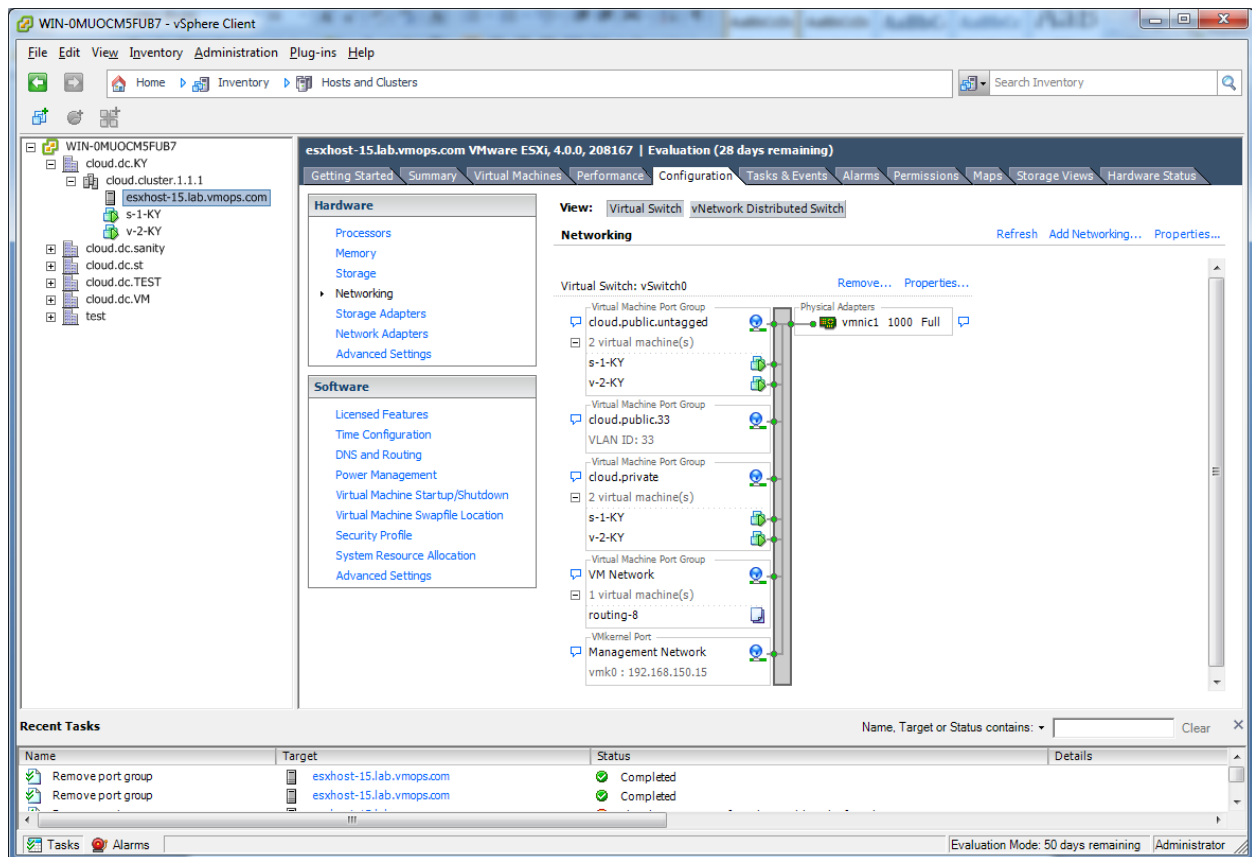
## ESXi Host setup

---

All ESXi hosts should enable CPU hardware virtualization support in BIOS. Please note hardware virtualization support is not enabled by default on most servers.

## Physical Host Networking

You should have a plan for cabling the vSphere hosts. Proper network configuration is required before adding a vSphere host to CloudPlatform. To configure an ESXi host, you can use vClient to add it as standalone host to vCenter first. Once you see the host appearing in the vCenter inventory tree, click the host node in the inventory tree, and navigate to the Configuration tab.



In the host configuration tab, click the “Hardware/Networking” link to bring up the networking configuration page as above.

## Configure Virtual Switch

A default virtual switch vSwitch0 is created. CloudPlatform requires all ESXi hosts in the cloud to use the same set of virtual switch names. If you change the default virtual switch name, you will need to configure one or more CloudPlatform configuration variables as well.

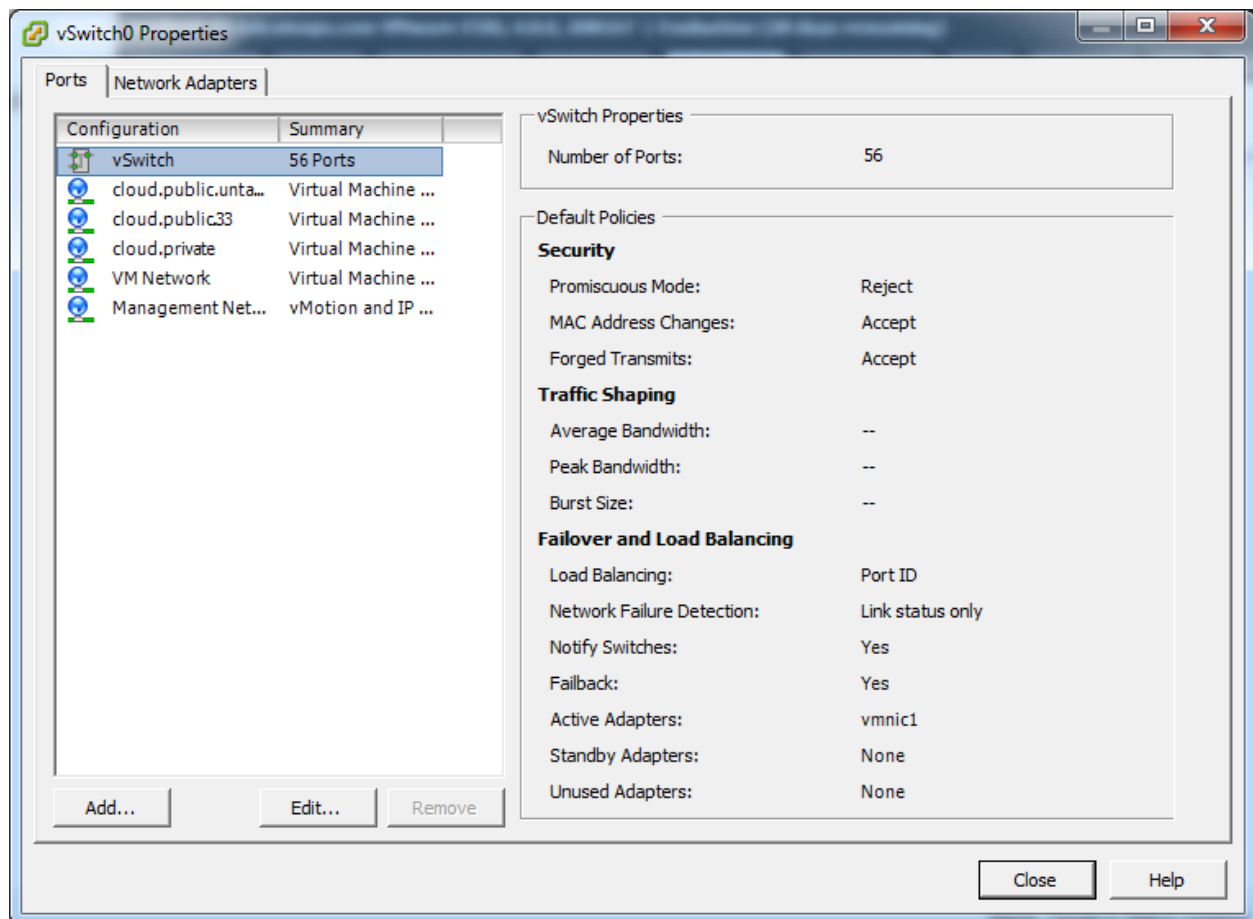
## Separating Traffic

CloudPlatform allows you to use vCenter to configure three separate networks per ESXi host. These networks are identified by the name of the vSwitch they are connected to. The allowed networks for configuration are public (for traffic to/from the public internet), guest (for guest-guest traffic), and private (for management and usually storage traffic). You can use the default virtual switch for all three, or create one or two other vSwitches for those traffic types.

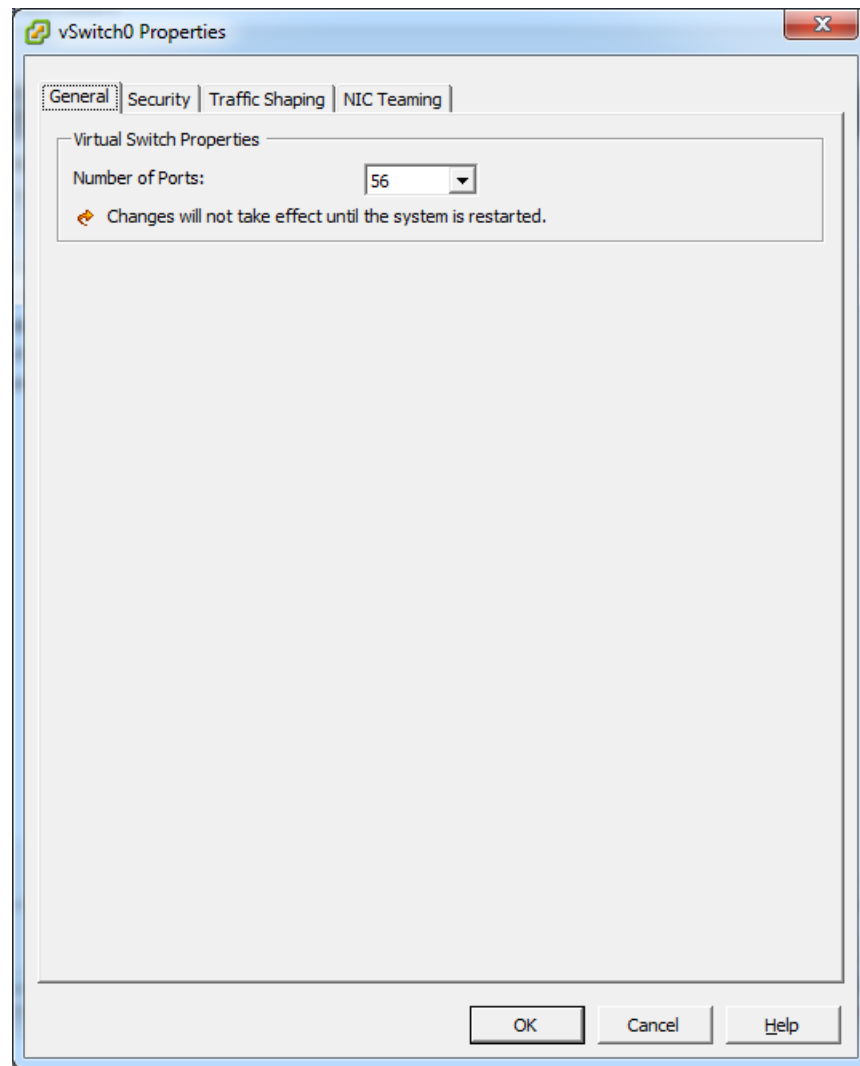
If you want to separate traffic in this way you should first create and configure vSwitches in vCenter according to the vCenter instructions. Take note of the vSwitch names you have used for each traffic type. You will configure CloudPlatform to use these vSwitches.

## Increasing Ports

By default a virtual switch on ESXi hosts is created with 56 ports. We recommend setting it to 4088, the maximum number of ports allowed. To do that, click the “Properties...” link for virtual switch (note this is not the Properties link for Networking).



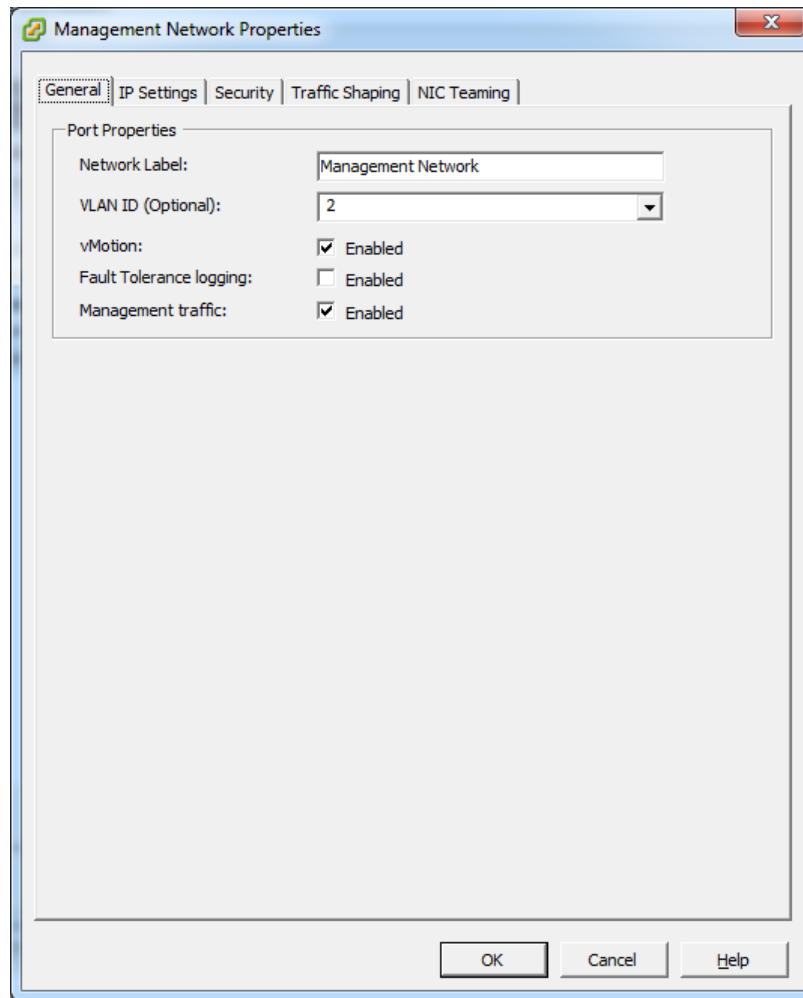
In vSwitch properties dialog, select the vSwitch and click Edit. You should see the following dialog:



In this dialog, you can change the number of switch ports. After you've done that, ESXi hosts are required to reboot in order for the setting to take effect.

## Configure vCenter Management Network

In the vSwitch properties dialog box, you may see a vCenter management network. This same network will also be used as the CloudPlatform management network. CloudPlatform requires the vCenter management network to be configured properly. Select the management network item in the dialog, then click Edit.



Make sure the following values are set:

- VLAN ID set to the desired ID
- vMotion enabled.
- Management traffic enabled.

If the ESXi hosts have multiple VMKernel ports, and ESXi is not using the default value "Management Network" as the management network name, you must follow these guidelines to configure the management network port group so that CloudPlatform can find it:

- Use one label for the management network port across all ESXi hosts.
- In the CloudPlatform UI, go to Configuration – Global Settings and set `vmware.management.portgroup` to the management network label from the ESXi hosts.

## Extend Port Range for CloudPlatform Console Proxy

(Applies only to VMware vSphere version 4.x)

You need to extend the range of firewall ports that the console proxy works with on the hosts. This is to enable the console proxy to work with VMware-based VMs. The default additional port range is 59000-60000. To extend the port range, log in to the VMware ESX service console on each host and run the following commands:

```
esxcfg-firewall -o 59000-60000,tcp,in,vncextras  
esxcfg-firewall -o 59000-60000,tcp,out,vncextras
```

## Configure NIC Bonding for vSphere

NIC bonding on vSphere hosts may be done according to the vSphere installation guide.

## Configuring a vSphere Cluster with Nexus 1000v Virtual Switch

---

CloudPlatform supports Cisco Nexus 1000v dvSwitch (Distributed Virtual Switch) for virtual network configuration in a VMware vSphere environment. This section helps you configure a vSphere cluster with Nexus 1000v virtual switch in a VMware vCenter environment. For information on creating a vSphere cluster, see [VMware vSphere Installation and Configuration](#).

### About Cisco Nexus 1000v Distributed Virtual Switch

The Cisco Nexus 1000V virtual switch is a software-based virtual machine access switch for VMware vSphere environments. It can span multiple hosts running VMware ESXi 4.0 and later. A Nexus virtual switch consists of two components: the Virtual Supervisor Module (VSM) and the Virtual Ethernet Module (VEM). The VSM is a virtual appliance that acts as the switch's supervisor. It controls multiple VEMs as a single network device. The VSM is installed independent of the VEM and is deployed in redundancy mode as pairs or as a standalone appliance. The VEM is installed on each VMware ESXi server to provide packet-forwarding capability. It provides each virtual machine with dedicated switch ports. This VSM-VEM architecture is analogous to a physical Cisco switch's supervisor (standalone or configured in high-availability mode) and multiple linecards architecture.

Nexus 1000v switch uses vEthernet port profiles to simplify network provisioning for virtual machines. There are two types of port profiles: Ethernet port profile and vEthernet port profile. The Ethernet port profile is applied to the physical uplink ports—the NIC ports of the physical NIC adapter on an ESXi server. The vEthernet port profile is associated with the virtual NIC (vNIC) that is plumbed on a guest VM on the ESXi server. The port profiles help the network administrators define network policies which can be reused for new virtual machines. The Ethernet port profiles are created on the VSM and are represented as port groups on the vCenter server.

## Prerequisites and Guidelines

This section discusses prerequisites and guidelines for using Nexus virtual switch in CloudPlatform. Before configuring Nexus virtual switch, ensure that your system meets the following requirements:

- A cluster of servers (ESXi 4.1 or later) is configured in the vCenter.
- Each cluster managed by CloudPlatform is the only cluster in its vCenter datacenter.
- A Cisco Nexus 1000v virtual switch is installed to serve the datacenter that contains the vCenter cluster. This ensures that CloudPlatform doesn't have to deal with dynamic migration of virtual adapters or networks across other existing virtual switches. See [Cisco Nexus 1000V Installation and Upgrade Guide](#) for guidelines on how to install the Nexus 1000v VSM and VEM modules.
- The Nexus 1000v VSM is not deployed on a vSphere host that is managed by CloudPlatform.
- When the maximum number of VEM modules per VSM instance is reached, an additional VSM instance is created before introducing any more ESXi hosts. The limit is 64 VEM modules for each VSM instance.
- CloudPlatform expects that the Management Network of the ESXi host is configured on the standard vSwitch and searches for it in the standard vSwitch. Therefore, ensure that you do not migrate the management network to Nexus 1000v virtual switch during configuration.
- All information given in Nexus 1000v Virtual Switch Preconfiguration on page 96 is followed.

## Nexus 1000v Virtual Switch Preconfiguration

### Preparation Checklist

For a smoother configuration of Nexus 1000v switch, gather the following information before you start:

- vCenter Credentials
- Nexus 1000v VSM IP address
- Nexus 1000v VSM Credentials
- Ethernet port profile names

## vCenter Credentials Checklist

You will need the following information about vCenter:

Nexus vSwitch Requirements	Value	Notes
vCenter IP		The IP address of the vCenter.
Secure HTTP Port Number	433	Port 443 is configured by default; however, you can change the port if needed.
vCenter User ID		The vCenter user with administrator-level privileges. The vCenter User ID is required when you configure the virtual switch in CloudPlatform.
vCenter Password		The password for the vCenter user specified above. The password for this vCenter user is required when you configure the switch in CloudPlatform.

## Network Configuration Checklist

The following information specified in the Nexus Configure Networking screen is displayed in the Details tab of the Nexus dvSwitch in the CloudPlatform UI:

Note: The VLANs used for control, packet, and management port groups can be the same.

Network Requirements	Value	Notes
Control Port Group VLAN ID		The VLAN ID of the Control Port Group. The control VLAN is used for communication between the VSM and the VEMs.
Management Port Group VLAN ID		The VLAN ID of the Management Port Group. The management VLAN corresponds to the mgmt0 interface that is used to establish and maintain the connection between the VSM and VMware vCenter Server.
Packet Port Group VLAN ID		The VLAN ID of the Packet Port Group. The packet VLAN forwards relevant data packets from the VEMs to the VSM.

For more information, see [Cisco Nexus 1000V Getting Started Guide](#).

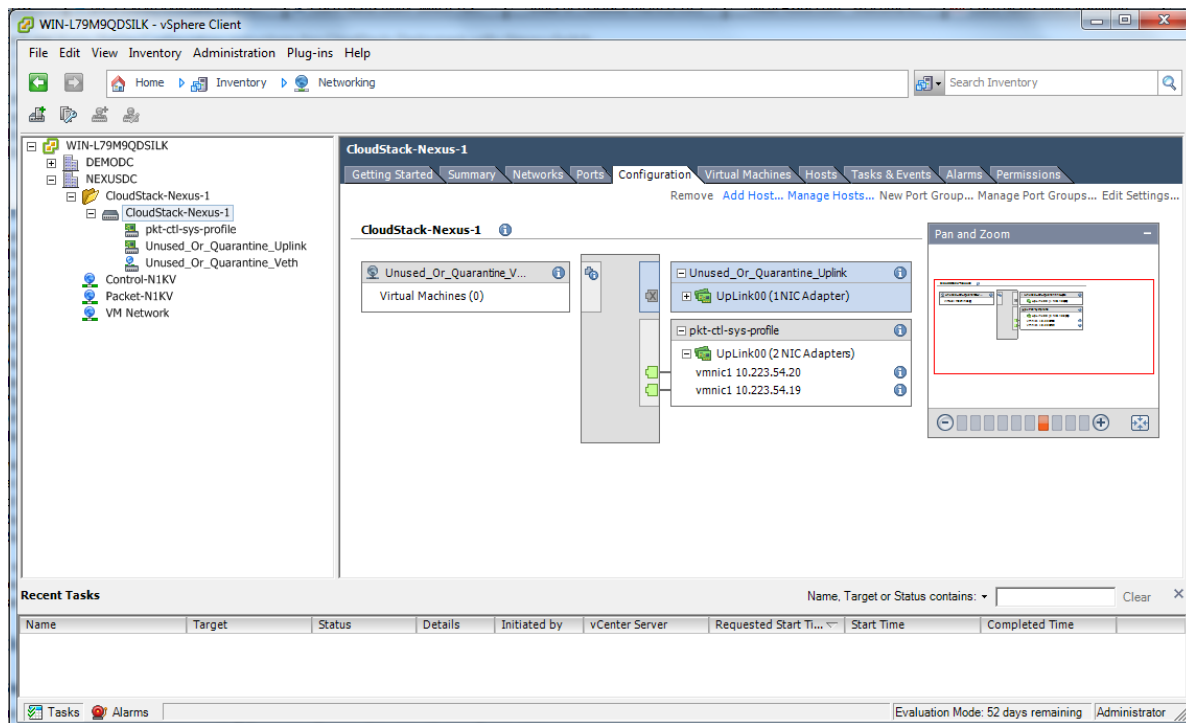
## VSM Configuration Checklist

You will need the following information about network configuration:

VSM Configuration Parameters	Value	Notes
Admin Name and Password		The admin name and password to connect to the VSM appliance. You must specify these credentials while configuring Nexus virtual switch.
Management IP Address		This is the IP address of the VSM appliance. This is the IP address you specify in the virtual switch IP Address field while configuring Nexus virtual switch.
SSL	Enable	Always enable SSL. SSH is usually enabled by default during the VSM installation. However, check whether the SSH connection to the VSM is working, without which CloudPlatform fails to connect to the VSM.

## Creating a Port Profile

- Whether you create a Basic or Advanced zone configuration, ensure that you always create an Ethernet port profile on the VSM after you install it and before you create the zone.
  - The Ethernet port profile created to represent the physical network or networks used by an Advanced zone configuration trunk all the VLANs including guest VLANs, the VLANs that serve the native VLAN, and the packet/control/data/management VLANs of the VSM.
  - The Ethernet port profile created for a Basic zone configuration does not trunk the guest VLANs because the guest VMs do not get their own VLANs provisioned on their network interfaces in a Basic zone.
- An Ethernet port profile configured on the Nexus 1000v virtual switch should not use in its set of system VLANs, or any of the VLANs configured or intended to be configured for use towards VMs or VM resources in the CloudPlatform environment.
- You do not have to create any vEthernet port profiles – CloudPlatform does that during VM deployment.
- Ensure that you create required port profiles to be used by CloudPlatform for different traffic types of CloudPlatform, such as Management traffic, Guest traffic, Storage traffic, and Public traffic. The physical networks configured during zone creation should have a one-to-one relation with the Ethernet port profiles.



For information on creating a port profile, see [Cisco Nexus 1000V Port Profile Configuration Guide](#).

## Assigning Physical NIC Adapters

Assign ESXi host's physical NIC adapters, which correspond to each physical network, to the port profiles. In each ESXi host that is part of the vCenter cluster, observe the physical networks assigned to each port profile and note down the names of the port profile for future use. This mapping information helps you when configuring physical networks during the zone configuration on CloudPlatform. These Ethernet port profile names are later specified as VMware Traffic Labels for different traffic types when configuring physical networks during the zone configuration. For more information on configuring physical networks, see [Configuring a vSphere Cluster with Nexus 1000v Virtual Switch](#) on page 95.

## Adding VLAN Ranges

Determine the public VLAN, System VLAN, and Guest VLANs to be used by the CloudPlatform. Ensure that you add them to the port profile database. Corresponding to each physical network, add the VLAN range to port profiles. In the VSM command prompt, run the `switchport trunk allowed vlan<range>` command to add the VLAN ranges to the port profile.

For example:

```
switchport trunk allowed vlan 1,140-147,196-203
```

In this example, the allowed VLANs added are 1, 140-147, and 196-203.

You must also add all the public and private VLANs or VLAN ranges to the switch. This range is the VLAN range you specify in your zone.

Note: Before you run the `vlan` command, ensure that the configuration mode is enabled in Nexus 1000v virtual switch.

For example:

If you want the VLAN 200 to be used on the switch, run the following command:

```
vlan 200
```

If you want the VLAN range 1350-1750 to be used on the switch, run the following command:

```
vlan 1350-1750
```

Refer to [Cisco Nexus 1000V Command Reference](#) of specific product version.

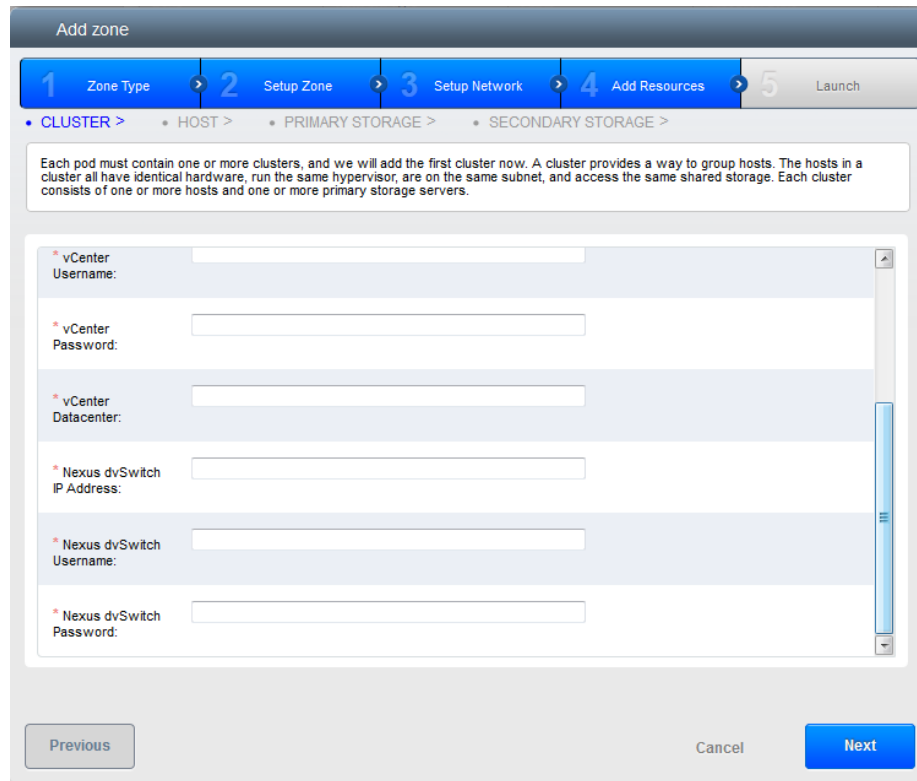
## Enabling Nexus Virtual Switch in CloudPlatform

To make a CloudPlatform deployment Nexus enabled, you must set the `vmware.use.nexus.vswitch` parameter true by using the Global Settings page in the CloudPlatform UI. Unless this parameter is set to "true" and restart the management server, you cannot see any UI options specific to Nexus virtual switch, and CloudPlatform ignores the Nexus virtual switch specific parameters specified in the `AddTrafficTypeCmd`, `UpdateTrafficTypeCmd`, and `AddClusterCmd` API calls.

Unless the CloudPlatform global parameter “`vmware.use.nexus.vswitch`” is set to “true”, CloudPlatform by default uses VMware standard vSwitch for virtual network infrastructure. In this release, CloudPlatform doesn’t support configuring virtual networks in a deployment with a mix of standard vSwitch and Nexus 1000v virtual switch. The deployment can have either standard vSwitch or Nexus 1000v virtual switch.

## Configuring Nexus 1000v Virtual Switch in CloudPlatform

You can configure Nexus dvSwitch by adding the necessary resources while the zone is being created.



Add zone

1 Zone Type 2 Setup Zone 3 Setup Network 4 Add Resources 5 Launch

• CLUSTER > • HOST > • PRIMARY STORAGE > • SECONDARY STORAGE >

Each pod must contain one or more clusters, and we will add the first cluster now. A cluster provides a way to group hosts. The hosts in a cluster all have identical hardware, run the same hypervisor, are on the same subnet, and access the same shared storage. Each cluster consists of one or more hosts and one or more primary storage servers.

\* vCenter Username:

\* vCenter Password:

\* vCenter Datacenter:

\* Nexus dvSwitch IP Address:

\* Nexus dvSwitch Username:

\* Nexus dvSwitch Password:


Previous Cancel Next

After the zone is created, if you want to create an additional cluster along with Nexus 1000v virtual switch in the existing zone, use the Add Cluster option. For information on creating a cluster, see [Add Cluster: vSphere](#) on page 64.

In both these cases, you must specify the following parameters to configure Nexus virtual switch:

Parameters	Description
<b>Cluster Name</b>	Enter the name of the cluster you created in vCenter. For example, "cloud.cluster".
<b>vCenter Host</b>	Enter the host name or the IP address of the vCenter host where you have deployed the Nexus virtual switch.
<b>vCenter User name</b>	Enter the username that CloudPlatform should use to connect to vCenter. This user must have all administrative privileges.
<b>vCenter Password</b>	Enter the password for the user named above.
<b>vCenter Datacenter</b>	Enter the vCenter datacenter that the cluster is in. For example, "cloud.dc.VM".
<b>Nexus dvSwitch IP Address</b>	The IP address of the VSM component of the Nexus 1000v virtual switch.
<b>Nexus dvSwitch Username</b>	The admin name to connect to the VSM appliance.
<b>Nexus dvSwitch Password</b>	The corresponding password for the admin user specified above.

## Removing Nexus Virtual Switch

1. In the vCenter datacenter that is served by the Nexus virtual switch, ensure that you delete all the hosts in the corresponding cluster.
2. Log in with Admin permissions to the CloudPlatform administrator UI.
3. In the left navigation bar, select Infrastructure.
4. In the Infrastructure page, click View all under Clusters.
5. Select the cluster where you want to remove the virtual switch.
6. In the dvSwitch tab, click the name of the virtual switch.
7. In the Details page, click Delete Nexus dvSwitch icon. 

Click Yes in the confirmation dialog box.

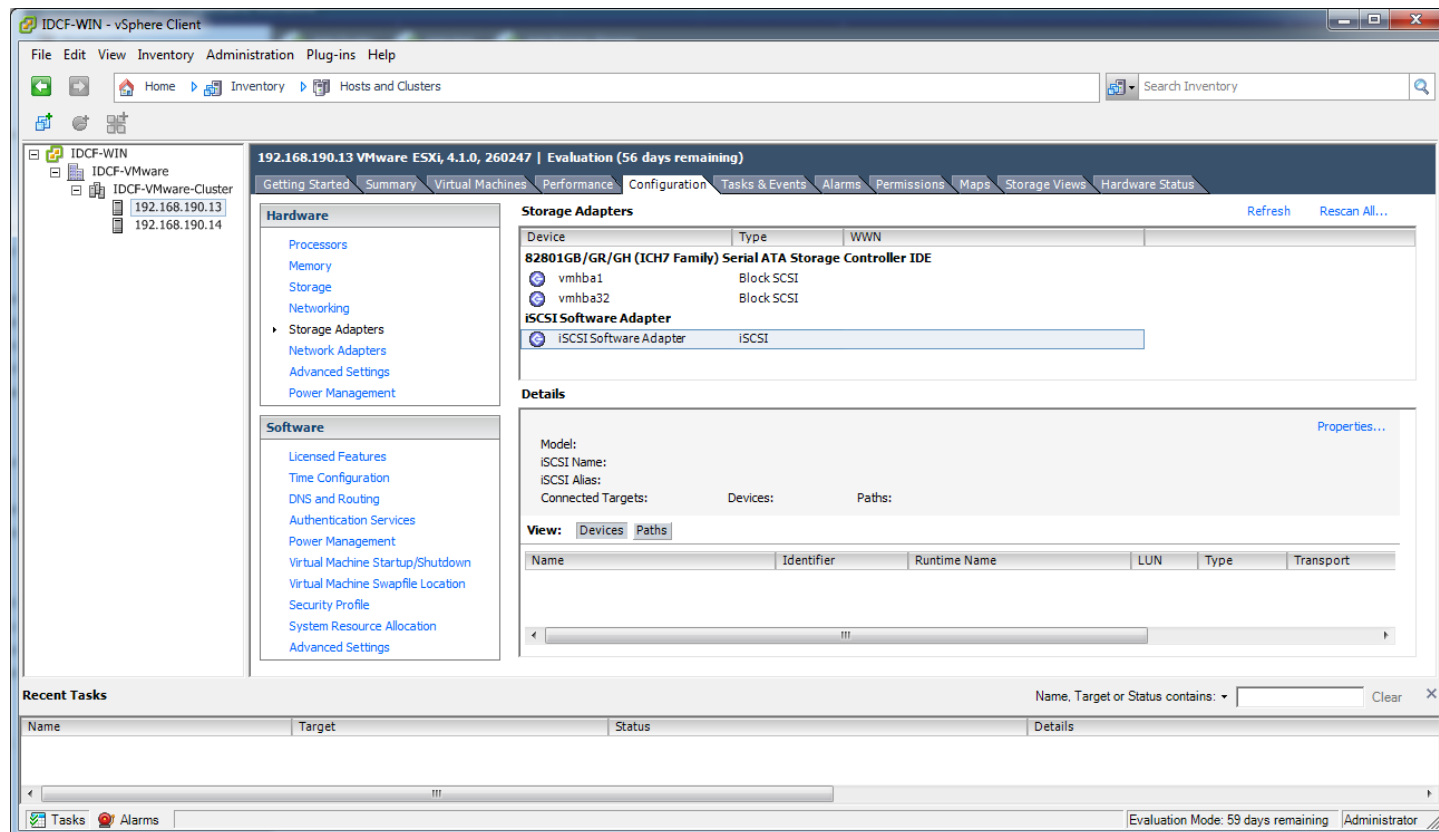
## Storage Preparation for vSphere (iSCSI only)

Use of iSCSI requires preparatory work in vCenter. You must add an iSCSI target and create an iSCSI datastore.

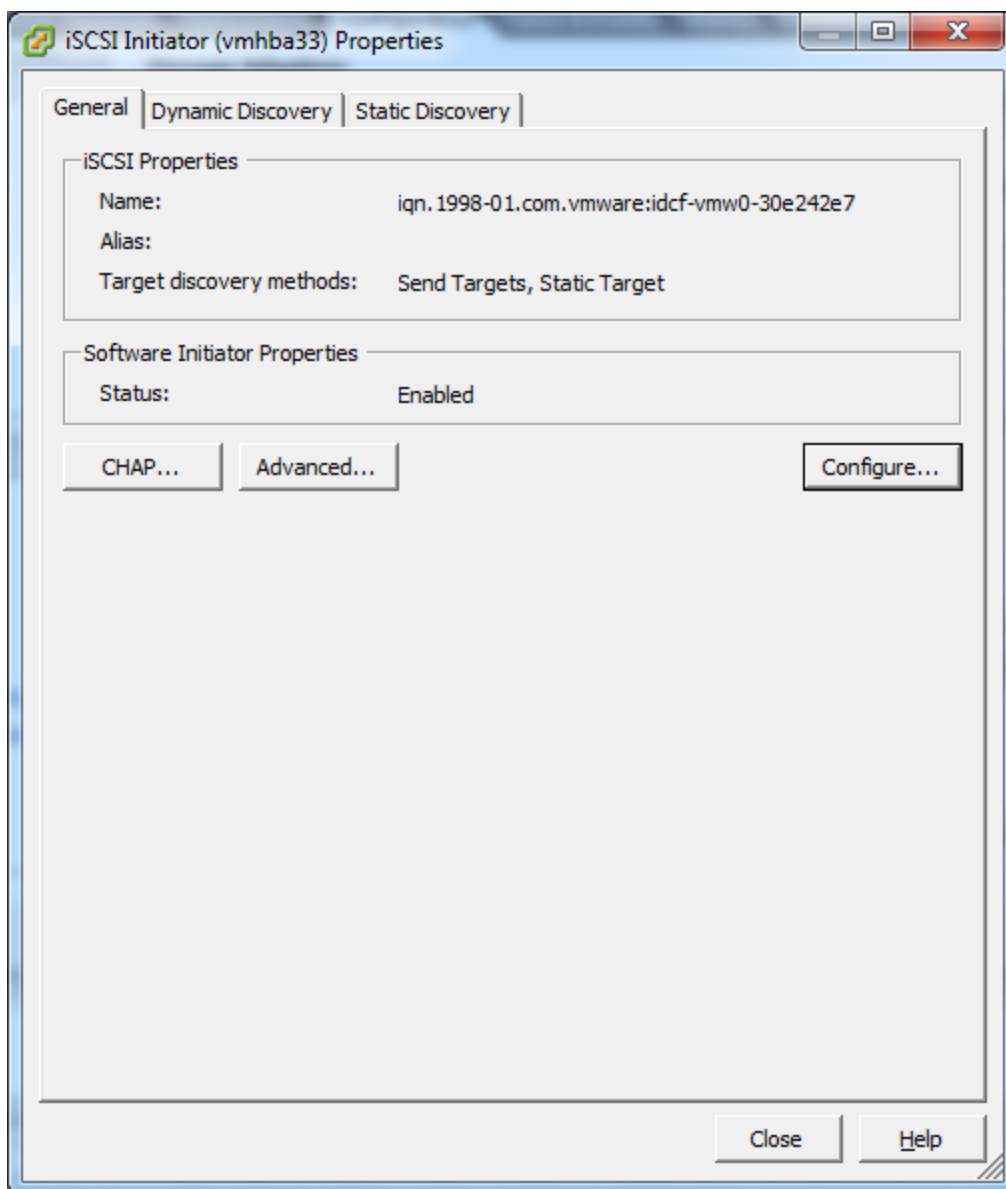
If you are using NFS, skip this section.

### Enable iSCSI initiator for ESXi hosts

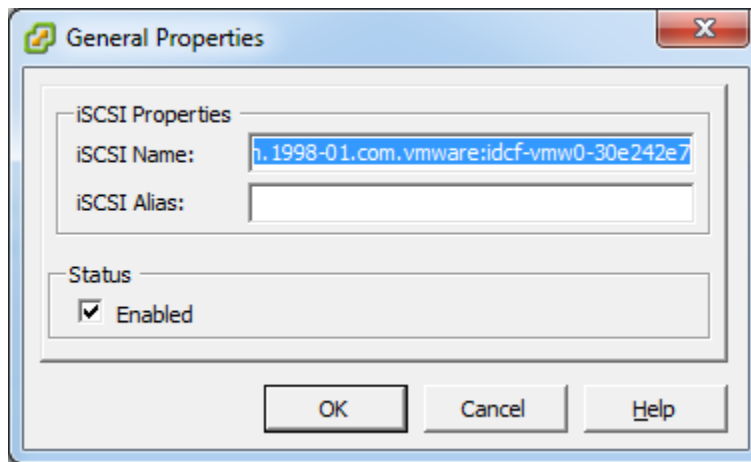
1. In vCenter, go to hosts and Clusters/Configuration, and click Storage Adapters link. You will see:



2. Select iSCSI software adapter and click Properties.



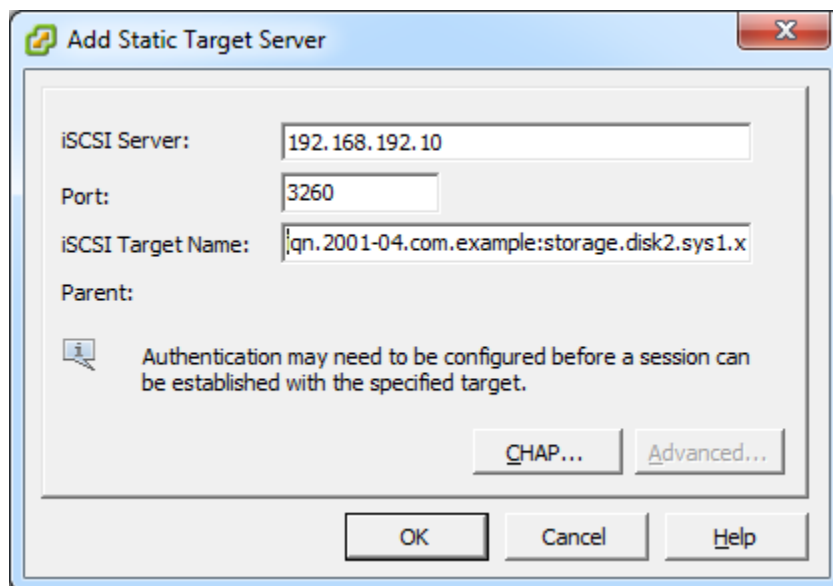
3. Click the Configure... button.



4. Check Enabled to enable the initiator.
5. Click OK to save.

## Add iSCSI target

Under the properties dialog, add the iSCSI target info:



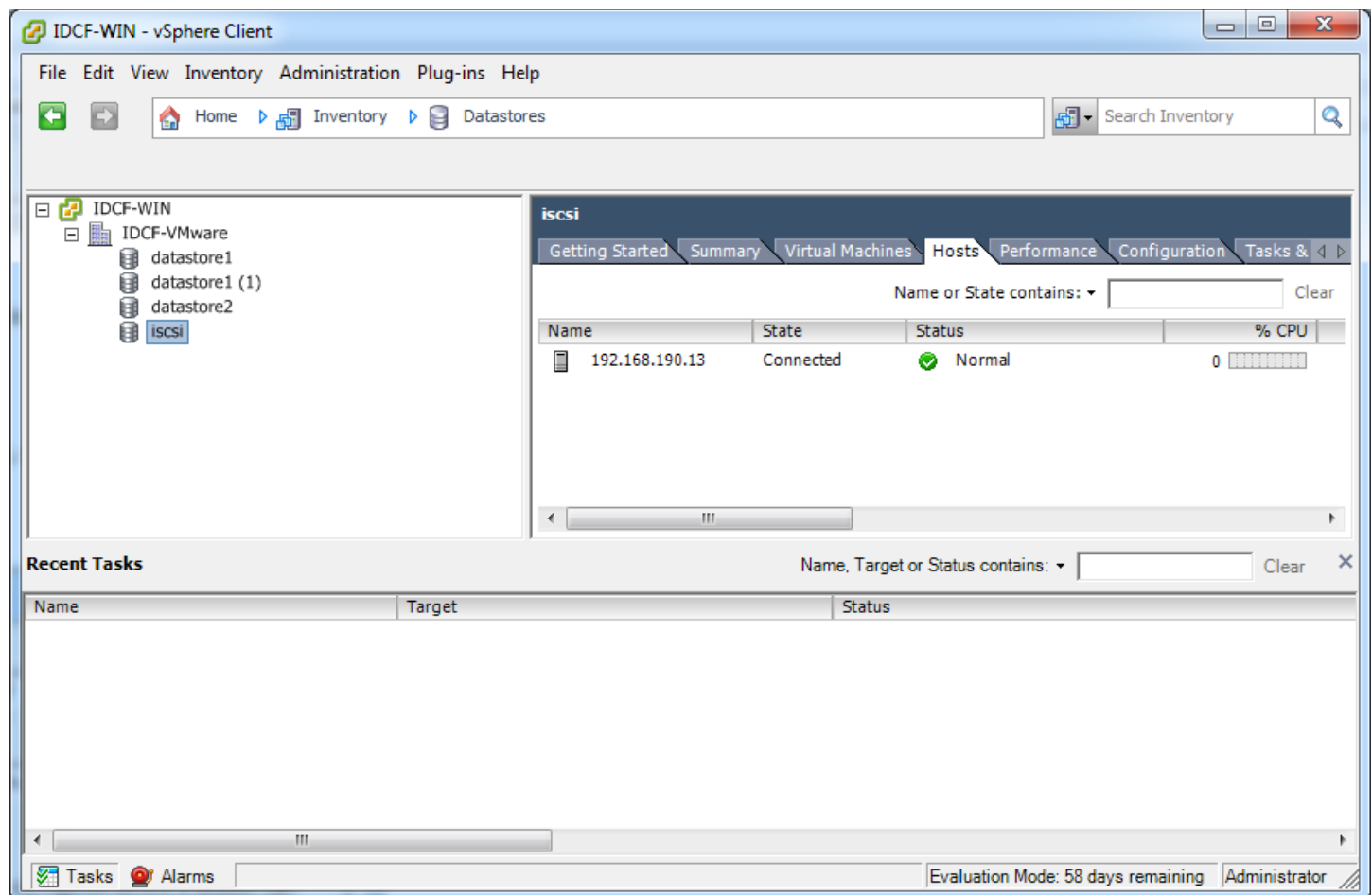
Repeat these steps for all ESXi hosts in the cluster.

## Create an iSCSI datastore

You should now create a VMFS datastore. Follow these steps to do so:

1. Select Home/Inventory/Datastores.
2. Right click on the datacenter node.
3. Choose Add Datastore... command.
4. Follow the wizard to create a iSCSI datastore.

This procedure should be done on one host in the cluster. It is not necessary to do this on all hosts.



## Multipathing for vSphere (Optional)

Storage multipathing on vSphere nodes may be done according to the vSphere installation guide.

## Add Hosts or Configure Clusters (vSphere)

---

Use vCenter to create a vCenter cluster and add your desired hosts to the cluster. You will later add the entire cluster to CloudPlatform. (see Add Cluster: vSphere on page 64).

# KVM Installation and Configuration

---

If you want to use the KVM hypervisor to run guest virtual machines, install KVM on the host(s) in your cloud. The material in this section doesn't duplicate KVM installation documentation, but it does give some CloudPlatform-specific tweaks.

## Supported Operating Systems

---

KVM is included with a variety of Linux-based operating systems. Those supported for use with CloudPlatform can be downloaded from the following websites and installed by following the Installation Guide provided with each operating system. Within a cluster, all KVM hosts must be running the same operating system.

Officially supported OS version for KVM hosts:

- RHEL 6.2: <https://access.redhat.com/downloads>
- It is highly recommended that you purchase a RHEL support license. Citrix support can not be responsible for helping fix issues with the underlying OS.

## System Requirements for KVM Hosts

---

- Must be certified as compatible with the selected operating system. For example, see the RHEL Hardware Compatibility Guide at <https://hardware.redhat.com/>.
- Must support HVM (Intel-VT or AMD-V enabled).
- Within a single cluster, the hosts must be homogenous. The CPUs must be of the same type, count, and feature flags.
- Within a single cluster, the hosts must be of the same kernel version. For example, if one host is RHEL6 64 bit, they must all be RHEL6 64 bit.
- 64-bit x86 CPU (more cores results in better performance)
- Hardware virtualization support required
- 4 GB of memory
- 36 GB of local disk
- At least 1 NIC
- Statically allocated IP Address
- Be sure all the hotfixes provided by the hypervisor vendor are applied. Track the release of hypervisor patches through your hypervisor vendor's support channel, and apply patches as soon as possible after they are released. CloudPlatform will not track or notify you of required hypervisor patches. It is essential that your hosts are completely up to date with the provided hypervisor patches. The hypervisor vendor is likely to refuse to support any system that is not up to date with patches.

**WARNING**

The lack of up-do-date hotfixes can lead to data corruption and lost VMs.

## KVM Installation Steps

1. Download one of the operating systems that includes KVM (see System Requirements for KVM Hosts on page 108) and install it by following the Installation Guide provided with your chosen operating system.
2. After installation, perform the following configuration tasks, which are described in the next few sections:

Required	Optional
Install the CloudPlatform agent on the host (p. 109)	Primary storage setup (p. 111)
Physical network configuration (p. 110)	
Time synchronization (p. 111)	

## Installing the CloudPlatform Agent on a KVM Host

Each KVM host must have the CloudPlatform Agent installed on it. Install the CloudPlatform Agent on each host using the following steps. Some of the steps in the installation procedure apply only to hosts running certain operating systems; these are noted at the beginning of the step.

1. (RHEL 6.2/Fedora) Check for a fully qualified hostname.

```
# hostname --fqdn
```

This should return a fully qualified hostname such as "kvm1.lab.example.org". If it does not edit `/etc/hosts` so that it does.

2. Remove `qemu-kvm`. CloudPlatform provides a patched version.

```
# yum erase qemu-kvm
```

3. (RHEL 6.2) If you do not have a Red Hat Network account, you need to prepare a local Yum repository.
  - a. If you are working with a physical host, insert the RHEL 6.2 installation CD. If you are using a VM, attach the RHEL6 ISO.
  - b. Mount the CDROM to `/media`.
  - c. Create a repo file at `/etc/yum.repos.d/rhel6.repo`. In the file, insert the following lines:

```
[rhel]
name=rhel6
baseurl=file:///media
enabled=1
gpgcheck=0
```

4. Install the CloudPlatform packages. You should have a file in the form of “CloudPlatform-VERSION-N-OSVERSION.tar.gz”.

Untar the file and then run the install.sh script inside it. Replace the file and directory names below with those you are using:

```
# tar xzf CloudStack-VERSION-N-OSVERSION.tar.gz
# cd CloudStack-VERSION-N-OSVERSION
# ./install.sh
```

You should see a few messages as the installer prepares, followed by a list of choices.

5. Choose “A” to install the Agent software.

```
> A
```

6. When the agent installation is finished, log in to the host as root and run the following commands to start essential services (the commands might be different depending on your OS):

```
# service rpcbind start
# service nfs start
# chkconfig nfs on
# chkconfig rpcbind on
```

The CloudPlatform Agent is now installed.

## Physical Network Configuration for KVM

---

You should have a plan for how the hosts will be cabled and which physical NICs will carry what types of traffic. By default, CloudPlatform will use the device that is used for the default route. This device will be placed in a CloudPlatform-created bridge.

If a system has multiple NICs or bonding is desired, the admin may configure the networking on the host. The admin must create a bridge and place the desired device into the bridge. This may be done for each of the public network and the management network. Then edit /etc/cloud/agent/agent.properties and add values for the following:

- public.network.device
- private.network.device

These should be set to the name of the bridge that the user created for the respective traffic type. For example:

- public.network.device=publicbondbr0

This should be done after the install of the software as described previously.

## Time Synchronization

---

The host must be set to use NTP. All hosts in a pod must have the same time.

**1.** Install NTP.

```
# yum install ntp
```

**2.** Edit the NTP configuration file to point to your NTP server.

```
# vi /etc/ntp.conf
```

Add one or more server lines in this file with the names of the NTP servers you want to use. For example:

```
server 0.xenserver.pool.ntp.org
server 1.xenserver.pool.ntp.org
server 2.xenserver.pool.ntp.org
server 3.xenserver.pool.ntp.org
```

**3.** Restart the NTP client.

```
# service ntpd restart
```

**4.** Make sure NTP will start again upon reboot.

```
# chkconfig ntpd on
```

## Primary Storage Setup for KVM (Optional)

---

CloudPlatform allows administrators to set up shared Primary Storage that uses iSCSI or fiber channel. With KVM, the storage is mounted on each host. This is called "SharedMountPoint" storage and is an alternative to NFS. The storage is based on some clustered file system technology, such as OCFS2. Note that the use of the Cluster Logical Volume Manager (CLVM) is not officially supported with CloudPlatform 3.0.x.

With SharedMountPoint storage:

- Each node in the KVM cluster mounts the storage in the same local location (e.g., /mnt/primary)
- A shared clustered file system is used
- The administrator manages the mounting and unmounting of the storage
- If you want to use SharedMountPoint storage you should set it up on the KVM hosts now. Note the mountpoint that you have used on each host; you will use that later to configure CloudPlatform.

# Oracle VM (OVM) Installation and Configuration

---

If you want to use the Oracle VM Server (OVM) hypervisor to run guest virtual machines, install OVM on the host(s) in your cloud.

## System Requirements for OVM Hosts

---

CloudPlatform works with the following version:

- OVM Server 2.2

The OVM hosts must follow these restrictions:

- All hosts must be 64-bit and must support HVM (Intel-VT or AMD-V enabled). All Hosts within a Cluster must be homogenous. That means the CPUs must be of the same type, count, and feature flags.
- Within a single cluster, the hosts must be of the same kernel version. For example, if one Host is OVM 2.2 64 bit, they must all be OVM 2.2 64 bit.
- Be sure all the hotfixes provided by the hypervisor vendor are applied. Track the release of hypervisor patches through your hypervisor vendor's support channel, and apply patches as soon as possible after they are released. CloudPlatform will not track or notify you of required hypervisor patches. It is essential that your hosts are completely up to date with the provided hypervisor patches. The hypervisor vendor is likely to refuse to support any system that is not up to date with patches.

### WARNING

The lack of up-to-date hotfixes can lead to data corruption and lost VMs.

## OVM Installation Overview

---

Certain essential CloudPlatform software components can not run on OVM, so your OVM Zone will need to include at least two clusters: one cluster containing the OVM hosts, and another cluster with a different hypervisor (KVM, XenServer, or VMWare), where the CloudPlatform system VMs will run.

## Installing OVM on the Host(s)

---

1. Download the OVM template from the Oracle website (<http://www.oracle.com/virtualization>) and install it using the OVM Installation Guide. The software download should be a .zip file that contains two files, an image (.img) file and vm.cfg. You need only the .img file. The default template password is ovsroot.
2. Unzip the file and copy the .img file to your HTTP server.

3. Follow the instructions in the OVM Installation Guide to install OVM on each host. During installation, you will be prompted to set an agent password and a root password. You can specify any desired text or accept the default.

Make a note of these passwords – you will need them later.

4. Repeat for any additional hosts that will be part of the OVM cluster.

**NOTE:** After ISO installation, the installer reboots into the operating system. Due to a known issue in OVM Server, the reboot will place the VM in the Stopped state. In the CloudPlatform UI, detach the ISO from the VM (so that the VM will not boot from the ISO again), then click the Start button to restart the VM.

## Primary Storage Setup for OVM

---

CloudPlatform natively supports NFS, iSCSI and local storage. Each iSCSI LUN can be assigned to exactly one OVM cluster as the cluster's primary storage device. Following is a summary of the steps that you need to do. For details, see Oracle documentation on preparing storage repositories at

[http://download.oracle.com/docs/cd/E15458\\_01/doc.22/e15444/storage.htm#sthref65](http://download.oracle.com/docs/cd/E15458_01/doc.22/e15444/storage.htm#sthref65).

1. Map your iSCSI device to the OVM host's local device. The exact steps to use depend on your system's peculiarities.
2. On every host in the cluster, create the same softlink name so CloudPlatform can use a consistent path to refer to the iSCSI LUN from any host. For example, if the softlink name is `/dev/ovm-iscsi0`:

```
ln -s /dev/disk/by-path/<output of previous command> /dev/ovm-iscsi0
```

Make a note of your softlink name. You will need it later.

3. Exactly once on any ONE host in the OVM cluster, format the OCFS2 file system on the iSCSI device.

## Set Up Host(s) for System VMs

---

Before proceeding to install the CloudPlatform Management Server, you need to install a non-OVM hypervisor on at least one host that will run the CloudPlatform System VMs (which are not supported by OVM).

1. Install the non-OVM hypervisor on at least one host by following one of the instructions below, depending on which hypervisor you want to use:
  - Citrix XenServer Installation for CloudPlatform on page 76
  - VMware vSphere Installation and Configuration on page 84
  - KVM Installation and Configuration on page 108
2. When you set up the pod that will contain the OVM cluster, remember to include this non-OVM host in its own cluster along with the OVM cluster in the same pod.

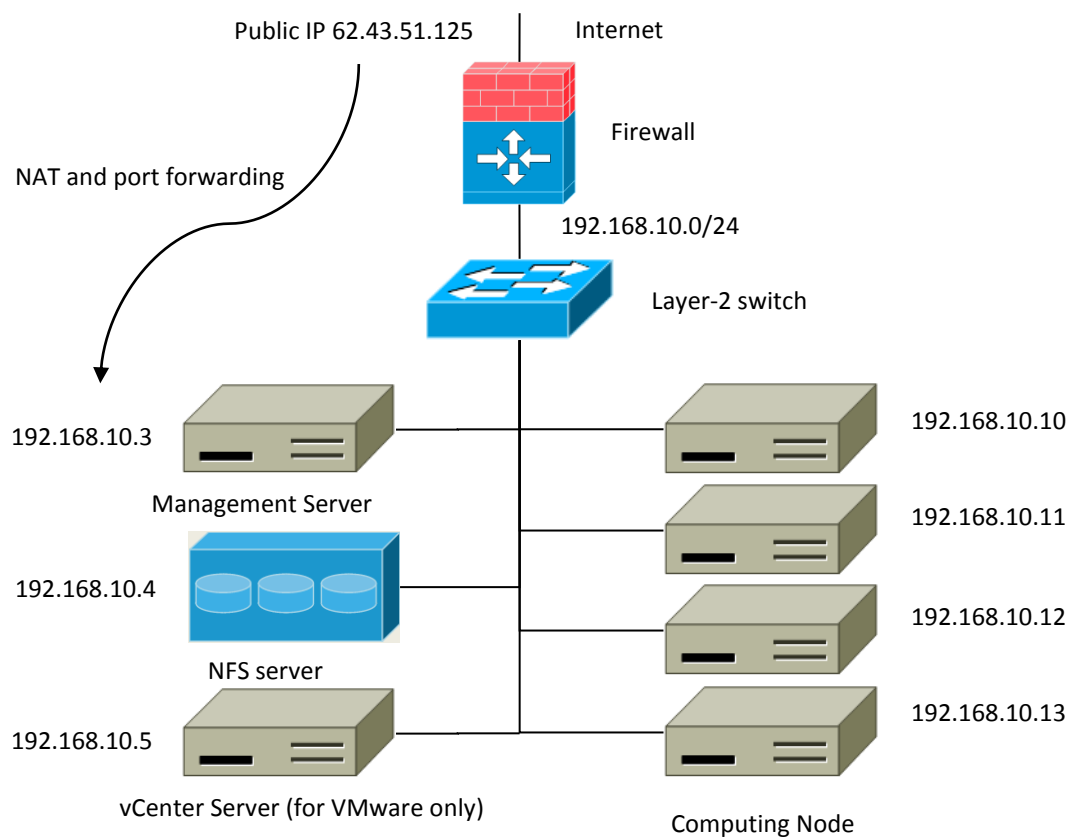
# Choosing a Deployment Architecture

The architecture used in a deployment will vary depending on the size and purpose of the deployment. This section contains examples of deployment architecture, including a small-scale deployment useful for test and trial deployments and a fully-redundant large-scale setup for production deployments.

## Who Should Read This

If you need help figuring out how many nodes to include, how they fit together, how to scale your deployment, or how the various parts of CloudPlatform work together in different scenarios, this section is for you.

## Small-Scale Deployment



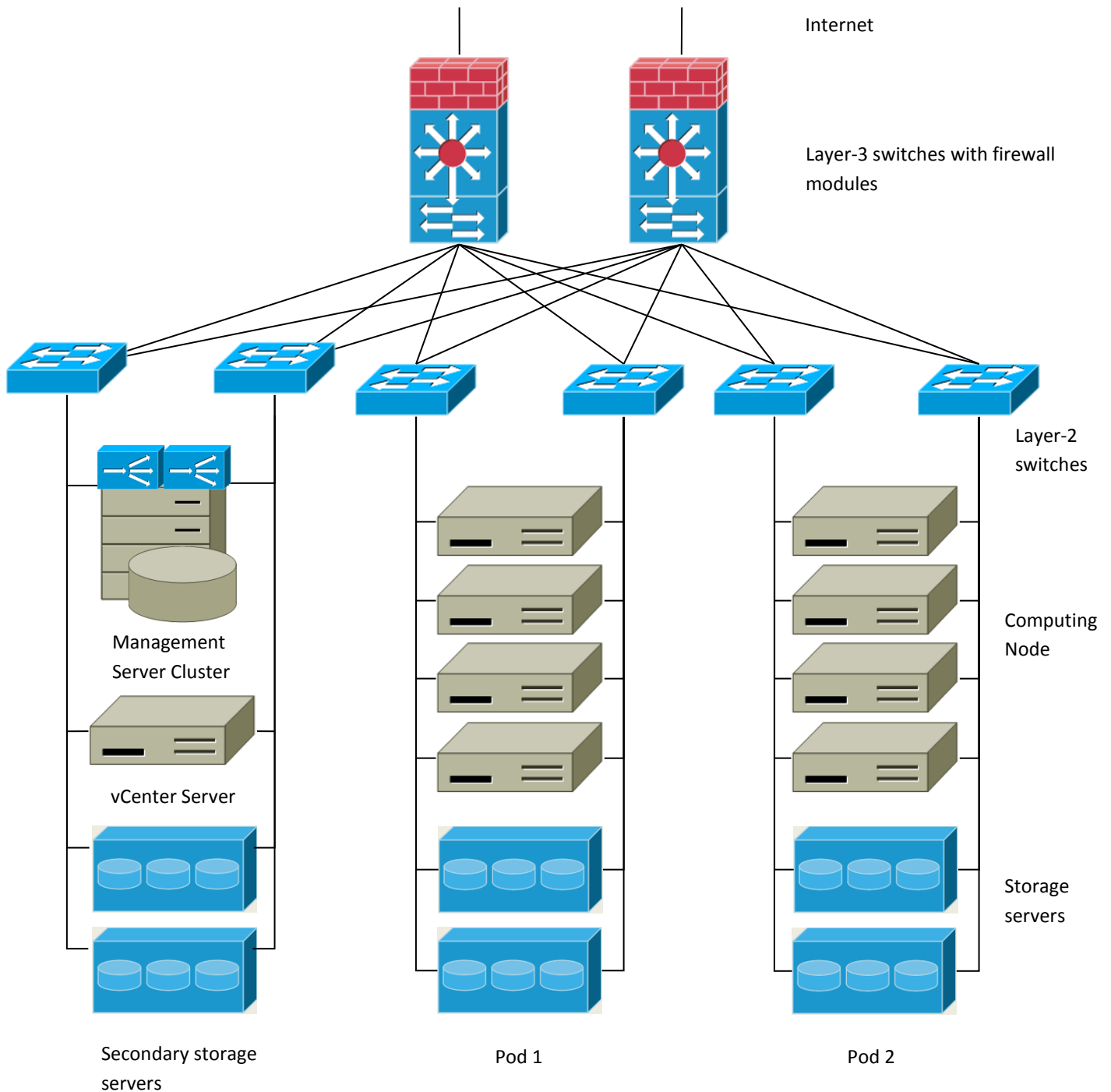
**Small-Scale Deployment**

This diagram illustrates the network architecture of a small-scale CloudPlatform deployment.

- A firewall provides a connection to the Internet. The firewall is configured in NAT mode. The firewall forwards HTTP requests and API calls from the Internet to the Management Server. The Management Server resides on the management network.

- A layer-2 switch connects all physical servers and storage.
- A single NFS server functions as both the primary and secondary storage.
- The Management Server is connected to the management network.

## Large-Scale Redundant Setup



This diagram illustrates the network architecture of a large-scale CloudPlatform deployment.

- A layer-3 switching layer is at the core of the data center. A router redundancy protocol like VRRP should be deployed. Typically high-end core switches also include firewall modules. Separate firewall appliances may also be used if the layer-3 switch does not have integrated firewall capabilities. The firewalls are configured in NAT mode. The firewalls provide the following functions:
  - Forwards HTTP requests and API calls from the Internet to the Management Server. The Management Server resides on the management network.
  - When the cloud spans multiple zones, the firewalls should enable site-to-site VPN such that servers in different zones can directly reach each other.
- A layer-2 access switch layer is established for each pod. Multiple switches can be stacked to increase port count. In either case, redundant pairs of layer-2 switches should be deployed.
- The Management Server cluster (including front-end load balancers, Management Server nodes, and the MySQL database) is connected to the management network through a pair of load balancers.
- Secondary storage servers are connected to the management network.
- Each pod contains storage and computing servers. Each storage and computing server should have redundant NICs connected to separate layer-2 access switches.

## Separate Storage Network

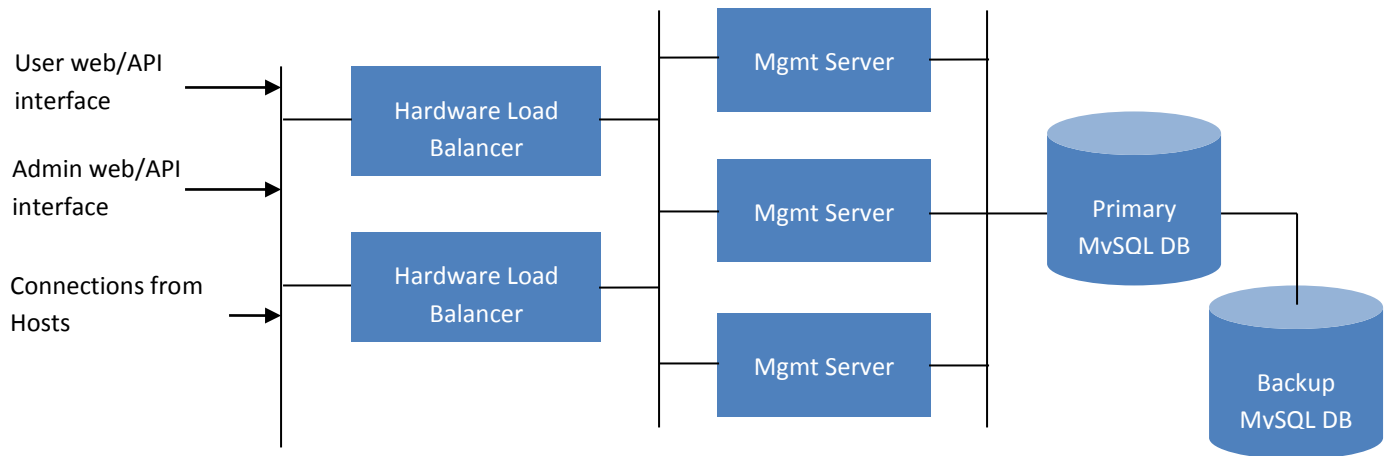
---

In the Large-Scale Redundant setup described in the previous section, storage traffic can overload the management network. A separate storage network is optional for deployments. Storage protocols such as iSCSI are sensitive to network delays. A separate storage network ensures guest network traffic contention does not impact storage performance.

## Multi-Node Management Server

---

The CloudPlatform Management Server is deployed on one or more front-end servers connected to a single MySQL database. Optionally a pair of hardware load balancers distributes requests from the web. A backup management server set may be deployed using MySQL replication at a remote site to add DR capabilities.



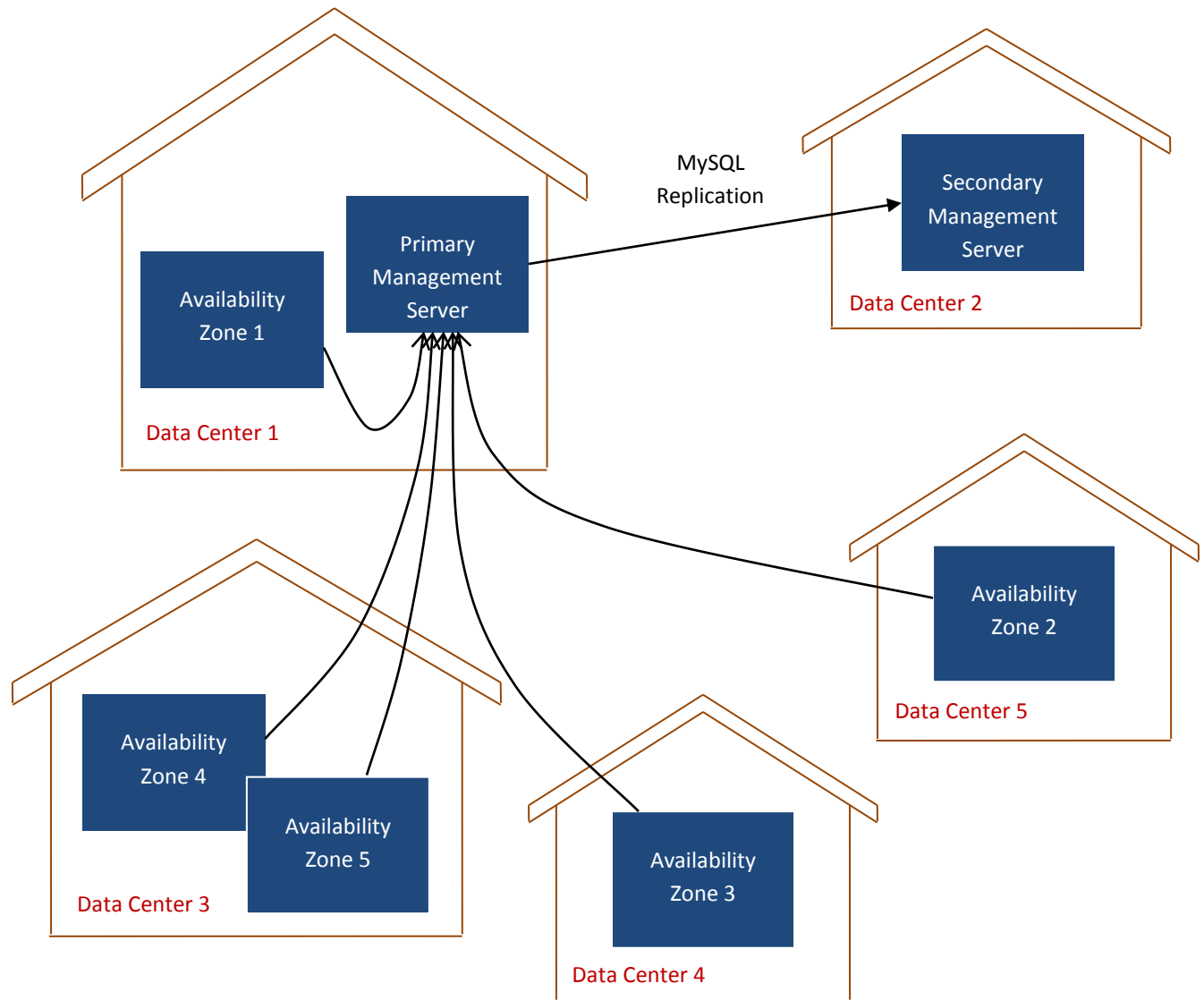
The administrator must decide the following.

- Whether or not load balancers will be used
- How many Management Servers will be deployed
- Whether MySQL replication will be deployed to enable disaster recovery.

## Multi-Site Deployment

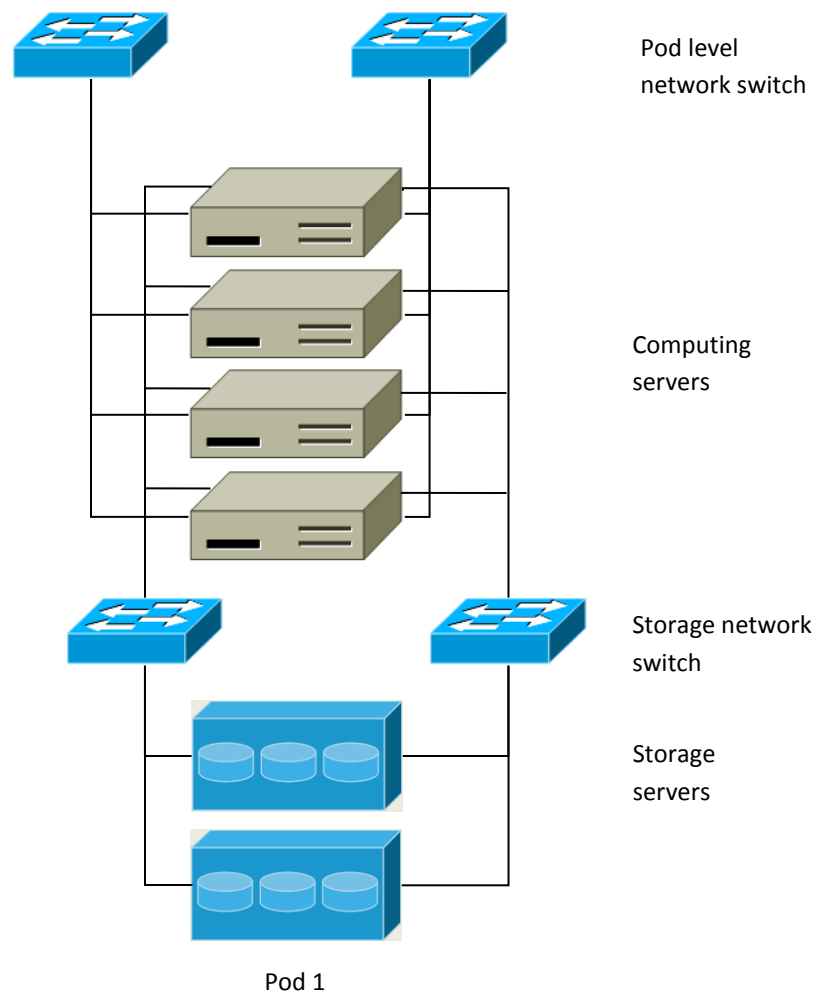
---

The CloudPlatform platform scales well into multiple sites through the use of zones. The following diagram shows an example of a multi-site deployment.



#### Example of a Multi-Site Deployment

Data Center 1 houses the primary Management Server as well as zone 1. The MySQL database is replicated in real time to the secondary Management Server installation in Data Center 2.

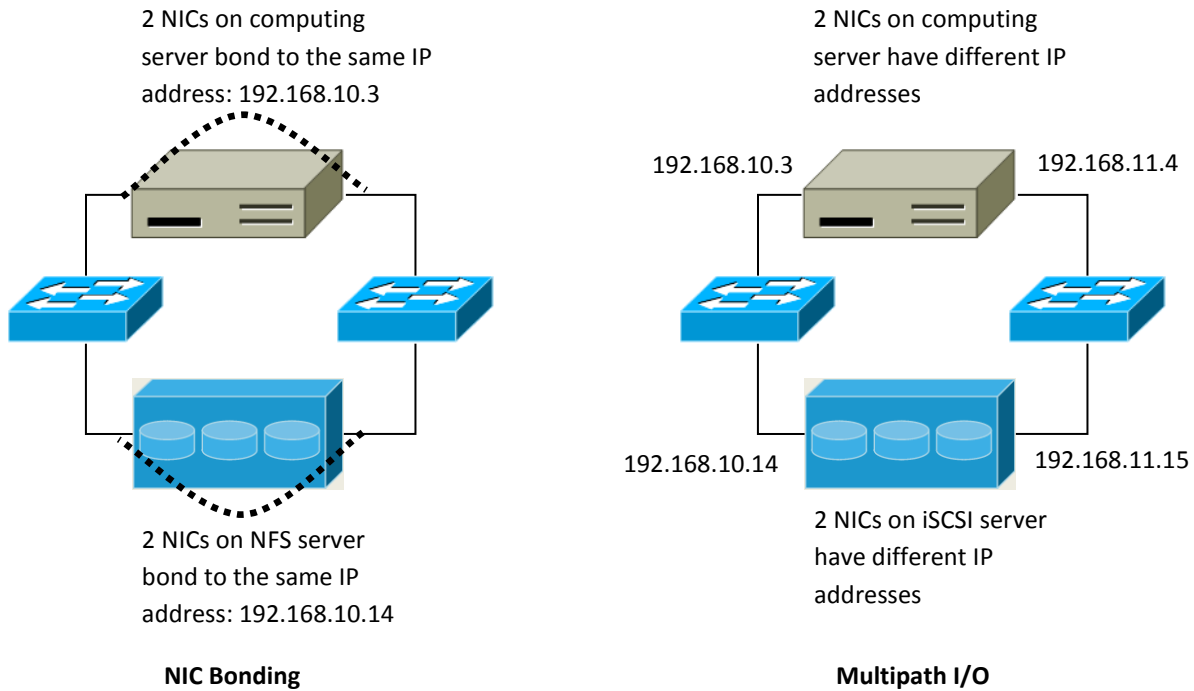


#### Separate Storage Network

This diagram illustrates a setup with a separate storage network. Each server has four NICs, two connected to pod-level network switches and two connected to storage network switches.

There are two ways to configure the storage network:

- Bonded NIC and redundant switches can be deployed for NFS. In NFS deployments, redundant switches and bonded NICs still result in one network (one CIDR block+ default gateway address).
- iSCSI can take advantage of two separate storage networks (two CIDR blocks each with its own default gateway). Multipath iSCSI client can failover and load balance between separate storage networks.



**NIC Bonding and Multipath I/O**

This diagram illustrates the differences between NIC bonding and Multipath I/O (MPIO). NIC bonding configuration involves only one network. MPIO involves two separate networks.

## Choosing a Hypervisor: Supported Features

---

CloudPlatform supports many popular hypervisors. Your cloud can consist entirely of hosts running a single hypervisor, or you can use multiple hypervisors. Each cluster of hosts must run the same hypervisor.

You might already have an installed base of nodes running a particular hypervisor, in which case, your choice of hypervisor has already been made. If you are starting from scratch, you need to decide what hypervisor software best suits your needs. A discussion of the relative advantages of each hypervisor is outside the scope of our documentation. However, it will help you to know which features of each hypervisor are supported by CloudPlatform. The following table provides this information.

Feature	XenServer 6.0.2	vSphere 4.1/5.0	KVM – RHEL 6.2	OVM 2.2
Network throttling	Yes	Yes	No	No
Security groups in zones that use basic networking	Yes	No	Yes	No
iSCSI	Yes	Yes	Yes	Yes
FibreChannel	Yes	Yes	Yes	No
Local disk	Yes	Yes	Yes	No
HA	Yes	Yes (Native)	Yes	Yes
Snapshots of local disk	Yes	Yes	Yes	No
Local disk as data disk	No	No	No	No
Work load balancing	No	DRS	No	No
Manual live migration of VMs from host to host	Yes	Yes	Yes	Yes
Conserve management traffic IP addresses by using link local network to communicate with virtual router	Yes	No	Yes	Yes

# Network Setup

Achieving the correct networking setup is crucial to a successful CloudPlatform installation. This section contains information to help you make decisions and follow the right procedures to get your network set up correctly.

## Basic and Advanced Networking

CloudPlatform provides two styles of networking:

- **Basic.** For AWS-style networking. Provides a single network where guest isolation can be provided through layer-3 means such as security groups (IP address source filtering).
- **Advanced.** For more sophisticated network topologies. This network model provides the most flexibility in defining guest networks, but requires more configuration steps than basic networking.

Each zone has either basic or advanced networking. Once the choice of networking model for a zone has been made and configured in CloudPlatform, it can not be changed. A zone is either basic or advanced for its entire lifetime.

The following table compares the networking features in the two networking models.

Networking Feature	Basic Network	Advanced Network
Number of networks	Single network	Multiple networks
Firewall type	Physical	Physical & virtual
Load balancer	Physical	Physical & virtual
Isolation type	Layer 3	Layer 2 & Layer 3
VPN support	No	Yes
Port forwarding	Physical	Physical & virtual
1:1 NAT	Physical	Physical & virtual
Source NAT	No	Physical & virtual
Userdata	Yes	Yes

Network usage monitoring	sFlow / netFlow at physical router	Hypervisor & virtual router
DHCP and DNS	Yes	Yes

The two types of networking may be in use in the same cloud. However, a given zone must use either Basic Networking or Advanced Networking.

Different types of network traffic can be segmented on the same physical network. Guest traffic can also be segmented by account. To isolate traffic, you can use separate VLANs. If you are using separate VLANs on a single physical network, make sure the VLAN tags are in separate numerical ranges.

## VLAN Allocation Example

VLANs are required for public and guest traffic. The following is an example of a VLAN allocation scheme:

VLAN IDs	Traffic type	Scope
< 500	Management traffic. Reserved for administrative purposes	CloudPlatform software can access this, hypervisors, system VMs.
500-599	VLAN carrying public traffic.	CloudPlatform accounts.
600-799	VLANs carrying guest traffic:	CloudPlatform accounts. Account-specific VLAN is chosen from this pool.
800-899	VLANs carrying guest traffic	CloudPlatform accounts. Account-specific VLAN chosen by CloudPlatform admin to assign to that account.
900-999	VLAN carrying guest traffic	CloudPlatform accounts. Can be scoped by project, domain, or all accounts.
> 1000	Reserved for future use	

## Example Hardware Configuration

---

This section contains an example configuration of specific switch models for zone-level layer-3 switching. It assumes VLAN management protocols, such as VTP or GVRP, have been disabled. The example scripts must be changed appropriately if you choose to use VTP or GVRP.

### Dell 62xx

The following steps show how a Dell 62xx is configured for zone-level layer-3 switching. These steps assume VLAN 201 is used to route untagged private IPs for pod 1, and pod 1's layer-2 switch is connected to Ethernet port 1/g1.

The Dell 62xx Series switch supports up to 1024 VLANs.

1. Configure all the VLANs in the database.

```
vlan database
vlan 200-999
exit
```

2. Configure Ethernet port 1/g1.

```
interface ethernet 1/g1
switchport mode general
switchport general pvid 201
switchport general allowed vlan add 201 untagged
switchport general allowed vlan add 300-999 tagged
exit
```

The statements configure Ethernet port 1/g1 as follows:

- VLAN 201 is the native untagged VLAN for port 1/g1.
- All VLANs (300-999) are passed to all the pod-level layer-2 switches.

### Cisco 3750

The following steps show how a Cisco 3750 is configured for zone-level layer-3 switching. These steps assume VLAN 201 is used to route untagged private IPs for pod 1, and pod 1's layer-2 switch is connected to GigabitEthernet1/0/1.

1. Setting VTP mode to transparent allows us to utilize VLAN IDs above 1000. Since we only use VLANs up to 999, vtp transparent mode is not strictly required.

```
vtp mode transparent
vlan 200-999
exit
```

## 2. Configure GigabitEthernet1/0/1.

```
interface GigabitEthernet1/0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 201
exit
```

The statements configure GigabitEthernet1/0/1 as follows:

- VLAN 201 is the native untagged VLAN for port GigabitEthernet1/0/1.
- Cisco passes all VLANs by default. As a result, all VLANs (300-999) are passed to all the pod-level layer-2 switches.

## Layer-2 Switch

---

The layer-2 switch is the access switching layer inside the pod.

- It should trunk all VLANs into every computing host.
- It should switch traffic for the management network containing computing and storage hosts. The layer-3 switch will serve as the gateway for the management network.

### Example Configurations

This section contains example configurations for specific switch models for pod-level layer-2 switching. It assumes VLAN management protocols such as VTP or GVRP have been disabled. The scripts must be changed appropriately if you choose to use VTP or GVRP.

#### Dell 62xx

The following steps show how a Dell 62xx is configured for pod-level layer-2 switching.

### 1. Configure all the VLANs in the database.

```
vlan database
vlan 300-999
exit
```

### 2. VLAN 201 is used to route untagged private IP addresses for pod 1, and pod 1 is connected to this layer-2 switch.

```
interface range ethernet all
switchport mode general
switchport general allowed vlan add 300-999 tagged
exit
```

- The statements configure all Ethernet ports to function as follows:
- All ports are configured the same way.
- All VLANs (300-999) are passed through all the ports of the layer-2 switch.

## Cisco 3750

The following steps show how a Cisco 3750 is configured for pod-level layer-2 switching.

1. Setting VTP mode to transparent allows us to utilize VLAN IDs above 1000. Since we only use VLANs up to 999, vtp transparent mode is not strictly required.

```
vtp mode transparent
vlan 300-999
exit
```

2. Configure all ports to dot1q and set 201 as the native VLAN.

```
interface range GigabitEthernet 1/0/1-24
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 201
exit
```

By default, Cisco passes all VLANs. Cisco switches complain if the native VLAN IDs are different when 2 ports are connected together. That's why we specify VLAN 201 as the native VLAN on the layer-2 switch.

## Hardware Firewall

---

All deployments should have a firewall protecting the management server; see [Generic Firewall Provisions](#). Optionally, some deployments may also have a Juniper SRX firewall that will be the default gateway for the guest networks; see [External Guest Firewall Integration for Juniper SRX \(Optional\)](#).

### Generic Firewall Provisions

The hardware firewall is required to serve two purposes:

- Protect the Management Servers. NAT and port forwarding should be configured to direct traffic from the public Internet to the Management Servers.
- Route management network traffic between multiple zones. Site-to-site VPN should be configured between multiple zones.

To achieve the above purposes you must set up fixed configurations for the firewall. Firewall rules and policies need not change as users are provisioned into the cloud. Any brand of hardware firewall that supports NAT and site-to-site VPN can be used.

### External Guest Firewall Integration for Juniper SRX (Optional)

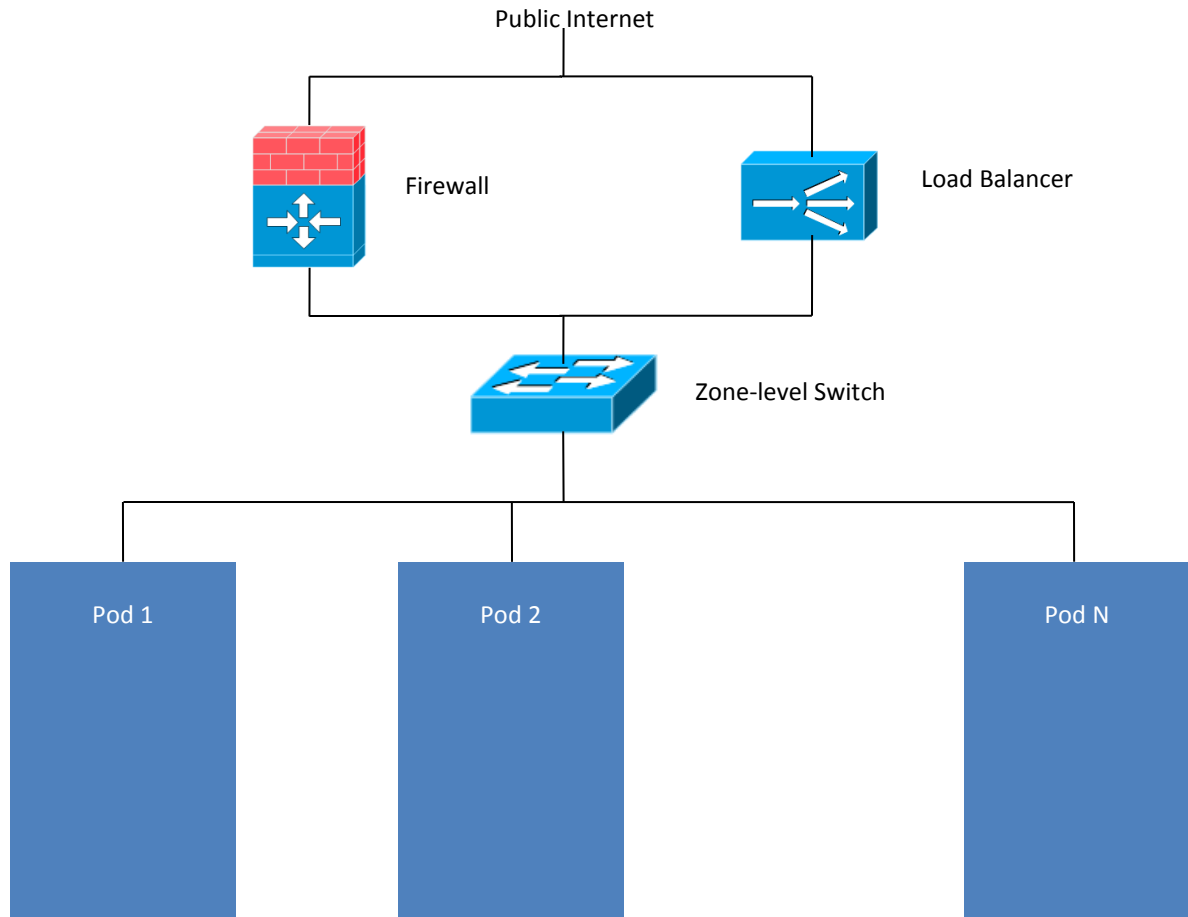
#### Available only for guests using advanced networking

CloudPlatform provides for direct management of the Juniper SRX series of firewalls. This enables CloudPlatform to establish static NAT mappings from public IPs to guest VMs, and to use the Juniper device in place of the virtual router for

firewall services. You can have one or more Juniper SRX per zone. This feature is optional. If Juniper integration is not provisioned, CloudPlatform will use the virtual router for these services.

The Juniper SRX can optionally be used in conjunction with an external load balancer.

External Network elements can be deployed in a side-by-side configuration.



CloudPlatform requires the Juniper to be configured as follows.

1. Install your SRX appliance according to the vendor's instructions.
2. Connect one interface to the management network and one interface to the public network. Alternatively, you can connect the same interface to both networks and use a VLAN for the public network.
3. Make sure "vlan-tagging" is enabled on the private interface.
4. Record the public and private interface names. If you used a VLAN for the public interface, add a ".[VLAN TAG]" after the interface name. For example, if you are using ge-0/0/3 for your public interface and VLAN tag 301, your

The SRX software must be version 10.3 or higher.

public interface name would be "ge-0/0/3.301". Your private interface name should always be untagged because the CloudPlatform software automatically creates tagged logical interfaces.

5. Create a public security zone and a private security zone. By default, these will already exist and will be called "untrust" and "trust". Add the public interface to the public zone and the private interface to the private zone. Note down the security zone names.
6. Make sure there is a security policy from the private zone to the public zone that allows all traffic.
7. Note the username and password of the account you want the CloudPlatform software to log in to when it is programming rules.
8. Make sure the "ssh" and "xnm-clear-text" system services are enabled.
9. If traffic metering is desired:
  - a. Create an incoming firewall filter and an outgoing firewall filter. These filters should be the same names as your public security zone name and private security zone name respectively. The filters should be set to be "interface-specific". For example, here is the configuration where the public zone is "untrust" and the private zone is "trust":

```
root@cloud-srx# show firewall
filter trust {
    interface-specific;
}

filter untrust {
    interface-specific;
}
```

- b. Add the firewall filters to your public interface. For example, a sample configuration output (for public interface ge-0/0/3.0, public security zone untrust, and private security zone trust) is:

```
ge-0/0/3 {
    unit 0 {
        family inet {
            filter {
                input untrust;
                output trust;
            }
            address 172.25.0.252/16;
        }
    }
}
```

10. Make sure all VLANs are brought to the private interface of the SRX.
11. After the CloudPlatform Management Server is installed, log in to the CloudPlatform UI as administrator.
12. In the left navigation bar, click Infrastructure.
13. In Zones, click View More.
14. Choose the zone you want to work with.
15. Click the Network tab.
16. In the Network Service Providers node of the diagram, click Configure. (You might have to scroll down to see this.)

17. Click SRX.

18. Click the Add New SRX button (+) and provide the following:

- **IP Address.** The IP address of the SRX.
- **Username.** The user name of the account on the SRX that CloudPlatform should use.
- **Password.** The password of the account.
- **Public Interface.** The name of the public interface on the SRX. For example, ge-0/0/2. A ".x" at the end of the interface indicates the VLAN that is in use.
- **Private Interface.** The name of the private interface on the SRX. For example, ge-0/0/1.
- **Usage Interface.** (Optional) Typically, the public interface is used to meter traffic. If you want to use a different interface, specify its name here.
- **Number of Retries.** The number of times to attempt a command on the SRX before failing. The default value is 2.
- **Timeout (seconds).** The time to wait for a command on the SRX before considering it failed. Default is 300 seconds.
- **Public Network.** The name of the public network on the SRX. For example, trust.
- **Private Network.** The name of the private network on the SRX. For example, untrust.
- **Capacity.** The number of networks the device can handle.
- **Dedicated.** When marked as dedicated, this device will be dedicated to a single account. When Dedicated is checked, the value in the Capacity field has no significance – implicitly, its value is 1.

19. Click OK.

20. Click Global Settings. Set the parameter `external.network.stats.interval` to indicate how often you want CloudPlatform to fetch network usage statistics from the Juniper SRX. If you are not using the SRX to gather network usage statistics, set to 0.

## Management Server Load Balancing

---

CloudPlatform can use a load balancer to provide a virtual IP for multiple Management Servers. The administrator is responsible for creating the load balancer rules for the Management Servers. The application requires persistence or stickiness across multiple sessions. The following chart lists the ports that should be load balanced and whether or not persistence is required.

Even if persistence is not required, enabling it is permitted.

Source Port	Destination Port	Protocol	Persistence Required?
80 or 443	8080 (or 20400 with AJP)	HTTP (or AJP)	Yes
8250	8250	TCP	Yes
8096	8096	HTTP	No

## Topology Requirements

---

### Security Requirements

The public Internet must not be able to access port 8096 or port 8250 on the Management Server.

### Runtime Internal Communications Requirements

- The Management Servers communicate with each other to coordinate tasks. This communication uses TCP on ports 8250 and 9090.
- The console proxy VMs connect to all hosts in the zone over the management traffic network. Therefore the management traffic network of any given pod in the zone must have connectivity to the management traffic network of all other pods in the zone.
- The secondary storage VMs and console proxy VMs connect to the Management Server on port 8250. If you are using multiple Management Servers, the load balanced IP address of the Management Servers on port 8250 must be reachable.

### Storage Network Topology Requirements

The secondary storage NFS export is mounted by the secondary storage VM. Secondary storage traffic goes over the management traffic network, even if there is a separate storage network. Primary storage traffic goes over the storage network, if available. If you choose to place secondary storage NFS servers on the storage network, you must make sure there is a route from the management traffic network to the storage network.

### External Firewall Topology Requirements

When external firewall integration is in place, the public IP VLAN must still be trunked to the Hosts. This is required to support the Secondary Storage VM and Console Proxy VM.

### Advanced Zone Topology Requirements

With Advanced Networking, separate subnets must be used for private and public networks.

## XenServer Topology Requirements

- The Management Servers communicate with XenServer hosts on ports 22 (ssh), 80 (HTTP), and 443 (HTTPS).

## VMware Topology Requirements

- The Management Server and secondary storage VMs must be able to access vCenter and all ESXi hosts in the zone. To allow the necessary access through the firewall, keep port 443 open.
- The Management Servers communicate with VMware vCenter servers on port 443 (HTTPS).
- The Management Servers communicate with the System VMs on port 3922 (ssh) on the management traffic network.

## KVM Topology Requirements

The Management Servers communicate with KVM hosts on port 22 (ssh).

## External Guest Load Balancer Integration (Optional)

---

CloudPlatform can optionally use a Citrix NetScaler or BigIP F5 load balancer to provide load balancing services to guests. If this is not enabled, CloudPlatform will use the software load balancer in the virtual router.

To install and enable an external load balancer for CloudPlatform management:

1. Set up the appliance according to the vendor's directions.
2. Connect it to the networks carrying public traffic and management traffic (these could be the same network).
3. Record the IP address, username, password, public interface name, and private interface name. The interface names will be something like "1.1" or "1.2".
4. Make sure that the VLANs are trunked to the management network interface.
5. After the CloudPlatform Management Server is installed, log in as administrator to the CloudPlatform UI.
6. In the left navigation bar, click Infrastructure.
7. In Zones, click View More.
8. Choose the zone you want to work with.
9. Click the Network tab.
10. In the Network Service Providers node of the diagram, click Configure. (You might have to scroll down to see this.)
11. Click NetScaler or F5.
12. Click the Add button (+) and provide the following:

For the NetScaler:

- **IP address.** The IP address of the device.
- **Username/Password.** The authentication credentials to access the device. CloudPlatform uses these credentials to access the device.

- **Type.** The type of device that is being added. It could be F5 Big Ip Load Balancer, NetScaler VPX, NetScaler MPX, or NetScaler SDX. For a comparison of the NetScaler types, see the CloudPlatform Administration Guide.
- **Public interface.** Interface of device that is configured to be part of the public network.
- **Private interface.** Interface of device that is configured to be part of the private network.
- **Number of retries.** Number of times to attempt a command on the device before considering the operation failed. Default is 2.
- **Capacity.** Number of guest networks/accounts that will share this device.
- **Dedicated.** When marked as dedicated, this device will be dedicated to a single account. When Dedicated is checked, the value in the Capacity field has no significance – implicitly, its value is 1.

The installation and provisioning of the external load balancer is finished. You can proceed to add VMs and NAT/load balancing rules.

## Guest Network Usage Integration for Traffic Sentinel

---

To collect usage data for a guest network, CloudPlatform needs to pull the data from an external network statistics collector installed on the network. Metering statistics for guest networks are available through CloudPlatform's integration with inMon Traffic Sentinel™.

Traffic Sentinel is a network traffic usage data collection package. CloudPlatform can feed statistics from Traffic Sentinel into its own usage records, providing a basis for billing users of cloud infrastructure. Traffic Sentinel uses the traffic monitoring protocol sFlow®. Routers and switches generate sFlow records and provide them for collection by Traffic Sentinel, then CloudPlatform queries the Traffic Sentinel database to obtain this information.

To construct the query, CloudPlatform determines what guest IPs were in use during the current query interval. This includes both newly assigned IPs and IPs that were assigned in a previous time period and continued to be in use. CloudPlatform queries Traffic Sentinel for network statistics that apply to these IPs during the time period they remained allocated in CloudPlatform. The returned data is correlated with the customer account that owned each IP and the timestamps when IPs were assigned and released in order to create billable metering records in CloudPlatform. When the Usage Server runs, it collects this data.

To set up the integration between CloudPlatform and Traffic Sentinel:

1. On your network infrastructure, install Traffic Sentinel and configure it to gather traffic data. For installation and configuration steps, see inMon documentation at <http://inmon.com>.
2. In the Traffic Sentinel UI, configure Traffic Sentinel to accept script querying from guest users. CloudPlatform will be the guest user performing the remote queries to gather network usage for one or more IP addresses.
  - a. Click File – Users – Access Control – Reports Query, then select Guest from the dropdown list.
  - b. Click File – Users – Access Control – Reports Script, then select Guest from the dropdown list.
3. On CloudPlatform, add the Traffic Sentinel host by calling the CloudPlatform API command `addTrafficMonitor`. Pass in the URL of the Traffic Sentinel as protocol + host + port (optional); for example, `http://10.147.28.100:8080`. For the `addTrafficMonitor` command syntax, see the API Reference at [http://download.cloud.com/releases/3.0.0/api\\_3.0.0/root\\_admin/addTrafficMonitor.html](http://download.cloud.com/releases/3.0.0/api_3.0.0/root_admin/addTrafficMonitor.html). For information about how to call the CloudPlatform API, see the Developer's Guide at <http://support.citrix.com/product/cs>.

4. Log in to the CloudPlatform UI as administrator.
5. Click Configuration – Global Settings. Set the following:
  - `direct.network.stats.interval` – how often you want CloudPlatform to query Traffic Sentinel.

## Setting Zone VLAN and Running VM Maximums

---

In the external networking case, every VM in a zone must have a unique guest IP address. There are two variables that you need to consider in determining how to configure CloudPlatform to support this: how many Zone VLANs do you expect to have and how many VMs do you expect to have running in the Zone at any one time.

Use the following table to determine how to configure CloudPlatform for your deployment.

guest.vlan.bits	Maximum Running VMs per Zone	Maximum Zone VLANs
12	4096	4094
11	8192	2048
10	16384	1024
9	32768	512

Based on your deployment's needs, choose the appropriate value of `guest.vlan.bits`. Set it as described in [Edit the Global Configuration Settings \(Optional\)](#) on page 139 and restart the Management Server.

# Storage Setup

CloudPlatform is designed to work with a wide variety of commodity and enterprise-grade storage. Local disk may be used as well, if supported by the selected hypervisor. Storage type support for guest virtual disks differs based on hypervisor selection.

	XenServer	vSphere	KVM
NFS	Supported	Supported	Supported
iSCSI	Supported	Supported via VMFS	Supported via Clustered Filesystems
Fiber Channel	Supported via Pre-existing SR	Supported	Supported via Clustered Filesystems
Local Disk	Supported	Supported	Not Supported

The use of the Cluster Logical Volume Manager (CLVM) for KVM is not officially supported with CloudPlatform 3.0.3 - 3.0.5.

## Small-Scale Setup

In a small-scale setup, a single NFS server can function as both primary and secondary storage. The NFS server just needs to export two separate shares, one for primary storage and the other for secondary storage.

## Secondary Storage

CloudPlatform is designed to work with any scalable secondary storage system. The only requirement is the secondary storage system supports the NFS protocol.

The storage server should be a machine with a large number of disks. The disks should ideally be managed by a hardware RAID controller. Modern hardware RAID controllers support hot plug functionality independent of the operating system so you can replace faulty disks without impacting the running operating system.

## Example Configurations

In this section we go through a few examples of how to set up storage to work properly on a few types of NFS and iSCSI storage systems.

### Linux NFS on Local Disks and DAS

This section describes how to configure an NFS export on a standard Linux installation. The exact commands might vary depending on the operating system version.

1. Install the RHEL/CentOS distribution on the storage server.
2. If the root volume is more than 2 TB in size, create a smaller boot volume to install RHEL/CentOS. A root volume of 20 GB should be sufficient.
3. After the system is installed, create a directory called /export. This can each be a directory in the root partition itself or a mount point for a large disk volume.
4. If you have more than 16TB of storage on one host, create multiple EXT3 file systems and multiple NFS exports. Individual EXT3 file systems cannot exceed 16TB.
5. After /export directory is created, run the following command to configure it as an NFS export.

```
# echo "/export <CIDR>(rw,async,no_root_squash)" >> /etc/exports
```

Adjust the above command to suit your deployment needs.

- **Limiting NFS export.** It is highly recommended that you limit the NFS export to a particular subnet by specifying a subnet mask (e.g., "192.168.1.0/24"). By allowing access from only within the expected cluster, you avoid having non-pool member mount the storage. **The limit you place must include the management network(s) and the storage network(s).** If the two are the same network then one CIDR is sufficient. If you have a separate storage network you must provide separate CIDR's for both or one CIDR that is broad enough to span both.

The following is an example with separate CIDRs:

```
/export 192.168.1.0/24(rw,async,no_root_squash) 10.50.1.0/24(rw,async,no_root_squash)
```

- **Removing the async flag.** The async flag improves performance by allowing the NFS server to respond before writes are committed to the disk. Remove the async flag in your mission critical production deployment.
6. Run the following command to enable NFS service.

```
# chkconfig nfs on
```

7. Edit the /etc/sysconfig/nfs file and uncomment the following lines.

```
LOCKD_TCPPOINT=32803
LOCKD_UDPOINT=32769
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=662
STATD_OUTGOING_PORT=2020
```

8. Edit the /etc/sysconfig/iptables file and add the following lines at the beginning of the INPUT chain.

```
-A INPUT -m state --state NEW -p udp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 111 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 2049 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 32803 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 32769 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 892 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 875 -j ACCEPT
-A INPUT -m state --state NEW -p tcp --dport 662 -j ACCEPT
-A INPUT -m state --state NEW -p udp --dport 662 -j ACCEPT
```

## 9. Reboot the server.

An NFS share called /export is now set up.

## Linux NFS on iSCSI

Use the following steps to set up a Linux NFS server export on an iSCSI volume. These steps apply to RHEL/CentOS 5 distributions.

When copying and pasting a command, be sure the command has pasted as a single line before executing. Some document viewers may introduce unwanted line breaks in copied text.

### 1. Install iscsiadm.

```
# yum install iscsi-initiator-utils
# service iscsi start
# chkconfig --add iscsi
# chkconfig iscsi on
```

### 2. Discover the iSCSI target.

```
# iscsiadm -m discovery -t st -p <iSCSI Server IP address>:3260
```

For example:

```
# iscsiadm -m discovery -t st -p 172.23.10.240:3260
172.23.10.240:3260,1 iqn.2001-05.com.equallogic:0-8a0906-83bcb3401-16e0002fd0a46f3d-rhel5-test
```

### 3. Log in.

```
# iscsiadm -m node -T <Complete Target Name> -l -p <Group IP>:3260
```

For example:

```
# iscsiadm -m node -l -T iqn.2001-05.com.equallogic:83bcb3401-16e0002fd0a46f3d-rhel5-test -p 172.23.10.240:3260
```

### 4. Discover the SCSI disk. For example:

```
# iscsiadm -m session -P3 | grep Attached
Attached scsi disk sdb State: running
```

### 5. Format the disk as ext3 and mount the volume.

```
# mkfs.ext3 /dev/sdb
# mkdir -p /export
# mount /dev/sdb /export
```

### 6. Add the disk to /etc/fstab to make sure it gets mounted on boot.

```
/dev/sdb /export ext3 _netdev 0 0
```

Now you can set up /export as an NFS share.

- **Limiting NFS export.** In order to avoid data loss, it is highly recommended that you limit the NFS export to a particular subnet by specifying a subnet mask (e.g., "192.168.1.0/24"). By allowing access from only within the

expected cluster, you avoid having non-pool member mount the storage and inadvertently delete all its data. **The limit you place must include the management network(s) and the storage network(s).** If the two are the same network then one CIDR is sufficient. If you have a separate storage network you must provide separate CIDRs for both or one CIDR that is broad enough to span both.

The following is an example with separate CIDRs:

```
/export 192.168.1.0/24(rw,async,no_root_squash) 10.50.1.0/24(rw,async,no_root_squash)
```

- **Removing the async flag.** The async flag improves performance by allowing the NFS server to respond before writes are committed to the disk. Remove the async flag in your mission critical production deployment.

## Additional Installation Options

The next few sections describe CloudPlatform features above and beyond the basic deployment options.

### Edit the Global Configuration Settings (Optional)

CloudPlatform provides a variety of settings you can use to set limits, configure features, and enable or disable features in the cloud. Once your Management Server is running, you might need to set some of these global configuration parameters, depending on what optional features you are setting up. The documentation for each CloudPlatform feature should direct you to the names of the applicable parameters. Many of them are discussed in the CloudPlatform Administration Guide. The following table shows a few of the more useful parameters.

Field	Value
management.network.cidr	A CIDR that describes the network that the management CIDRs reside on. <b>This variable must be set for deployments that use vSphere.</b> It is recommended to be set for other deployments as well. Example: 192.168.3.0/24.
xen.setup.multipath	For XenServer nodes, this is a true/false variable that instructs CloudPlatform to enable iSCSI multipath on the XenServer Hosts when they are added. This defaults to false. Set it to true if you would like CloudPlatform to enable multipath.  If this is true for a NFS-based deployment multipath will still be enabled on the XenServer host. However, this does not impact NFS operation and is harmless.
secstorage.allowed.internal.sites	This is used to protect your internal network from rogue attempts to download arbitrary files using the template download feature. This is a comma-separated list of CIDRs. If a requested URL matches any of these CIDRs the Secondary Storage VM will use the private network interface to fetch the URL. Other URLs will go through the public interface. We suggest you set this to 1 or 2 hardened internal machines where you keep your templates. For example, set it to 192.168.1.66/32.
use.local.storage	Determines whether CloudPlatform will use storage that is local to the Host for data disks, templates, and snapshots. By default CloudPlatform will not use this storage. You should change this to true if you want to use local storage and you understand the reliability and feature drawbacks to choosing local storage.
host	This is the IP address of the Management Server. If you are using multiple Management Servers you should enter a load balanced IP address that is reachable via the private network.


default.page.size	Maximum number of items per page that can be returned by a CloudPlatform API command. The limit applies at the cloud level and can vary from cloud to cloud. You can override this with a lower value on a particular API call by using the page and pagesize API command parameters. For more information, see the Developer's Guide. Default: 500.
ha.tag	The label you want to use throughout the cloud to designate certain hosts as dedicated HA hosts. These hosts will be used only for HA-enabled VMs that are restarting due to the failure of another host. For example, you could set this to ha_host. Specify the ha.tag value as a host tag when you add a new host to the cloud.

To modify global configuration parameters:

1. Log in as administrator to the CloudPlatform UI. Substitute your own management server IP address.

```
http://management-server-ip-address:8080/client
```

The default credentials are “admin” for user and “password” for password. The domain field should be left blank. A blank domain field is defaulted to the ROOT domain.

2. In the left navigation bar, click Global Settings.
3. Use the Search box to find the setting you need.
4. Click the Edit button next to the parameter, type a new value, then click the Apply icon. 
5. After you change any global configuration parameter, restart the Management Server. You might also need to restart other services as directed in the confirmation popup dialog that appears when you click Apply.

```
# service cloud-management restart
```

## Installing the Usage Server (Optional)

You can optionally install the Usage Server once the Management Server is configured properly. The Usage Server takes data from the events in the system and enables usage-based billing for accounts.

When multiple Management Servers are present, the Usage Server may be installed on any number of them. The Usage Servers will coordinate usage processing. A site that is concerned about availability should install Usage Servers on at least two Management Servers.

## Requirements for Installing the Usage Server

- The Management Server must be running when the Usage Server is installed.
- The Usage Server must be installed on the same server as a Management Server.

## Steps to Install the Usage Server

1. Run `./install.sh`.

```
# ./install.sh
```

You should see a few messages as the installer prepares, followed by a list of choices.

2. Choose “S” to install the Usage Server.

```
> S
```

3. Once installed, start the Usage Server with the following command.

```
# service cloud-usage start
```

The Administration Guide discusses further configuration of the Usage Server.

## SSL (Optional)

---

CloudPlatform provides HTTP access in its default installation. There are a number of technologies and sites which choose to implement SSL. As a result, we have left CloudPlatform to expose HTTP under the assumption that a site will implement its typical practice.

CloudPlatform uses Tomcat as its servlet container. For sites that would like CloudPlatform to terminate the SSL session, Tomcat’s SSL access may be enabled. Tomcat SSL configuration is described at <http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html>.

## Database Replication (Optional)

---

CloudPlatform supports database replication from one MySQL node to another. This is achieved using standard MySQL replication. You may want to do this as insurance against MySQL server or storage loss. MySQL replication is implemented using a master/slave model. The master is the node that the Management Servers are configured to use. The slave is a standby node that receives all write operations from the master and applies them to a local, redundant copy of the database. The following steps are a guide to implementing MySQL replication.

Creating a replica is not a backup solution. You should develop a backup procedure for the MySQL data that is distinct from replication.

1. Ensure that this is a fresh install with no data in the master.
2. Edit `my.cnf` on the master and add the following in the `[mysqld]` section below `datadir`.

```
log_bin=mysql-bin  
server_id=1
```

The `server_id` must be unique with respect to other servers. The recommended way to achieve this is to give the master an ID of 1 and each slave a sequential number greater than 1, so that the servers are numbered 1, 2, 3, etc.

**3.** Restart the MySQL service:

```
# service mysqld restart
```

**4.** Create a replication account on the master and give it privileges. We will use the “cloud-repl” user with the password “password”. This assumes that master and slave run on the 172.16.1.0/24 network.

```
# mysql -u root
mysql> create user 'cloud-repl'@'172.16.1.%' identified by 'password';
mysql> grant replication slave on *.* TO 'cloud-repl'@'172.16.1.%;
mysql> flush privileges;
mysql> flush tables with read lock;
```

**5.** Leave the current MySQL session running.**6.** In a new shell start a second MySQL session.**7.** Retrieve the current position of the database.

```
# mysql -u root
mysql> show master status;
+-----+-----+-----+-----+
| File           | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+-----+-----+-----+-----+
| mysql-bin.000001 |      412 |              |                  |
+-----+-----+-----+-----+
```

**8.** Note the file and the position that are returned by your instance.**9.** Exit from this session.**10.** Complete the master setup. Returning to your first session on the master, release the locks and exit MySQL.

```
mysql> unlock tables;
```

**11.** Install and configure the slave. On the slave server, run the following commands.

```
# yum install mysql-server
# chkconfig mysqld on
```

**12.** Edit my.cnf and add the following lines in the [mysqld] section below datadir.

```
server_id=2
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
```

**13.** Restart MySQL.

```
# service mysqld restart
```

14. Instruct the slave to connect to and replicate from the master. Replace the IP address, password, log file, and position with the values you have used in the previous steps.

```
mysql> change master to
-> master_host='172.16.1.217',
-> master_user='cloud-repl',
-> master_password='password',
-> master_log_file='mysql-bin.000001',
-> master_log_pos=412;
```

15. Then start replication on the slave.

```
mysql> start slave;
```

16. Optionally, open port 3306 on the slave as was done on the master earlier.

This is not required for replication to work. But if you choose not to do this, you will need to do it when failover to the replica occurs.

## Failover

This will provide for a replicated database that can be used to implement manual failover for the Management Servers. CloudPlatform failover from one MySQL instance to another is performed by the administrator. In the event of a database failure you should:

1. Stop the Management Servers (via service cloud-management stop).
2. Change the replica's configuration to be a master and restart it.
3. Ensure that the replica's port 3306 is open to the Management Servers.
4. Make a change so that the Management Server uses the new database. The simplest process here is to put the IP address of the new database server into each Management Server's `/etc/cloud/management/db.properties`.
5. Restart the Management Servers:

```
# service cloud-management start
```

## Amazon Web Services API Compatibility (Optional)

---

(Introduced in CloudPlatform 3.0.3)

CloudPlatform can translate Amazon Web Services (AWS) API calls to native CloudPlatform (CloudStack) API calls so that clients can continue using existing AWS-compatible tools. This translation service runs as a separate web application in the same tomcat server as CloudPlatform, listening on the same port. This Amazon EC2-compatible API is accessible through a SOAP web service.

Limitations:

- Supported only in zones that use basic networking.
- Available in fresh installations of CloudPlatform 3.0.3 and greater. Not available through upgrade of previous versions.

- If you need to support features such as elastic IP, set up a Citrix NetScaler to provide this service. The commands such as `ec2-associate-address` will not work without EIP setup; see Elastic IP Addresses on page 146 for a list of these commands. Users running VMs in this zone will be using the NetScaler-enabled network offering (`DefaultSharedNetscalerEIPandELBNetworkOffering`).

## System Requirements for AWS API Compatibility

This feature has the same system requirements as CloudPlatform, with the addition of the following:

<b>EC2 tools v. 1.3.6230</b>	Client interface to the Amazon EC2 service	CloudPlatform works with version 1.3.6230 of the EC2 Tools. Download the correct version here: <a href="http://s3.amazonaws.com/ec2-downloads/ec2-api-tools-1.3-62308.zip">http://s3.amazonaws.com/ec2-downloads/ec2-api-tools-1.3-62308.zip</a>
------------------------------	--	---

The CloudPlatform AWS API compatibility feature complies with Amazon's WDSL version dated November 15, 2010, available at <http://ec2.amazonaws.com/doc/2010-11-15/>.

## Enabling AWS API Compatibility

The software that provides AWS API compatibility is installed along with CloudPlatform. However, you must enable the feature and perform some setup steps.

1. Set the global configuration parameter `enable.ec2.api` to `true`. See Edit the Global Configuration Settings (Optional) on page 139.
2. Create a set of CloudPlatform service offerings with names that match the Amazon service offerings. You can do this through the CloudPlatform UI as described in the Administration Guide.

**WARNING:** Be sure you have included the Amazon default service offering, `m1.small`.

3. If you did not already do so when you set the configuration parameter in step 1, restart the Management Server.

```
# service cloud-management restart
```

4. (Optional) The AWS API listens for requests on port 7080. If you prefer AWS API to listen on another port, you can change it as follows:
  - a. Edit the files `/etc/cloud/management/server.xml`, `/etc/cloud/management/server-nonssl.xml`, and `/etc/cloud/management/server-ssl.xml`.
  - b. In each file, find the tag `<Service name="Catalina7080">`. Under this tag, locate `<Connector executor="tomcatThreadPool-internal" port= .....>`.
  - c. Change the port to whatever port you want to use, then save the files.
  - d. Restart the Management Server.
  - e. If you re-install CloudPlatform, make these changes again.

## AWS API User Setup

In general, users need not be aware that they are using a translation service provided by CloudPlatform. They need only send AWS API calls to CloudPlatform's endpoint, and it will translate the calls to the native API. However, each user must perform the following setup steps:

- Register.
- Set up their environment and/or tools appropriately.
- For SOAP access, use the endpoint `http://<cloud-platform-server>:7080/awsapi`. The cloud platform server can be specified by a fully-qualified domain name or IP address.

Each user must perform a one-time registration. The user follows these steps:

1. Obtain the following from your cloud administrator:
  - The CloudPlatform server's publicly available DNS name or IP address
  - Your account's API key and Secret key
2. Generate a private key and a self-signed X.509 certificate. Substitute your own desired storage location for `/path/to/...` below.

```
$ openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /path/to/private_key.pem -  
out /path/to/cert.pem
```

3. Register the mapping from the X.509 certificate to the API/Secret keys. Download the following script from <http://download.cloud.com/releases/3.0.3/cloudstack-aws-api-register> and run it. Substitute the values you obtained from the administrator in the URL below.

```
$ cloudstack-aws-api-register --apikey=<User's CloudPlatform API key> --  
secretkey=<User's CloudPlatform Secret key> --cert=</path/to/cert.pem> --  
url=http://<cloud-platform-server>:7080/awsapi
```

4. Be sure you have the right version of EC2 Tools. The supported version is available at <http://s3.amazonaws.com/ec2-downloads/ec2-api-tools-1.3-62308.zip>.
5. Set up the environment variables that will direct the tools to the server. As a best practice, you may wish to place these commands in a script that may be sourced before using the AWS API translation feature.

```
$ export EC2_CERT=/path/to/cert.pem  
$ export EC2_PRIVATE_KEY=/path/to/private_key.pem  
$ export EC2_URL=http://<cloud-platform-server>:7080/awsapi  
$ export EC2_HOME=/path/to/EC2_installation_directory
```

For more information about how to set up your Amazon EC2 environment for use with the Amazon EC2 command line tools, see:

- [http://docs.amazonwebservices.com/AWSEC2/2010-11-15/UserGuide/index.html?SettingUp\\_CommandLine.html](http://docs.amazonwebservices.com/AWSEC2/2010-11-15/UserGuide/index.html?SettingUp_CommandLine.html)

## Ensuring AWS API Command Completion: Timeouts

The Amazon EC2 command-line tools have a default connection timeout. When used with CloudPlatform, a longer timeout might be needed for some commands. If you find that commands are not completing due to timeouts, you can gain more

time for commands to finish by overriding the default timeouts on individual commands. You can add the following optional command-line parameters to any CloudPlatform-supported EC2 command:

<code>--connection-timeout <i>TIMEOUT</i></code>	Specifies a connection timeout (in seconds). Example: <code>--connection-timeout 30</code>
<code>--request-timeout <i>TIMEOUT</i></code>	Specifies a request timeout (in seconds). Example: <code>--request-timeout 45</code>

Example:

```
ec2-run-instances 2 -z us-test1 -n 1-3 --connection-timeout 120 --request-timeout 120
```

## Supported AWS API Commands and Parameters

The following Amazon EC2 commands are supported by CloudPlatform when the AWS API compatibility feature is enabled. For a few commands, there are differences between the CloudPlatform and Amazon EC2 versions, and these differences are noted. The underlying SOAP call for each command is also given, for those who have built tools using those calls.

More information:

- [CloudStack API](#)
- [Amazon EC2 API](#)

## Elastic IP Addresses

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-allocate-address	AllocateAddress	associateIpAddress
ec2-associate-address	AssociateAddress	enableStaticNat
<b>Supported parameters</b> Required: ip_address, -i --instance instance_id		
ec2-describe-addresses  <b>Supported parameters</b> Optional: public_ip, --filter name=value  The following filters are supported: instance-id public-ip	DescribeAddresses	listPublicIpAddresses
ec2-disassociate-address  <b>Supported parameters</b> Required: ip_address	DisassociateAddress	disableStaticNat
ec2-release-address  <b>Supported parameters</b>	ReleaseAddress	disassociateIpAddress

Required: ip_address		
----------------------	--	--

## Availability Zones

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-describe-availability-zones	DescribeAvailabilityZones	listZones
<b>Supported Parameters</b> Optional: [zone_name ...]		

## Images

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-create-image  <b>Supported Parameters</b> Required: instance_id Optional: --name name, --description description	CreateImage	createTemplate
ec2-deregister  <b>Supported Parameters</b> Required: ami_id	DeregisterImage	deleteTemplate
ec2-describe-images  <b>Supported Parameters</b> Optional: ami_id	DescribeImages	listTemplates
ec2-register  <b>Supported Parameters</b> Required: name, -a architecture Optional: [imageLocation] [-d description] <ul style="list-style-type: none"> <li>In CloudPlatform, the <code>architecture</code> parameter is required and is used to pass the following required values: the template format (QCOW2, RAW, or VHD); zone where the template is hosted; template OS; and hypervisor type. Use the format "<code>&lt;format&gt;:&lt;zoneName&gt;:&lt;osTypeName&gt;:&lt;hypervisor&gt;</code>". For example, "VHD:ZONE1:Centos 5.3 (64-bit):xenserver"</li> <li>The <code>imageLocation</code> parameter is the URL where the template is hosted, starting with <code>http://</code> or <code>https://</code>.</li> </ul>	RegisterImage	registerTemplate

## Image Attributes

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-describe-image-attribute	DescribeImageAttribute	listTemplatePermissions

<b>Supported Parameters</b> Required: ami_id, --launch-permission		
ec2-modify-image-attribute  <b>Supported Parameters</b> Required: ami_id, --launch-permission Optional: [--add all   --remove all]	ModifyImageAttribute	updateTemplatePermissions
ec2-reset-image-attribute  <b>Supported Parameters</b> Required: ami_id, --launch-permission	ResetImageAttribute	updateTemplatePermissions

## Instances

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-describe-instances  <b>Supported Parameters</b> Optional: [instance_id ...] [--filter name=value] ...]  The following filters are supported:  availability-zone hypervisor image-id instance-id instance-state-code instance-state-name instance-type ip-address owner-id private-ip-address	DescribeInstances	listVirtualMachines
ec2-run-instances  <b>Supported Parameters</b> Required: ami_id Optional: [--availability-zone zone] [-n instance_count] [-g group [-g group ...]] [-k keypair] [-d user_data  -f user_data_file] [-- instance-type instance_type]	RunInstances	deployVirtualMachine
ec2-reboot-instances  <b>Supported Parameters</b> Required: instance_id Optional: instance_id...	RebootInstances	rebootVirtualMachine
ec2-start-instances  <b>Supported Parameters</b> Required: instance_id Optional: instance_id...	StartInstances	startVirtualMachine

ec2-stop-instances  <b>Supported Parameters</b> Required: instance_id Optional: instance_id...	StopInstances	stopVirtualMachine
ec2-terminate-instances  <b>Supported Parameters</b> Required: instance_id Optional: instance_id...	TerminateInstances	destroyVirtualMachine

## Instance Attributes

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-describe-instance-attribute  <ul style="list-style-type: none"> <li>Partially supported. Only the &lt;instanceId&gt; -t options are supported.</li> </ul> <b>Supported Parameters</b> Required: instance_id Optional: --instance-type type	DescribeInstanceAttribute	listVirtualMachines

## Key Pairs

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-add-keypair  <b>Supported Parameters:</b> Required: key	CreateKeyPair	createSSHKeyPair
ec2-delete-keypair  <b>Supported Parameters:</b> Required: key_pair	DeleteKeyPair	deleteSSHKeyPair
ec2-describe-keypairs  <b>Supported Parameters:</b> Optional: [keypair_name ...] [--filter name=value] ...  The following filters are supported: fingerprint key-name	DescribeKeyPairs	listSSHKeyPairs
ec2-import-keypair  <b>Supported Parameters</b> Required: key_name --public-key-file key_file	ImportKeyPair	registerSSHKeyPair

## Passwords

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-get-password	GetPasswordData	getVMPassword
<b>Supported Parameters</b> Required: instanceld -k key_file		

## Security Groups

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-authorize	AuthorizeSecurityGroupIngress	authorizeSecurityGroupIngress
<b>Supported Parameters</b> Required: group Optional: [-P protocol] (-p port_range   -t icmp_type_code) [-u source_group_user ...] [-o source_group ...] [-s source_subnet ...]		
ec2-add-group	CreateSecurityGroup	createSecurityGroup
<b>Supported Parameters</b> Required: group -d description		
ec2-delete-group	DeleteSecurityGroup	deleteSecurityGroup
<b>Supported Parameters</b> Required: group		
ec2-describe-group	DescribeSecurityGroups	listSecurityGroups
<b>Supported Parameters</b> Optional: [group_name ...] [--filter name=value] ...  The following filters are supported: description group-name ip-permission.cidr ip-permission.from-port ip-permission.protocol ip-permission.to-port owner-id		
ec2-revoke	RevokeSecurityGroupIngress	revokeSecurityGroupIngress
<b>Supported Parameters</b> Required: group Optional: [-P protocol] (-p port_range   -t icmp_type_code) [-o source_group ...] [-u source_group_user ...] [-s source_subnet ...]		

## Snapshots

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-create-snapshot  <b>Supported Parameters</b> Required: volume_id	CreateSnapshot	createSnapshot
ec2-delete-snapshot  <b>Supported Parameters</b> Required: snapshot_id	DeleteSnapshot	deleteSnapshot
ec2-describe-snapshots  <b>Supported Parameters</b> Optional: [snapshot_id ...] [-a] [-o owner ...] [-r user_id] [--filter name=value] ...  The following filters are supported: owner-alias owner-id (use the CloudPlatform API key) snapshot-id volume-id volume-size	DescribeSnapshots	listSnapshots

## Volumes

EC2 Command	SOAP Call	CloudPlatform API Call
ec2-attach-volume  <b>Supported Parameters</b> Required: volume_id,-i --instance instance_id,-d --device device	AttachVolume	attachVolume
ec2-create-volume  <ul style="list-style-type: none"> <li>Must have at least one disk offering with customizable disk size available.</li> </ul> <b>Supported Parameters</b> Required: --availability-zone zone  Optional: size <size> , snapshot <snapshot>	CreateVolume	createVolume
ec2-delete-volume  <b>Supported Parameters</b> Required: volume_id	DeleteVolume	deleteVolume

<p>ec2-describe-volumes</p> <p><b>Supported Parameters</b> Optional: [volume_id ...] [--filter name=value] ...]</p> <p>The following filters are supported:</p> <p>attachment.device attachment.instance-id availability-zone size snapshot-id status volume-id</p>	DescribeVolumes	listVolumes
<p>ec2-detach-volume</p> <ul style="list-style-type: none"><li>• The optional parameters instance_id and device are not needed for CloudPlatform.</li></ul> <p><b>Supported Parameters</b> Required: volume_id Optional: instance &lt;instance_id&gt;,device &lt;device&gt;</p>	DetachVolume	detachVolume

# Best Practices

---

Deploying a cloud is challenging. There are many different technology choices to make, and CloudPlatform is flexible enough in its configuration that there are many possible ways to combine and configure the chosen technology. This section contains suggestions and requirements about cloud deployments.

These should be treated as suggestions and not absolutes. However, we do encourage anyone planning to build a cloud outside of these guidelines to discuss their needs with us.

## Process Best Practices

---

- A staging system that models the production environment is strongly advised. It is critical if customizations have been applied to CloudPlatform.
- Allow adequate time for installation, a beta, and learning the system. Installs with basic networking can be done in hours. Installs with advanced networking usually take several days for the first attempt, with complicated installations taking longer. For a full production system, allow at least 4-8 weeks for a beta to work through all of the integration issues. If you are in contact with the CloudPlatform sales team, you can contact your representative to discuss the options for obtaining help and training. CloudPlatform also offers a variety of ways to submit support requests and get help from fellow users; see [Contacting Support](#) on page 161.

## Setup Best Practices

---

- Each host should be configured to accept connections only from well-known entities such as the CloudPlatform Management Server or your network monitoring software.
- Use multiple clusters per pod if you need to achieve a certain switch density.
- Primary storage mountpoints or LUNs should not exceed 6 TB in size. It is better to have multiple smaller primary storage elements per cluster than one large one.
- When exporting shares on primary storage, avoid data loss by restricting the range of IP addresses that can access the storage. See "Linux NFS on Local Disks and DAS" on page 135 or "Linux NFS on iSCSI" on page 137.
- NIC bonding is straightforward to implement and provides increased reliability.
- 10G networks are generally recommended for storage access when larger servers that can support relatively more VMs are used.
- Host capacity should generally be modeled in terms of RAM for the guests. Storage and CPU may be overprovisioned. RAM may not. RAM is usually the limiting factor in capacity designs.
- (XenServer) Configure the XenServer dom0 settings to allocate more memory to dom0. This can enable XenServer to handle larger numbers of virtual machines. We recommend 2940 MB of RAM for XenServer dom0. For instructions on how to do this, see <http://support.citrix.com/article/CTX126531>. The article refers to XenServer 5.6, but the same information applies to XenServer 6.0.

## Maintenance Best Practices

---

- Monitor host disk space. Many host failures occur because the host's root disk fills up from logs that were not rotated adequately.

- Monitor the total number of VM instances in each cluster, and disable allocation to the cluster if the total is approaching the maximum that the hypervisor can handle. Be sure to leave a safety margin to allow for the possibility of one or more hosts failing, which would increase the VM load on the other hosts as the VMs are redeployed. Consult the documentation for your chosen hypervisor to find the maximum permitted number of VMs per host, then use CloudPlatform global configuration settings to set this as the default limit. Monitor the VM activity in each cluster and keep the total number of VMs below a safe level that allows for the occasional host failure. For example, if there are N hosts in the cluster, and you want to allow for one host in the cluster to be down at any given time, the total number of VM instances you can permit in the cluster is at most  $(N-1) * (\text{per-host-limit})$ . Once a cluster reaches this number of VMs, use the CloudPlatform UI to disable allocation to the cluster.
- Be sure all the hotfixes provided by the hypervisor vendor are applied. Track the release of hypervisor patches through your hypervisor vendor's support channel, and apply patches as soon as possible after they are released. CloudPlatform will not track or notify you of required hypervisor patches. It is essential that your hosts are completely up to date with the provided hypervisor patches. The hypervisor vendor is likely to refuse to support any system that is not up to date with patches. XenServer users can find more information at [Highly Recommended Hotfixes for XenServer](#) in the CloudPlatform Knowledge Base.

**WARNING**

The lack of up-to-date hotfixes can lead to data corruption and lost VMs.

# Troubleshooting

## Checking the Management Server Log

The command below shows a quick way to look for errors in the management server log. When copying and pasting this command, be sure the command has been pasted as a single line before executing. Some document viewers may introduce unwanted line breaks in copied text.

```
# grep -i -E 'exception|unable|fail|invalid|leak|invalid|warn'  
/var/log/cloud/management/management-server.log
```

## Troubleshooting the Secondary Storage VM

Many install problems relate to the secondary storage VM. Sample common problems:

- SSVM cannot reach the DNS server
- SSVM cannot reach the Management Server
- SSVM cannot reach the outside world to download templates. It contacts download.cloud.com via HTTP.
- The configured DNS server cannot resolve your internal hostnames. E.g., you entered private-nfs.lab.example.org for secondary storage NFS, but gave a DNS server that your customers use, and that server cannot resolve private-nfs.lab.example.org.

To recover a failed SSVM after making changes that fix the root cause of the failure, you must stop the VM first and then start it. A restart merely reboots the VM without resending the configuration, which may have changed.

You can troubleshoot the secondary storage VM either by running a diagnostic script or by checking the log file. The following sections detail each of these methods.

If you have corrected the problem but the template hasn't started to download, restart the cloud service with "service cloud restart". This will restart the default CentOS template download.

## Running a Diagnostic Script

You can log into the SSVM. To do this you have to find the host running the SSVM, ssh into it, then ssh into the SSVM's private IP from that host. Once you are logged in, use the following steps to run a diagnostic script.

1. In the admin UI, go to Infrastructure -> Virtual Resources -> System VMs. Select the target VM.
2. Note the name of the host hosting the SSVM as shown in the Host row. Also note the private IP of the SSVM as shown in the Private IP row.

### 3. ssh into the private IP of the SSVM with the following.

For XenServer or KVM:

- ssh into the host using your known user and password.
- Run this command:

```
# ssh -i /root/.ssh/id_rsa.cloud -p 3922 root@link-local-ip
```

For VMware:

- ssh into the CloudPlatform Management Server using your known user and password.
- Run this command:

```
# ssh -i /var/lib/cloud/management/.ssh/id_rsa -p 3922 root@private-ip
```

### 4. Once into the SSVM, run the following diagnostic script:

```
# /usr/local/cloud/systemvm/ssvm-check.sh
```

This script will test various aspects of the SSVM and report warnings and errors.

## Checking the Log Files

You can also check the log files in `/var/log/cloud/` for any error messages.

## Troubleshooting AWS API Compatibility

---

The log file for messages related to translation of Amazon Web Services API calls is located in `var/log/cloud/awsapi.log`.

## VLAN Issues

---

A common installation issue is that your VLANs are not set up correctly. VLANs must be trunked into every host in the zone.

## Console Proxy VM Issues

---

### Symptom

When you launch the Console Viewer, you see this error:

```
Access is denied for console session. Please close the window
```

### Cause

This most likely means that the Console Proxy VM cannot connect from its private interface to port 8250 on the Management Server (or load balanced Management server pool).

## Solution

Check the following:

- Load balancer has port 8250 open
- All Management Servers have port 8250 open
- There is a network path from the CIDR in the pod hosting the Console Proxy VM to the load balancer or Management Server
- The "host" global configuration parameter is set to the load balancer if in use

## Binary Logging Error when Upgrading Database

---

### Symptom

When attempting to upgrade the database, an error like the following:

```
Unable to upgrade the db due to java.sql.SQLException: Binary logging not possible.
```

### Cause

Binary logging is not enabled.

### Solution

1. Edit the MySQL configuration (/etc/my.cnf or /etc/mysql/my.cnf, depending on your OS) and set the log-bin and binlog-format variables in the [mysqld] section. For example:

```
log-bin=mysql-bin  
binlog-format= 'ROW'
```

2. After editing my.cnf, restart the MySQL server.

```
# service mysqld restart
```

**NOTE:** The binlog-format variable is supported in MySQL versions 5.1 and greater. It is not supported in MySQL 5.0. In some versions of MySQL, an underscore character is used in place of the hyphen in the variable name. For the exact syntax and spelling of each variable, consult the documentation for your version of MySQL.

## Can't Add Host

---

A host must have a statically allocated IP address. Host addition will error and fail if a dynamically-assigned address is present.

# Preparation Checklists

Start by gathering the information in the following checklists. This will make installation go more smoothly.

## Management Server Checklist

You will need the following information for the Management Server.

Installation Requirement	Value	Notes
IP Address		No IPV6 addresses
Netmask		
Gateway		
FQDN		DNS should resolve the FQDN of the Management Server.
Root user		Login id of the root user.
Root password		Password for the root user.
OS	Choose: RHEL 6.2 (or later) or CentOS 6.2 (or later)	Choose one of the supported OS platforms.
ISO Available		CloudPlatform requires the ISO used for installing the OS in order to install dependent RPMS.

## Database Checklist

---

For database setup, you will need the following information.

Installation Requirement	Value	Notes
IP Address		Do not use IPV6 addresses.
Netmask		
Gateway		
FQDN		DNS should resolve the FQDN of the Database Server.
Root user		Login id of the root user.
Root password		Password for the root user.
OS	Choose: RHEL 6.2 (or later) or CentOS 6.2 (or later)	Choose one of the supported OS platforms.
ISO Available		CloudPlatform requires the ISO used for installing the OS in order to install dependent RPMS.
Username for Cloud User in MySQL		Default is cloud.
Password for Cloud user in MySQL		Default is password.

## Storage Checklist

CloudPlatform requires two types of storage: Primary (in a Basic Installation, this uses local disk) and Secondary Storage (NFS). The volumes used for Primary and Secondary storage should be accessible from Management Server and the hypervisors. These volumes should allow root users to read/write data. These volumes must be for the exclusive use of CloudPlatform and should not contain any data.

You will need the following information when setting up storage.

Installation Requirement	Value	Notes
Type of Storage	Choose: NFS or iSCSI or local	
Storage Server IP Address		
Storage Server Path		
Storage Size		
Secondary Storage Type	NFS	Only NFS is supported.
Secondary Storage IP Address(es)		
Secondary Storage Path		
Secondary Storage Size		
Existing data backed up?		Please back up any data on Primary and Secondary storage volumes, as they may be overwritten by CloudPlatform.

## Contacting Support

---

The CloudPlatform support team is available to help customers plan and execute their installations. To contact the support team, log in to the support portal at <http://support.citrix.com/cloudsupport> using the account credentials you received when you purchased your support contract.