



# CloudStack Advanced Installation Guide

For CloudStack Version 3.0.0 – 3.0.2

Revised August 16, 2012 3:17 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 CloudStack 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 .....                          | 10 |
| What Is CloudStack? .....                           | 11 |
| What Can CloudStack Do? .....                       | 12 |
| Deployment Architecture Overview .....              | 13 |
| Management Server Overview .....                    | 13 |
| Cloud Infrastructure Overview .....                 | 14 |
| Networking Overview .....                           | 15 |
| Overview of Installation Steps .....                | 16 |
| System Requirements .....                           | 17 |
| Management Server Single-Node Installation .....    | 19 |
| Prepare the Operating System .....                  | 19 |
| Install the Management Server .....                 | 21 |
| Install and Configure the Database .....            | 22 |
| Prepare NFS Shares .....                            | 24 |
| Using a Separate NFS Server .....                   | 24 |
| About Password and Key Encryption .....             | 25 |
| Using the Management Server as the NFS Server ..... | 26 |
| Prepare the System VM Template .....                | 27 |
| Single-Node Installation Complete! Next Steps ..... | 28 |
| Management Server Multi-Node Installation .....     | 30 |
| Prepare the Operating System .....                  | 30 |
| Install the First Management Server .....           | 32 |
| Install and Configure the Database .....            | 33 |
| About Password and Key Encryption .....             | 35 |
| Prepare NFS Shares .....                            | 35 |

|   |    |
|---|----|
| Using a Separate NFS Server .....                     | 35 |
| Using the Management Server as the NFS Server .....   | 36 |
| Prepare and Start Additional Management Servers ..... | 38 |
| Prepare the System VM Template .....                  | 39 |
| Multi-Node Installation Complete! Next Steps .....    | 40 |
| Log In to the CloudStack UI .....                     | 41 |
| Provision Your Cloud Infrastructure .....             | 42 |
| Change the Root Password .....                        | 43 |
| Add a Zone .....                                      | 44 |
| About Zones .....                                     | 44 |
| About Physical Networks .....                         | 45 |
| Basic Zone Network Traffic Types .....                | 45 |
| Basic Zone Guest IP Addresses .....                   | 46 |
| Advanced Zone Network Traffic Types .....             | 46 |
| Advanced Zone Guest IP Addresses .....                | 46 |
| Advanced Zone Public IP Addresses .....               | 46 |
| System Reserved IP Addresses .....                    | 47 |
| Using Security Groups to Control Traffic to VMs ..... | 48 |
| About Security Groups .....                           | 48 |
| Enabling Security Groups .....                        | 48 |
| Working With Security Groups .....                    | 48 |
| Adding a Zone .....                                   | 48 |
| Basic Zone Configuration .....                        | 49 |
| Advanced Zone Configuration .....                     | 54 |
| Add More Pods (Optional) .....                        | 58 |
| About Pods .....                                      | 58 |
| Adding a Pod .....                                    | 58 |

|  |    |
|--|----|
| Add More Clusters (Optional) .....                     | 60 |
| About Clusters .....                                   | 60 |
| Add Cluster: KVM or XenServer .....                    | 60 |
| Add Cluster: vSphere .....                             | 61 |
| Add Cluster: OVM .....                                 | 62 |
| Add More Hosts (Optional) .....                        | 64 |
| About Hosts .....                                      | 64 |
| Host Allocation.....                                   | 64 |
| Install Hypervisor Software on Hosts.....              | 65 |
| Add Hosts to CloudStack (XenServer, KVM, or OVM) ..... | 65 |
| Requirements for XenServer, KVM, and OVM Hosts .....   | 65 |
| Adding a XenServer, KVM, or OVM Host .....             | 66 |
| Add Hosts (vSphere) .....                              | 67 |
| Add Primary Storage.....                               | 68 |
| About Primary Storage .....                            | 68 |
| System Requirements for Primary Storage.....           | 68 |
| Adding Primary Storage .....                           | 68 |
| Add Secondary Storage.....                             | 70 |
| About Secondary Storage .....                          | 70 |
| System Requirements for Secondary Storage .....        | 70 |
| Adding Secondary Storage .....                         | 70 |
| Initialization and Testing.....                        | 72 |
| Citrix XenServer Installation for CloudStack .....     | 73 |
| System Requirements for XenServer Hosts .....          | 73 |
| XenServer Installation Steps .....                     | 73 |
| Configure XenServer dom0 Memory .....                  | 74 |
| Username and Password .....                            | 74 |

|  |    |
|--|----|
| Time Synchronization .....   | 74 |
| Licensing .....  | 75 |
| Getting and Deploying a License.....   | 75 |
| Install CloudStack XenServer Support Package (CSP) .....                       | 75 |
| Primary Storage Setup for XenServer .....                                      | 76 |
| iSCSI Multipath Setup for XenServer (Optional) .....                           | 77 |
| Physical Networking Setup for XenServer .....                                  | 77 |
| Configuring Public Network with a Dedicated NIC for XenServer (Optional) ..... | 78 |
| Configuring Multiple Guest Networks for XenServer (Optional) .....             | 78 |
| Separate Storage Network for XenServer (Optional) .....                        | 79 |
| NIC Bonding for XenServer (Optional) .....                                     | 79 |
| Upgrading XenServer Versions .....   | 81 |
| VMware vSphere Installation and Configuration .....                            | 84 |
| System Requirements for vSphere Hosts .....                                    | 84 |
| Preparation Checklist for VMware.....  | 85 |
| vCenter Checklist .....  | 86 |
| Networking Checklist for VMware .....  | 86 |
| vSphere Installation Steps .....   | 87 |
| ESXi Host setup .....  | 87 |
| Physical Host Networking .....   | 88 |
| Configure Virtual Switch .....   | 88 |
| Configure vCenter Management Network .....                                     | 90 |
| Extend Port Range for CloudStack Console Proxy .....                           | 92 |
| Configure NIC Bonding for vSphere .....  | 92 |
| Storage Preparation for vSphere (iSCSI only) .....                             | 92 |
| Enable iSCSI initiator for ESXi hosts .....                                    | 92 |
| Add iSCSI target .....   | 94 |

|   |     |
|---|-----|
| Create an iSCSI datastore.....                      | 95  |
| Multipathing for vSphere (Optional) .....           | 95  |
| Add Hosts or Configure Clusters (vSphere).....      | 96  |
| KVM Installation and Configuration.....             | 97  |
| Supported Operating Systems .....                   | 97  |
| System Requirements for KVM Hosts .....             | 97  |
| KVM Installation Steps .....                        | 98  |
| Installing the CloudStack Agent on a KVM Host ..... | 98  |
| Physical Network Configuration for KVM .....        | 99  |
| Time Synchronization .....                          | 100 |
| Primary Storage Setup for KVM (Optional).....       | 100 |
| Oracle VM (OVM) Installation and Configuration..... | 102 |
| System Requirements for OVM Hosts .....             | 102 |
| OVM Installation Overview .....                     | 102 |
| Installing OVM on the Host(s).....                  | 102 |
| Primary Storage Setup for OVM .....                 | 103 |
| Set Up Host(s) for System VMs .....                 | 103 |
| Choosing a Deployment Architecture.....             | 104 |
| Small-Scale Deployment .....                        | 104 |
| Large-Scale Redundant Setup .....                   | 105 |
| Separate Storage Network.....                       | 106 |
| Multi-Node Management Server.....                   | 106 |
| Multi-Site Deployment.....                          | 107 |
| Choosing a Hypervisor: Supported Features .....     | 111 |
| Network Setup .....                                 | 113 |
| Basic and Advanced Networking .....                 | 113 |
| VLAN Allocation Example.....                        | 114 |

|   |     |
|---|-----|
| Example Hardware Configuration.....                                 | 115 |
| Dell 62xx.....  | 115 |
| Cisco 3750.....   | 115 |
| Layer-2 Switch.....   | 116 |
| Hardware Firewall.....  | 117 |
| Generic Firewall Provisions.....                                    | 117 |
| External Guest Firewall Integration for Juniper SRX (Optional)..... | 117 |
| Management Server Load Balancing .....                              | 120 |
| Topology Requirements.....  | 121 |
| Security Requirements.....  | 121 |
| Runtime Internal Communications Requirements .....                  | 121 |
| Storage Network Topology Requirements.....                          | 121 |
| External Firewall Topology Requirements .....                       | 121 |
| Advanced Zone Topology Requirements .....                           | 121 |
| XenServer Topology Requirements .....                               | 122 |
| VMware Topology Requirements .....                                  | 122 |
| KVM Topology Requirements .....                                     | 122 |
| External Guest Load Balancer Integration (Optional) .....           | 122 |
| Guest Network Usage Integration for Traffic Sentinel .....          | 123 |
| Setting Zone VLAN and Running VM Maximums.....                      | 124 |
| Storage Setup.....  | 125 |
| Small-Scale Setup.....  | 125 |
| Secondary Storage .....   | 125 |
| Example Configurations .....  | 125 |
| Additional Installation Options .....                               | 129 |
| Edit the Global Configuration Settings (Optional) .....             | 129 |
| Installing the Usage Server (Optional) .....                        | 130 |



|  |     |
|--|-----|
| Requirements for Installing the Usage Server ..... | 130 |
| Steps to Install the Usage Server .....            | 131 |
| SSL (Optional).....                                | 131 |
| Database Replication (Optional) .....              | 131 |
| Failover .....                                     | 133 |
| Best Practices.....                                | 134 |
| Process Best Practices.....                        | 134 |
| Setup Best Practices.....                          | 134 |
| Maintenance Best Practices.....                    | 135 |
| Troubleshooting.....                               | 136 |
| Checking the Management Server Log .....           | 136 |
| Troubleshooting the Secondary Storage VM .....     | 136 |
| Running a Diagnostic Script .....                  | 136 |
| Checking the Log Files.....                        | 137 |
| VLAN Issues.....                                   | 137 |
| Console Proxy VM Issues .....                      | 137 |
| Binary Logging Error when Upgrading Database ..... | 138 |
| Can't Add Host .....                               | 138 |
| Preparation Checklists .....                       | 139 |
| Management Server Checklist .....                  | 139 |
| Database Checklist .....                           | 140 |
| Storage Checklist.....                             | 141 |
| Contacting Support .....                           | 142 |

## What's In This Guide

---

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

With the procedures in this Advanced Installation Guide, you can start using the more powerful features of CloudStack, 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 CloudStack?

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

Typical users are service providers and enterprises. With CloudStack, 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 CloudStack an enterprise can offer self-service virtual machines to users without involving IT departments.

## Who Should Read This

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

If you just want to get started, you can skip to Overview of Installation Steps on page 16.



# What Can CloudStack Do?

---

## Multiple Hypervisor Support

CloudStack 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. CloudStack 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

CloudStack 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

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

CloudStack 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

CloudStack 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

CloudStack 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://docs.cloud.com/CloudStack\\_Documentation](http://docs.cloud.com/CloudStack_Documentation).

The CloudStack 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.cloud.com/CloudStack\\_Documentation/Allocator\\_Implementation\\_Guide](http://docs.cloud.com/CloudStack_Documentation/Allocator_Implementation_Guide)).

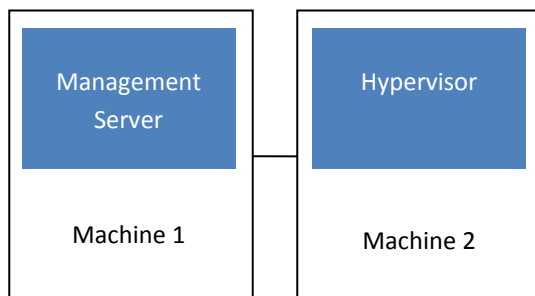
## High Availability

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

## Deployment Architecture Overview

A CloudStack installation consists of two parts: the Management Server and the cloud infrastructure that it manages. When you set up and manage a CloudStack 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 CloudStack 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 104.

## Management Server Overview

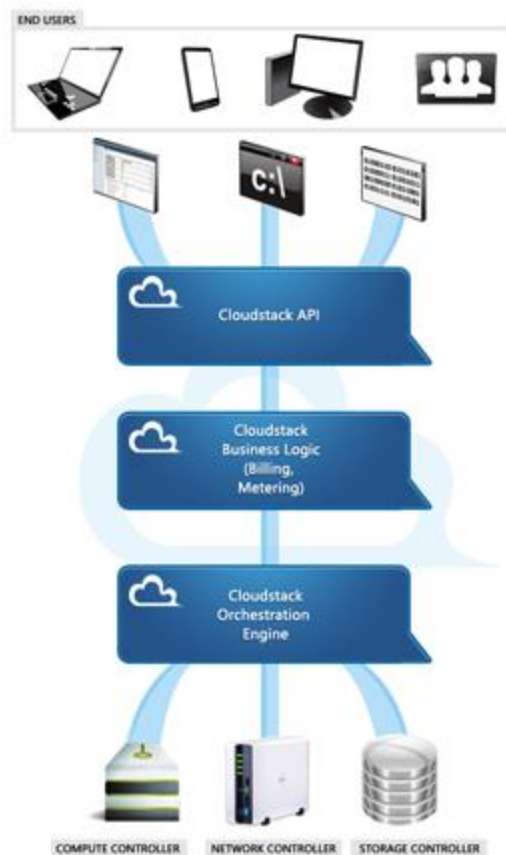
The Management Server is the CloudStack software that manages cloud resources. By interacting with the Management Server through its UI or API, you can configure and manage your cloud infrastructure.

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 CloudStack 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 17.

The Management Server:

- Provides the web user interface for the administrator and a reference user interface for end users.
- Provides the APIs for the CloudStack 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

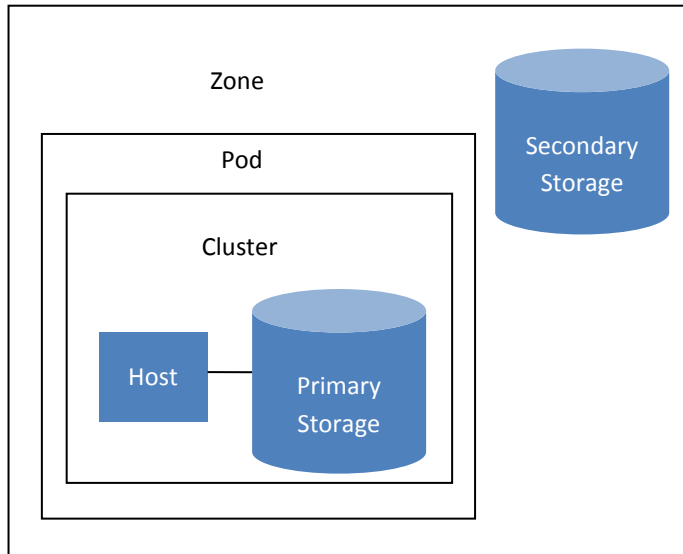
For additional options, including how to set up a multi-node management server installation, see [Choosing a Deployment Architecture](#) on page 104.

## 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 44.
- **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 58.
- **Cluster:** A cluster consists of one or more hosts and primary storage. See [About Clusters](#) on page 60.
- **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 64.
- **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 68.

- **Secondary storage** is associated with a zone, and it stores templates, ISO images, and disk volume snapshots. See About Secondary Storage on page 70.



Nested organization of a zone

## Networking Overview

CloudStack 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 113.

# Overview of Installation Steps

---

## Prepare

1. Make sure you have the required hardware ready (p. 17)
2. (Optional) Fill out the preparation checklists (p. 139)

## Install the CloudStack software

3. Install the CloudStack Management Server (single-node, p. 19, or multi-node, p. 30)
4. Log in to the CloudStack UI (p. 41)

## Provision your cloud infrastructure

5. Add a zone. Includes the first pod, cluster, and host (p. 44)
6. Add more pods (p. 58)
7. Add more clusters (p. 60)
8. Add more hosts (p. 64)
9. Add more primary storage (p. 68)
10. Add more secondary storage (p. 70)

## Try using the cloud

11. Initialization and testing (p. 72)

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 104
- Choosing a Hypervisor: Supported Features on page 111
- Network Setup on page 113
- Storage Setup on page 125
- Best Practices on page 134



# 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:
  - Commercial users: 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/)).
  - Open-source community users: RHEL 5.4-5.x 64-bit or 6.2+ 64-bit; CentOS 5.4-5.x 64-bit or 6.2+ 64-bit; Ubuntu 10.04 LTS
- 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

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, if you are using the KVM hypervisor, 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 CloudStack, the hypervisor host must not have any VMs already running

Hosts have additional requirements depending on the hypervisor. See the requirements listed at the top of the Installation section for your chosen hypervisor:

- Citrix XenServer Installation for CloudStack on page 73
- VMware vSphere Installation and Configuration on page 84
- KVM Installation and Configuration on page 97

## 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 CloudStack. For example, the requirements for XenServer are listed under Citrix XenServer Installation for CloudStack on page 73.

- [Oracle VM \(OVM\) Installation and Configuration on page 102](#)

# 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 17.

If you prefer to set up a Management Server with multiple nodes for high availability, see Management Server Multi-Node Installation on page 30.

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
```

In Ubuntu, SELinux is not installed by default. You can verify this with:

```
# dpkg --get-selections | 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.

In RHEL or CentOS:

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

In Ubuntu (do this step only if SELinux was found on the machine in the previous step):

```
# selinux-config-enforcing permissive
```

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

In CentOS:

```
# setenforce permissive
```

In RHEL:

```
# setenforce 0
```

In Ubuntu (do this step only if SELinux was found on the machine):

```
# setenforce permissive
```

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.

On RHEL or CentOS:

```
# yum install ntp
```

On Ubuntu:

```
# apt-get install ntp
```

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

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

**TIP**

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

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.

On RHEL or CentOS:

```
# chkconfig ntpd on
```

On Ubuntu:

```
# chkconfig ntp on
```

## 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 30.

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

- Open-source community: [http://sourceforge.net/projects/cloudstack/files/CloudStack Acton/](http://sourceforge.net/projects/cloudstack/files/CloudStack%20Acton/)
- Commercial customers: <https://www.citrix.com/English/ss/downloads/>

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

2. Install the CloudStack 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.” Continue to Install and Configure the Database on page 22.

4. (RHEL or CentOS) 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 22.

## 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 CloudStack 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 CloudStack.

2. On the same computer where you installed the CloudStack 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.

On RHEL or CentOS:

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

On Ubuntu, use the following. Replace the password with the root password you set during MySQL installation.

```
# service mysql restart
# mysql -u root -p<password>
```

6. (RHEL or CentOS) 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.

On RHEL or CentOS:

```
# service mysqld restart
```

On Ubuntu:

```
# service mysql 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 CloudStack 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 CloudStack 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 “CloudStack 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 “CloudStack Management Server setup is done.”

11. Continue to Prepare NFS Shares on page 24.

## Prepare NFS Shares

CloudStack needs a place to keep primary and secondary storage (see Cloud Infrastructure Overview on page 14). Both of these can be NFS shares. This section tells how to set up the NFS shares before adding the storage to CloudStack. 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 68
- About Secondary Storage on page 70

## 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
```

Insert the following line.

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

### WARNING

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



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. If you are using iSCSI for primary storage, continue with Log In to the CloudStack UI on page 41.
7. Continue with Prepare the System VM Template on page 27.

## About Password and Key Encryption

CloudStack 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

CloudStack 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 CloudStack's internal properties files along with the database password. The other encrypted values listed above (SSH keys, etc.) are in the CloudStack internal database.

Of course, the database secret key itself can not be stored in the open – it must be encrypted. How then does CloudStack 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 CloudStack administrator. The CloudStack 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.util.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 CloudStack installation. They are all parameters to the CloudStack 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.

## 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_TCPPORT=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 test to be sure the previous steps have been successful.

- a. Log in to the hypervisor host.
- b. (RHEL or CentOS) 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 27.

## Prepare the System VM Template

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

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 CloudStack 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 35.

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.

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:

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

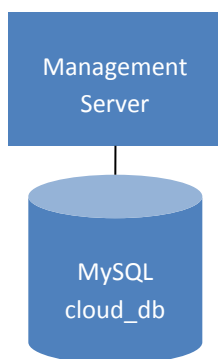
2. When the script has finished, unmount secondary storage and remove the created directory.

```
# 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 CloudStack 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 CloudStack on an ongoing basis. See Log In to the CloudStack UI on page 41.
- When you're ready, add the cloud infrastructure and try running some virtual machines on it, so you can watch how CloudStack manages the infrastructure. See Provision Your Cloud Infrastructure on page 42.

- If desired, you can scale up by adding more Management Server nodes. See Management Server Multi-Node Installation on page 30.

# 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 17.

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
```

In Ubuntu, SELinux is not installed by default. You can verify this with:

```
# dpkg --get-selections | 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.

In RHEL or CentOS:

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

In Ubuntu (do this step only if SELinux was found on the machine in the previous step):

```
# selinux-config-enforcing permissive
```

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

In CentOS:

```
# setenforce permissive
```

In RHEL:

```
# setenforce 0
```

In Ubuntu (do this step only if SELinux was found on the machine):

```
# setenforce permissive
```

4. Make sure that the machine 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.

On RHEL or CentOS:

```
# yum install ntp
```

On Ubuntu:

```
# apt-get install ntp
```

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

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

You can use the NTP servers provided by Citrix:

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

**TIP**

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

- c. Restart the NTP client.

```
# service ntpd restart
```

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

On RHEL or CentOS:

```
# chkconfig ntpd on
```

On Ubuntu:

```
# chkconfig ntp on
```

---

## Install the First Management Server

---

1. Download the CloudStack Management Server onto the host where it will run from one of the following links. If your operating system is CentOS, use the download file for RHEL.
  - Open-source community: [http://sourceforge.net/projects/cloudstack/files/CloudStack Acton/](http://sourceforge.net/projects/cloudstack/files/CloudStack%20Acton/)
  - Commercial customers: <https://www.citrix.com/English/ss/downloads/>You will need a [MyCitrix account](#).

2. Install the CloudStack 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. (RHEL or CentOS) 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 33.



## 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 CloudStack 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 CloudStack.

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.

On RHEL or CentOS:

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

On Ubuntu, use the following. Replace the password with the root password you set during MySQL installation.

```
# service mysql restart
# mysql -u root -p<password>
```

5. (RHEL or CentOS) 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.

On RHEL or CentOS:

```
# service mysqld restart
```

On Ubuntu:

```
# service mysql 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 35.
- (Optional) For `management_server_key`, substitute the default key that is used to encrypt confidential parameters in the CloudStack 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 35.
- (Optional) For `database_key`, substitute the default key that is used to encrypt confidential parameters in the CloudStack database. Default: password. It is highly recommended that you replace this with a more secure value. See About Password and Key Encryption on page 35.

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

**9.** 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 “CloudStack Management Server setup is done.”

**10.** Continue to Prepare NFS Shares on page 35.

## About Password and Key Encryption

CloudStack 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

CloudStack 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 CloudStack's internal properties files along with the database password. The other encrypted values listed above (SSH keys, etc.) are in the CloudStack internal database.

Of course, the database secret key itself can not be stored in the open – it must be encrypted. How then does CloudStack 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 CloudStack administrator. The CloudStack 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 CloudStack installation. They are all parameters to the CloudStack 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

---

CloudStack needs a place to keep primary and secondary storage (see Cloud Infrastructure Overview on page 14). Both of these can be NFS shares. This section tells how to set up the NFS shares before adding the storage to CloudStack. 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 68
- About Secondary Storage on page 70

## 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 38.

## 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. (Ubuntu only) Run the following command to enable essential services.

```
# apt-get install portmap nfs-kernel-server
```

2. 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
```

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

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

Insert the following line.

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

4. Export the `/export` directory.

```
# exportfs -a
```

5. (Not applicable on Ubuntu) Edit the `/etc/sysconfig/nfs` file and uncomment the following lines.

```
LOCKD_TCPPORT=32803
LOCKD_UDPPORT=32769
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=662
STATD_OUTGOING_PORT=2020
```

6. (Not applicable on Ubuntu) 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
```

7. (Not applicable on Ubuntu) Run the following commands:

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

8. 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
```

9. Reboot the Management Server host.

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

10. (Ubuntu) Restart essential services.

```
# service portmap restart
# service nfs-kernel-server restart
```

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

- a. Log in to the hypervisor host.
- b. (Not applicable on Ubuntu) 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
```

**12.** Continue with Prepare and Start Additional Management Servers on page 38.

## Prepare and Start Additional Management Servers

For your second and subsequent Management Servers, you will install CloudStack, 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 30.
2. Run these commands on each additional Management Server. 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.

3. Choose “M” to install the Management Server.
4. (RHEL or CentOS) 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. 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>
```

6. Configure the OS and start the Management Server:

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

The Management Server on this node should now be running.

7. Be sure to configure a load balancer for the Management Servers. See Management Server Load Balancing on page 120.
8. Continue with Prepare the System VM Template on page 39.

## Prepare the System VM Template

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

1. On the Management Server, run one or more of the following `cloud-install-sys-templ` 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 CloudStack 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 35.

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:

```
# /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-templ -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-templ -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-templ -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.

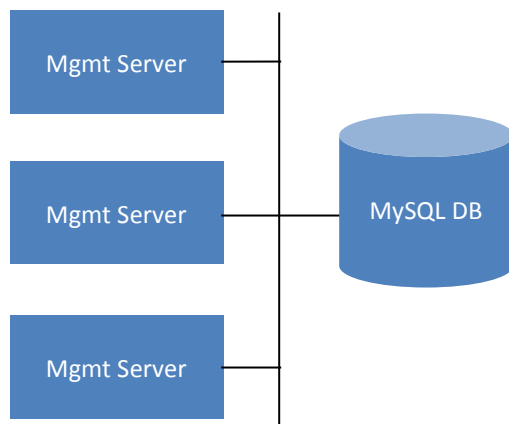
```
# umount /mnt/secondary
# rmdir /mnt/secondary
```

3. Repeat these steps for each secondary storage server.

## Multi-Node Installation Complete! Next Steps

---

Congratulations! You have now installed CloudStack 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 CloudStack on an ongoing basis. See [Log In to the CloudStack UI](#) on page 41.
- When you're ready, add the cloud infrastructure and try running some virtual machines on it, so you can watch how CloudStack manages the infrastructure. See [Provision Your Cloud Infrastructure](#) on page 42.



# Log In to the CloudStack UI

---

After the Management Server software is installed and running, you can run the CloudStack 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 CloudStack, and you want a guided walkthrough of the simplest possible configuration so that you can get started using CloudStack right away. We'll help you set up a cloud with the following features: a single machine that runs CloudStack 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 CloudStack Basic Installation Guide.

- **I have used CloudStack before.** Choose this if you have already gone through a design phase and planned a more sophisticated CloudStack 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 CloudStack, 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 43.

You are logging in as the root administrator. This account manages the CloudStack 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.

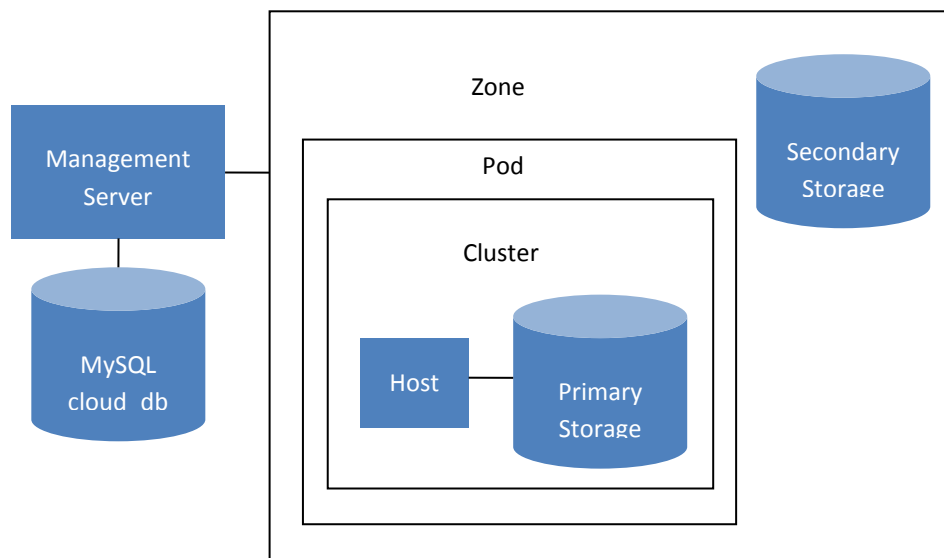
# Provision Your Cloud Infrastructure

After the Management Server is installed and running, you can add the compute resources for it to manage. For an overview of how a CloudStack cloud infrastructure is organized, see [Cloud Infrastructure Overview](#) on page 14.

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

1. Change the Root Password on page 43
2. Add a Zone on page 44
3. Add More Pods (Optional) on page 58
4. Add More Cluster on page 60
5. Add More Hosts (Optional) on page 64
6. Add Primary Storage on page 68
7. Add Secondary Storage on page 70
8. Initialization and Testing on page 72

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 CloudStack installation, you are logging in as the root administrator. This account manages the CloudStack 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 CloudStack 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.

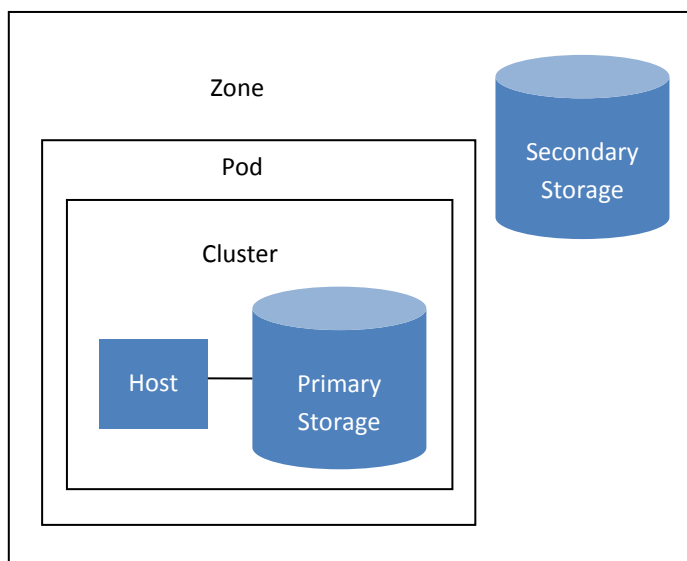
# Add a Zone

## About Zones

A zone is the largest organizational unit within a CloudStack 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.

### 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 CloudStack's internal resources communicate with each other, they generate management traffic. This includes communication between hosts, system VMs (VMs used by CloudStack to perform various tasks in the cloud), and any other component that communicates directly with the CloudStack 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. CloudStack 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 CloudStack 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. CloudStack 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, CloudStack 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 CloudStack 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 CloudStack account's network (potentially a large number of VLANs). In a shared guest network, all guest VMs share a single network.
- **Management.** When CloudStack's internal resources communicate with each other, they generate management traffic. This includes communication between hosts, system VMs (VMs used by CloudStack to perform various tasks in the cloud), and any other component that communicates directly with the CloudStack 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 CloudStack 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. CloudStack 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

CloudStack provisions one public IP address per account for use as the source NAT IP address. If a Juniper SRX firewall is used, CloudStack 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 CloudStack. 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 CloudStack 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. CloudStack 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 CloudStack.

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 CloudStack 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 CloudStack 3.0.0 - 3.0.3, 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 CloudStack 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 CloudStack 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 49.

### 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 CloudStack UI (see page 41).

1. (Optional) If you are going to use Swift for cloud-wide secondary storage, you need to add it to CloudStack before you add zones.
  - a. Log in to the CloudStack 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 CloudStack 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 113.
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 49
    - Advanced Zone Configuration on page 54

## 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 CloudStack 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 48.)   |
| 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 45. 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.

**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. CloudStack 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 CloudStack 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, CloudStack 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 58.
- 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 CloudStack 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 47.
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 CloudStack 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, CloudStack 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 60.
- 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 CloudStack. See [Add Cluster: vSphere](#) on page 61.

- **Cluster name.** Enter a name for the cluster. This can be text of your choosing and is not used by CloudStack.

- 10.** In a new cluster, CloudStack 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 64.

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 CloudStack and what additional configuration is required to ensure the host will work with CloudStack. To find these installation details, see:

- [Citrix XenServer Installation for CloudStack](#) on page 73
- [VMware vSphere Installation and Configuration](#) on page 84
- [KVM Installation and Configuration](#) on page 97
- [Oracle VM \(OVM\) Installation and Configuration](#) on page 102

When you deploy CloudStack, 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 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, CloudStack 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 68.

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: <code>iqn.1986-03.com.sun:02:01ec9bb549-1271378984</code></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 CloudStack.</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, CloudStack adds the first secondary storage server for you. For an overview of what secondary storage is, see About Secondary Storage on page 70.

Before you can fill out this screen, you need to prepare the secondary storage by setting up NFS shares and installing the latest CloudStack System VM template. See Adding Secondary Storage on page 70.

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 CloudStack 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 46. 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.

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, CloudStack 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 58.

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 CloudStack 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 47.
7. Specify a range of VLAN IDs to carry guest traffic for each physical network (see VLAN Allocation Example on page 114), then click Next.
  8. In a new pod, CloudStack 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 60.

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 CloudStack. See Add Cluster: vSphere on page 61.
  - **Cluster name.** Enter a name for the cluster. This can be text of your choosing and is not used by CloudStack.
9. In a new cluster, CloudStack 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 64.

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 CloudStack and what additional configuration is required to ensure the host will work with CloudStack. To find these installation details, see:

- Citrix XenServer Installation for CloudStack on page 73
- VMware vSphere Installation and Configuration on page 84
- KVM Installation and Configuration on page 97

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

- Oracle VM (OVM) Installation and Configuration on page 102

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, CloudStack 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 68.

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 CloudStack.</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.<br/><br/>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 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.<br/><br/>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> 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.<br/><br/>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> |

- 11.** In a new zone, CloudStack 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 70.

Before you can fill out this screen, you need to prepare the secondary storage by setting up NFS shares and installing the latest CloudStack System VM template. See Adding Secondary Storage on page 70.

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, CloudStack adds the first pod for you. You can add more pods at any time using the procedure in this section.

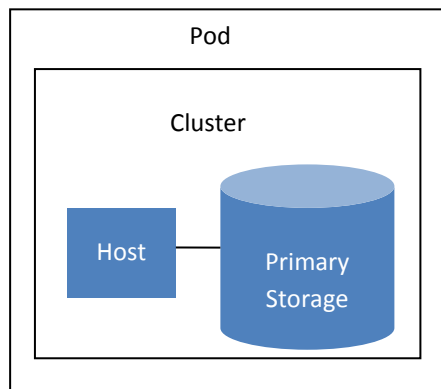
### About Pods

---

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 CloudStack 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 CloudStack UI (see page 41).

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 CloudStack 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 47.
5. Click OK.

## Add More Clusters (Optional)

---

You need to tell CloudStack 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.

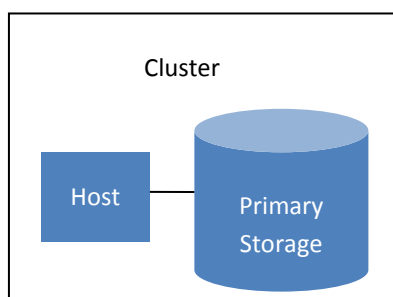
### About Clusters

---

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 CloudStack deployment. Clusters are contained within pods, and pods are contained within zones. Size of the cluster is limited by the underlying hypervisor, although the CloudStack recommends less in most cases; see Best Practices on page 134.

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



**A simple cluster**

CloudStack allows multiple clusters in a cloud deployment.

Every VMware cluster is managed by a vCenter server. Administrator must register the vCenter server with CloudStack. 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 CloudStack on page 73 or KVM Installation and Configuration on page 97 for essential configuration requirements) and logged in to the CloudStack UI (see page 41).

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 CloudStack.
8. Click OK.

## Add Cluster: vSphere

---

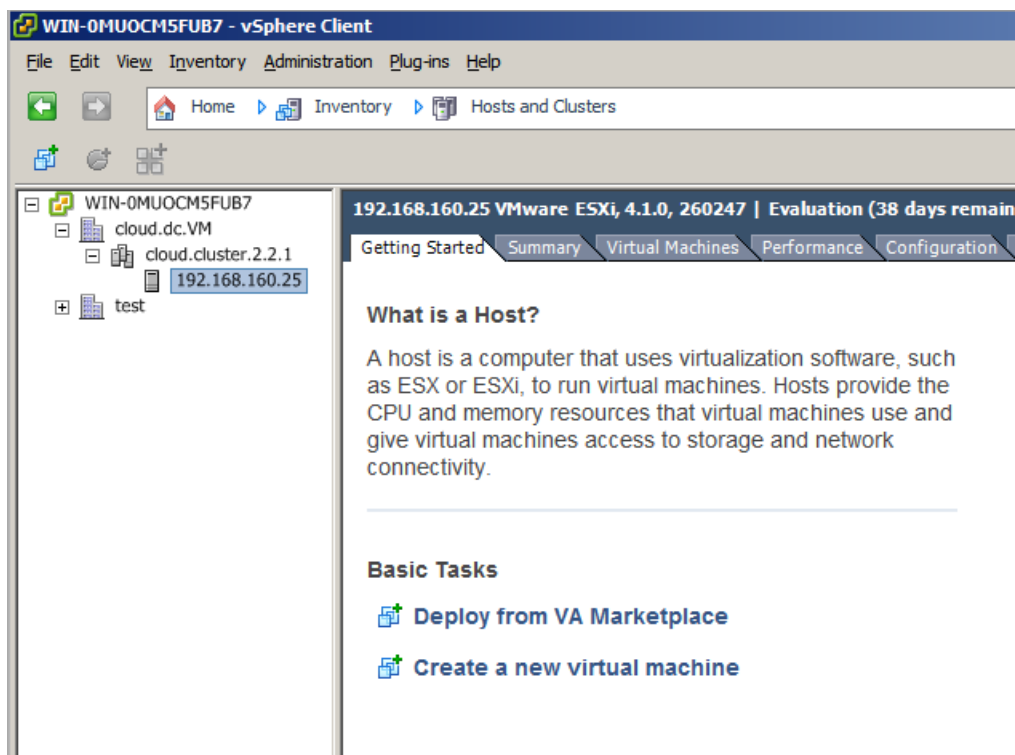
Host management for vSphere is done through a combination of vCenter and the CloudStack admin UI. CloudStack requires that all hosts be in a CloudStack cluster, but the cluster may consist of a single host. As an administrator you must decide if you would like to use clusters of one host or of multiple 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 CloudStack. 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 CloudStack.

To add a vSphere cluster to CloudStack:

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 CloudStack UI (see page 41).
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 CloudStack 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".

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

## 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 CloudStack 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 61. 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 60. 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 More Hosts (Optional)

---

After adding at least one cluster to your CloudStack 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 CloudStack deployment. Hosts are contained within clusters, clusters are contained within pods, and pods are contained within zones.

Hosts in a CloudStack 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.

CloudStack 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 CloudStack, 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 CloudStack Management Server

## Host Allocation

At runtime, when a user creates a new guest VM, the CloudStack platform chooses an available Host to run the new guest VM. The chosen Host will always be close to where the guest's virtual disk image is stored. Both vertical and horizontal allocation is allowed. Vertical allocation consumes all the resources of a given Host before allocating any guests on a second Host. This reduces power consumption in the cloud. Horizontal allocation places a guest on each Host in a round-robin fashion. This may yield better performance to the guests in some cases. The CloudStack platform also allows an element of CPU over-provisioning as configured by the administrator. Over-provisioning allows the administrator to commit more CPU cycles to the allocated guests than are actually available from the hardware.



The CloudStack platform also provides a pluggable interface for adding new allocators. These custom allocators can provide any policy the administrator desires.

## Install Hypervisor Software on Hosts

---

Before adding a host to the CloudStack configuration, you must first install your chosen hypervisor on the host. CloudStack can manage hosts running VMs under a variety of hypervisors. For a comparison of CloudStack supported features for each hypervisor, see [Choosing a Hypervisor: Supported Features](#) on page 111.

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

- [Citrix XenServer Installation for CloudStack](#) on page 73
- [VMware vSphere Installation and Configuration](#) on page 84
- [KVM Installation and Configuration](#) on page 97
- [Oracle VM \(OVM\) Installation and Configuration](#) on page 102

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

## Add Hosts to CloudStack (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 CloudStack.

For hardware requirements, see the appropriate section:

- [Citrix XenServer Installation for CloudStack](#) on page 73
- [KVM Installation and Configuration](#) on page 97
- [Oracle VM \(OVM\) Installation and Configuration](#) on page 102

### 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.

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. 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
```

## 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.

## OVМ Host Additional Requirements

Before adding a used host in CloudStack, 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 CloudStack and what additional configuration is required to ensure the host will work with CloudStack. To find these installation details, see:
  - Citrix XenServer Installation for CloudStack on page 73
  - KVM Installation and Configuration on page 97
2. Log in to the CloudStack UI (see page 41).
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 CloudStack. See Add Cluster: vSphere on page 61.

# 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 CloudStack 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 69.

## 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 CloudStack UI (see page 41).

### WARNING

Be sure there is nothing stored on the server. Adding the server to CloudStack 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 CloudStack.
  - **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. CloudStack 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 CloudStack, 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 CloudStack before you add the local zone secondary storage servers. See Adding a Zone on page 48.

### WARNING

Be sure there is nothing stored on the server. Adding the server to CloudStack 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 24.
3. Make sure you prepared the system VM template during Management Server installation. See [Prepare the System VM Template](#) on page 27.
4. Now that the secondary storage server for per-zone storage is prepared, add it to CloudStack. Secondary storage is added as part of the procedure for adding a new zone. See [Add a Zone](#) on page 44.

# Initialization and Testing

---

After everything is configured, CloudStack 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 CloudStack 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 the Basic Installation, you should 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 CloudStack Installation.

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



# Citrix XenServer Installation for CloudStack

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 81.

## System Requirements for XenServer Hosts

- The host must be certified as compatible with one of the following. See the Citrix Hardware Compatibility Guide: <http://hcl.xensource.com>
  - XenServer 5.6 SP2 or 6.0.2 (for CloudStack 3.0.2 and greater)
  - XenServer 6.0.2 (for CloudStack 3.0.1)
  - XenServer 6.0 (for CloudStack 3.0.0)
- 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. CloudStack 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 CloudStack 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 CloudStack version (see System Requirements for XenServer Hosts on page 73). 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. 74) | Install CSP package (p. 75)  |
| Username and password (p. 74)           | Set up SR if not using NFS, iSCSI, or local disk for primary storage (p. 76) |
| Time synchronization (p. 74)            | iSCSI multipath setup (p. 77)  |
| Licensing (p. 75)                       | Physical networking setup, including NIC bonding (p. 77)                     |

## 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 CloudStack.

## 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
```

You can use the NTP servers provided by Citrix:

```
0.xenserver.pool.ntp.org
1.xenserver.pool.ntp.org
2.xenserver.pool.ntp.org
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 CloudStack XenServer Support Package (CSP)

---

(Optional)

To enable security groups, elastic load balancing, and elastic IP on XenServer, download and install the CloudStack 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 CloudStack 3.0.1 and greater):

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

For XenServer 5.6 SP2 (can be used with CloudStack 3.0.2 and greater):

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

For XenServer 6.0 (used with CloudStack 3.0.0 only):

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

2. Extract the file:

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

3. Run the following script:

```
# xe-install-supplemental-pack xenserver-cloud-supp.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 CloudStack.

---

## Primary Storage Setup for XenServer

---

CloudStack 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=lvmmohba 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 CloudStack later (see Add Primary Storage on page 68). 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 CloudStack later (see Add Primary Storage on page 68). 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 142.

---

## 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.

CloudStack 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 CloudStack. In some simple cases the name labels are not required.

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

CloudStack supports the use of a second NIC (or bonded pair of NICs, described in NIC Bonding for XenServer (Optional) on page 79) 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 19.

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 CloudStack 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)

CloudStack 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 CloudStack is aware of the networks.

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

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 CloudStack.

### 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. CloudStack 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 CloudStack 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. CloudStack 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 CloudStack 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 CloudStack hosts. The actual upgrade is described in XenServer documentation, but there are some additional steps you must perform before and after the upgrade.

The following upgrades are supported:

- XenServer 5.6, 5.6 FP1, or 5.6 SP2 to XenServer 6.0 (for CloudStack 3.0.0) or XenServer 6.0.2 (for CloudStack 3.0.1)

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
```

### Tip

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

- b. 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 CloudStack.

- a. Log in to the CloudStack UI as root.
- b. Navigate to the XenServer cluster, and click Actions – Unmanage.
- c. 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.

- a. 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
```

- b. Reboot the host.
- c. 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 CloudStack.
  - Log in to the CloudStack 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. CloudStack 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 CloudStack Management Server.
- You must re-install VMware ESXi if you are going to re-use a host from a previous install.
- CloudStack 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 CloudStack management network **must not** be configured as a separate virtual network. The CloudStack management network is the same as the vCenter management network, and will inherit its configuration. See Configure vCenter Management Network on page 90.
- CloudStack requires ESXi. ESX is not supported.
- All resources used for CloudStack must be used for CloudStack only. CloudStack cannot share instance of ESXi or storage with other management consoles. Do not share the same storage volumes that will be used by CloudStack with a different set of ESXi servers that are not managed by CloudStack.
- Put all target ESXi hypervisors in a cluster in a separate Datacenter in vCenter.
- The cluster that will be managed by CloudStack should not contain any VMs. Do not run the management server, vCenter or any other VMs on the cluster that is designated for CloudStack use. Create a separate cluster for use of CloudStack 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 19) is a contiguous range of VLANs that will be managed by CloudStack. CloudStack does not support Distributed vSwitches in VMware.

## Preparation Checklist for VMware

---

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

- vCenter Checklist on page 86
- Networking Checklist for VMware on page 86
- In addition to the VMware-specific checklists, you should also see Preparation Checklists on page 139

## 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 CloudStack 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 CloudStack use. These addresses will be used for virtual router on CloudStack 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:

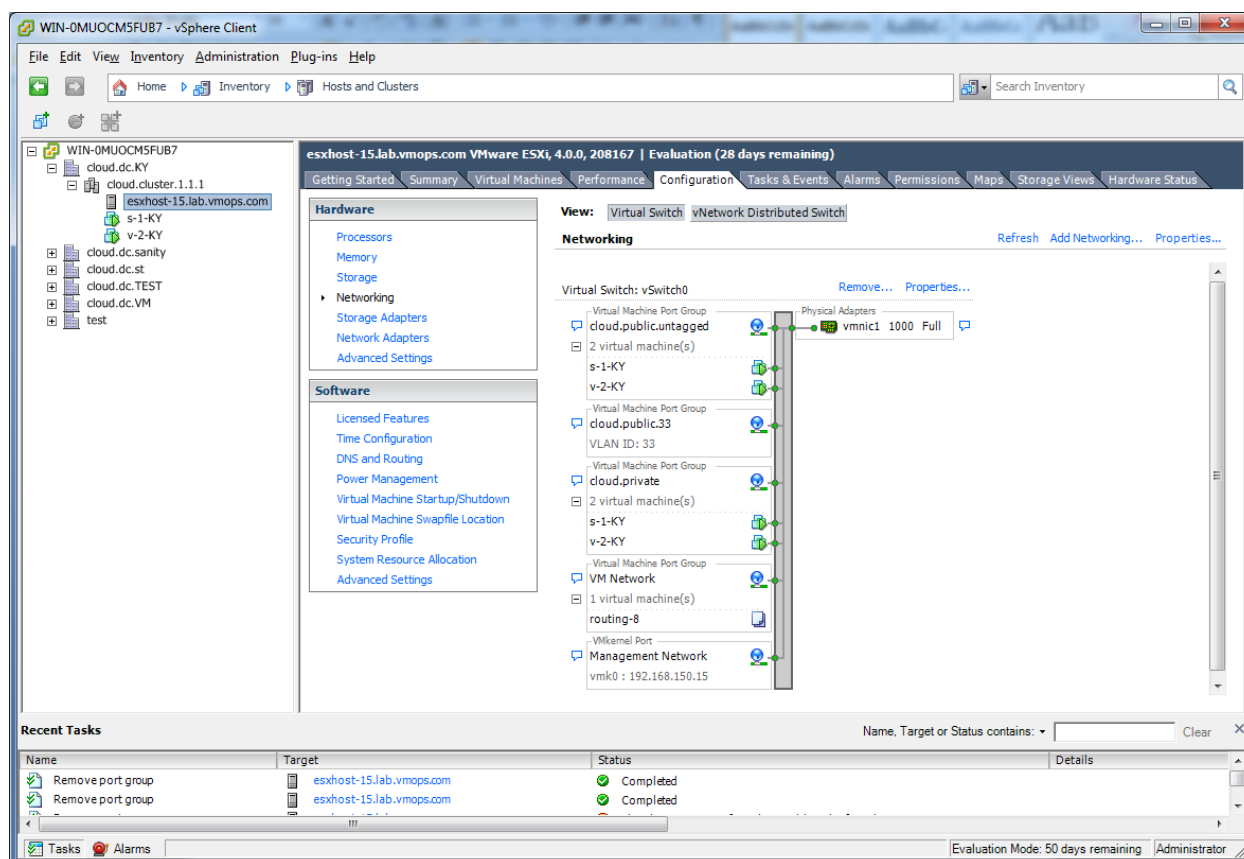
| Required  | Optional          |
|---|-------------------|
| ESXi host setup   | NIC bonding       |
| Configure host physical networking, virtual switch, vCenter Management Network, and extended port range | Multipath storage |
| Prepare storage for iSCSI   |                   |
| Configure clusters 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 CloudStack. 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. CloudStack 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 CloudStack configuration variables as well.



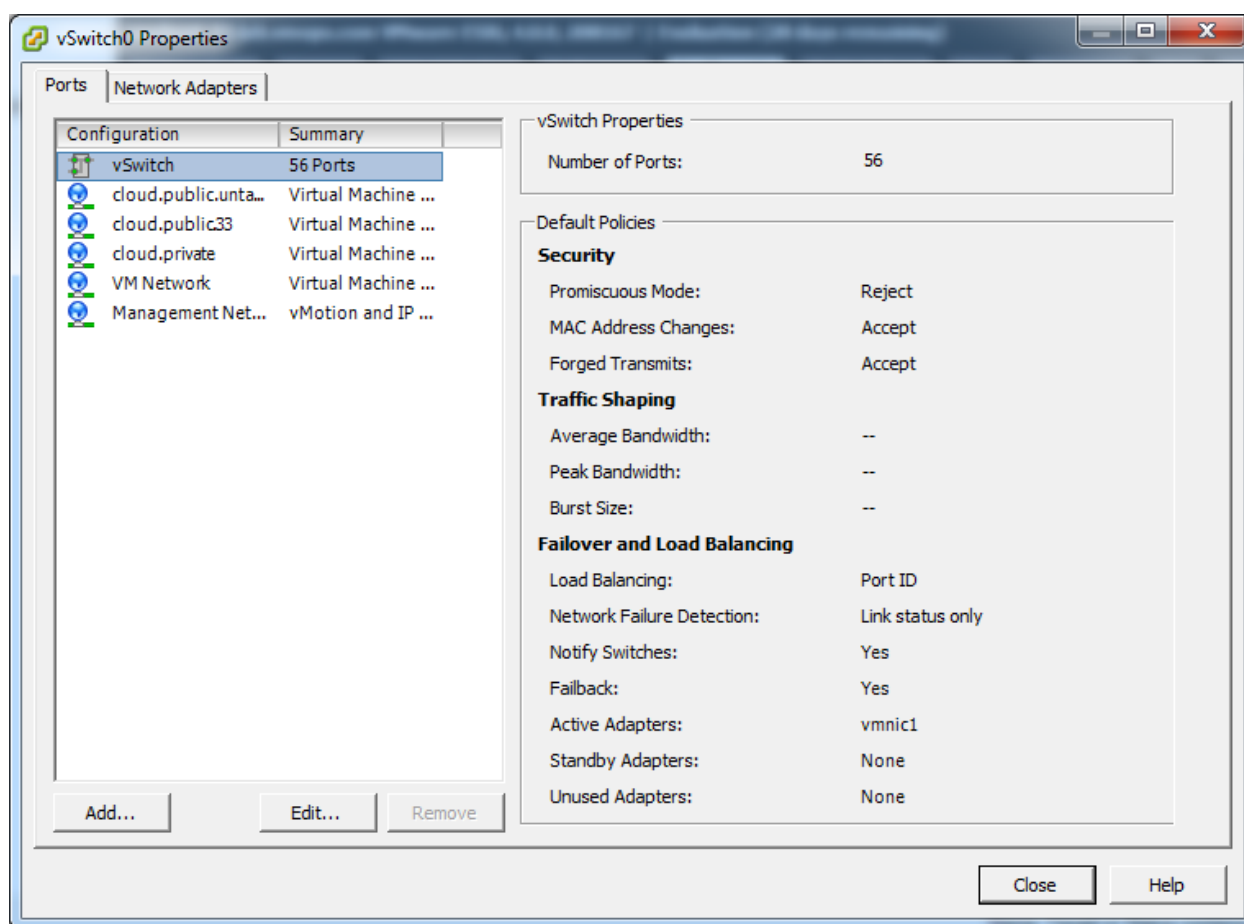
## Separating Traffic

CloudStack 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.

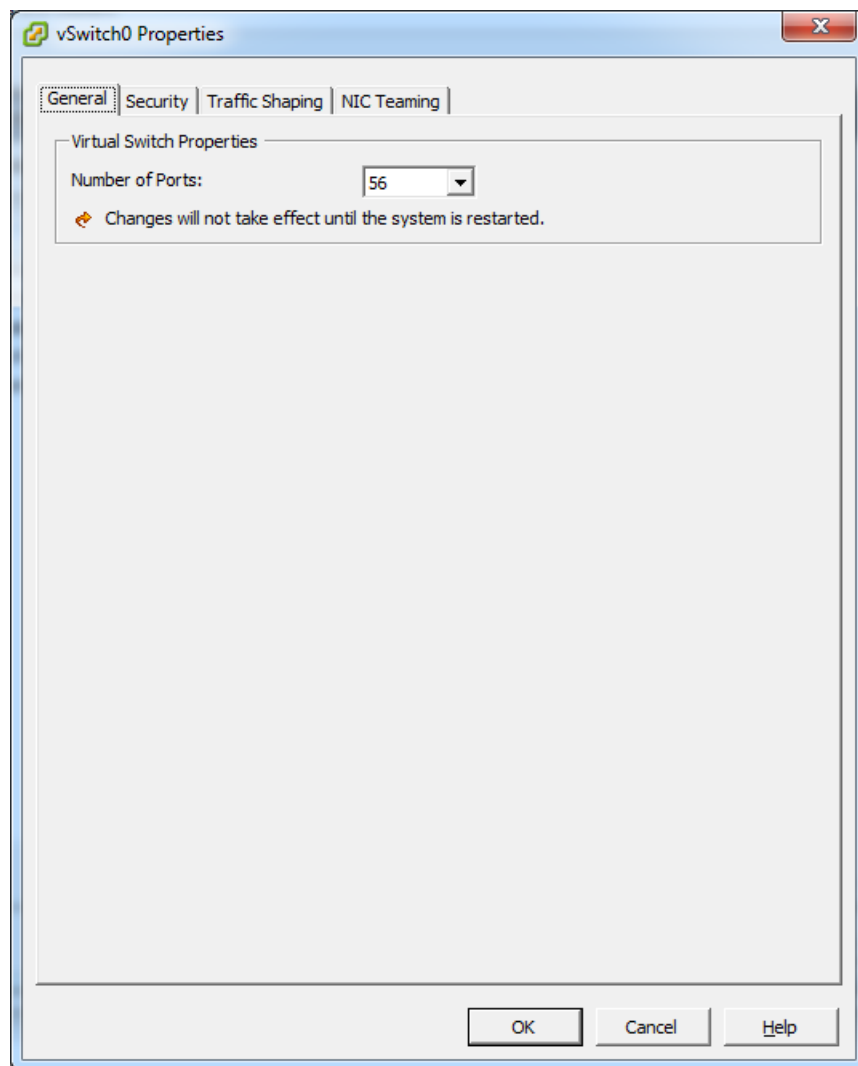
If you want to separate traffic in this way you should first create and configure vSwitches in vCenter according to the vCenter instructions. Take note of the vSwitch names you have used for each traffic type. You will configure CloudStack to use these vSwitches.

## Increasing Ports

By default a virtual switch on ESXi hosts is created with 56 ports. We recommend setting it to 4096, 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).



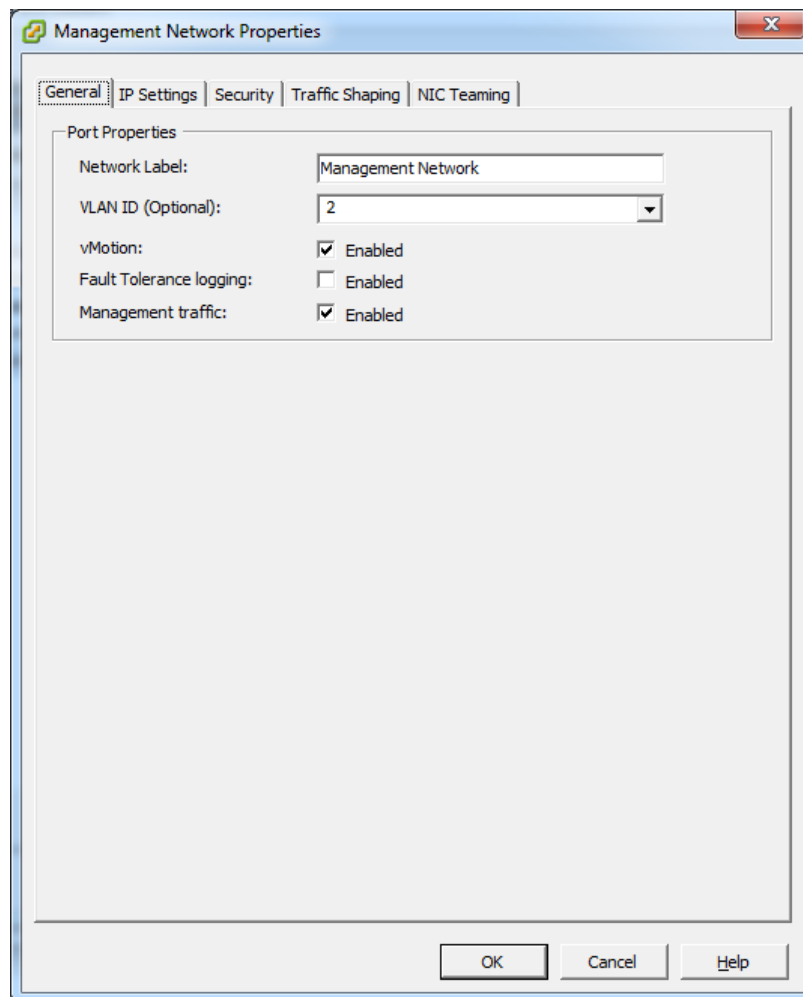
In vSwitch properties dialog, select the vSwitch and click Edit. You should see the following dialog:



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 CloudStack management network. CloudStack 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 CloudStack can find it:

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

## Extend Port Range for CloudStack Console Proxy

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.

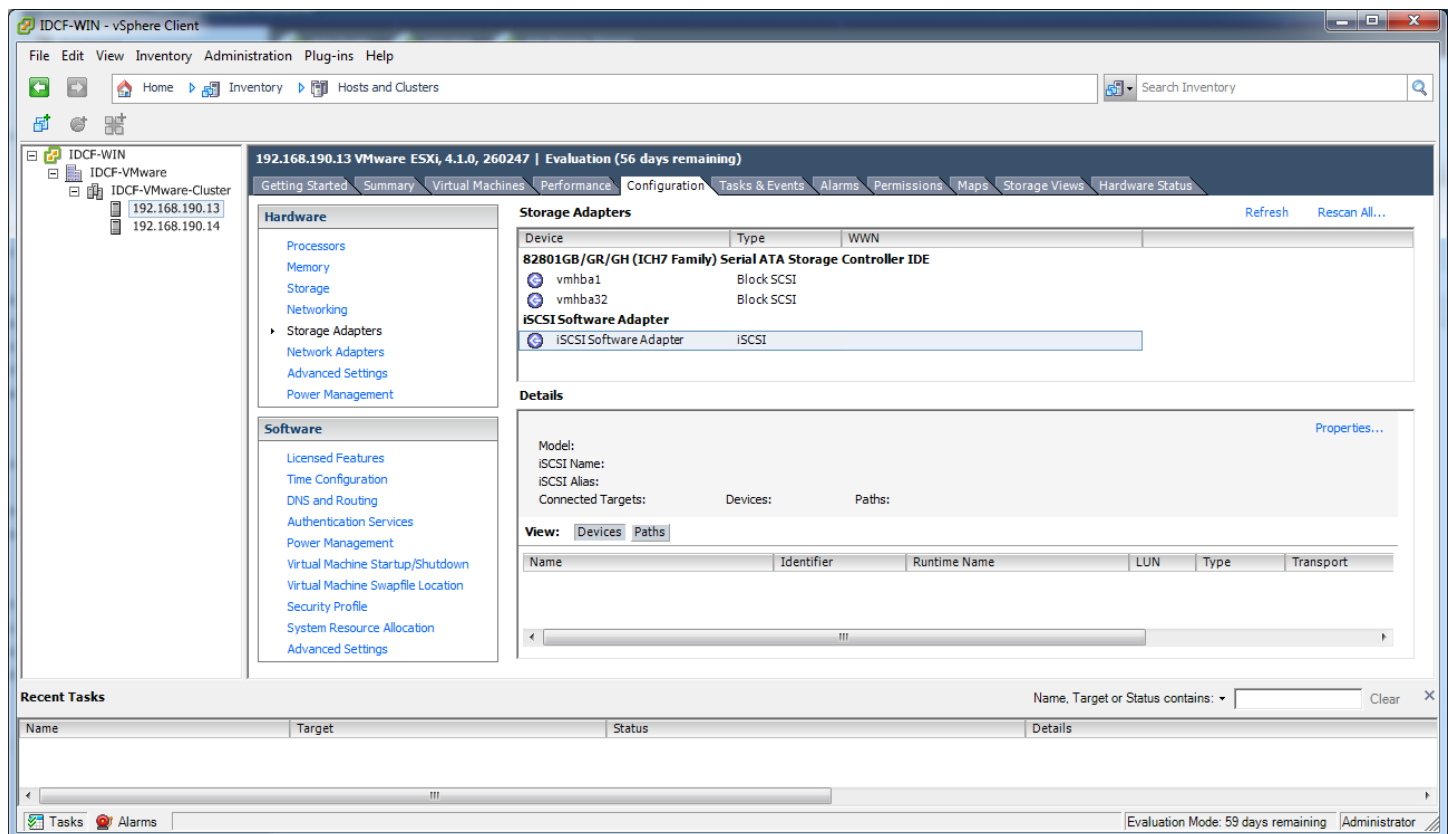
## Storage Preparation for vSphere (iSCSI only)

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

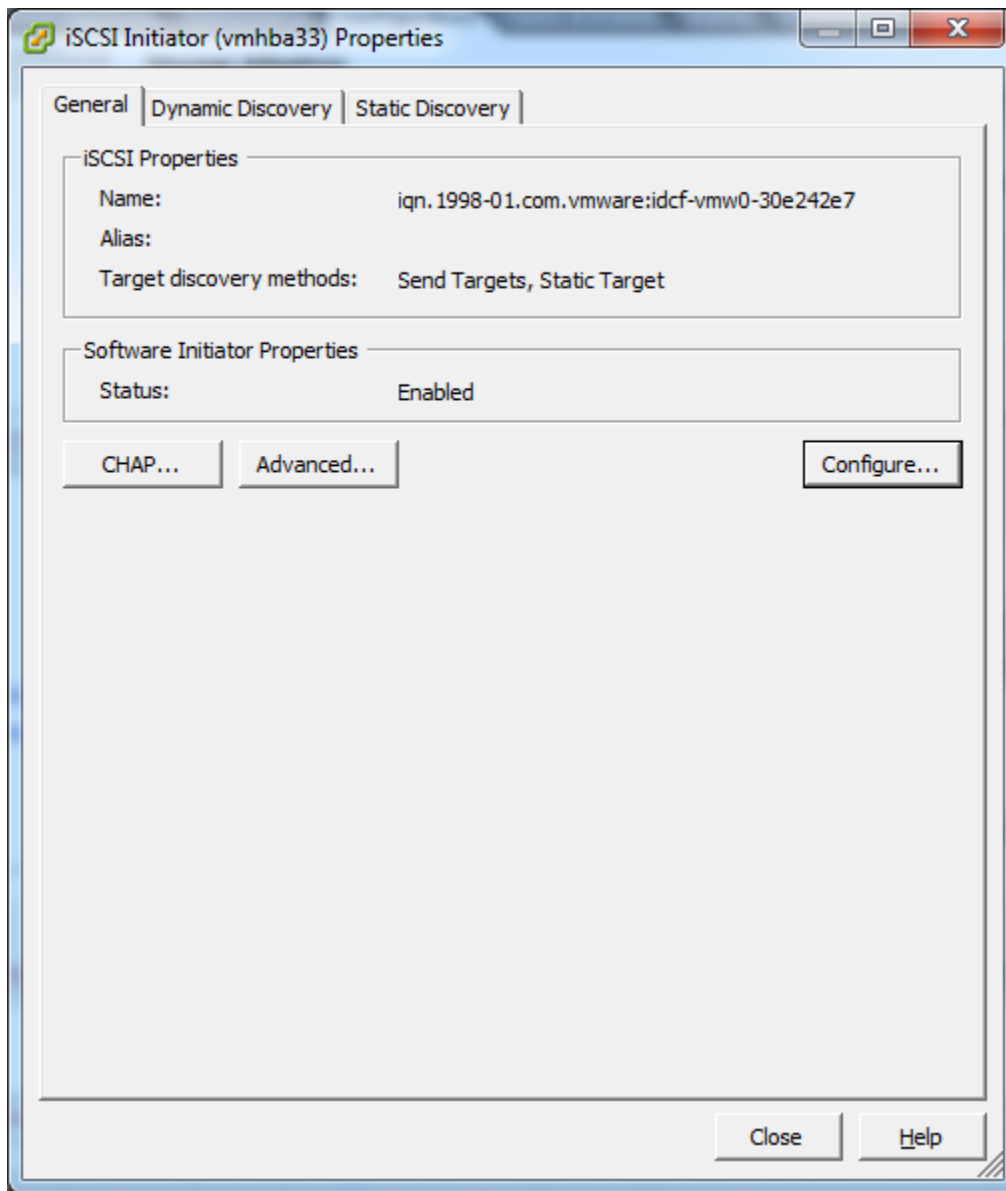
If you are using NFS, skip this section.

## Enable iSCSI initiator for ESXi hosts

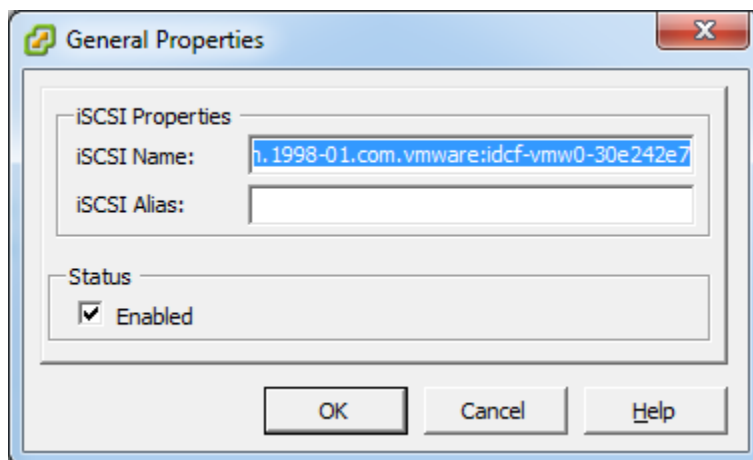
1. In vCenter, go to hosts and Clusters/Configuration, and click Storage Adapters link. You will see:



2. Select iSCSI software adapter and click Properties.



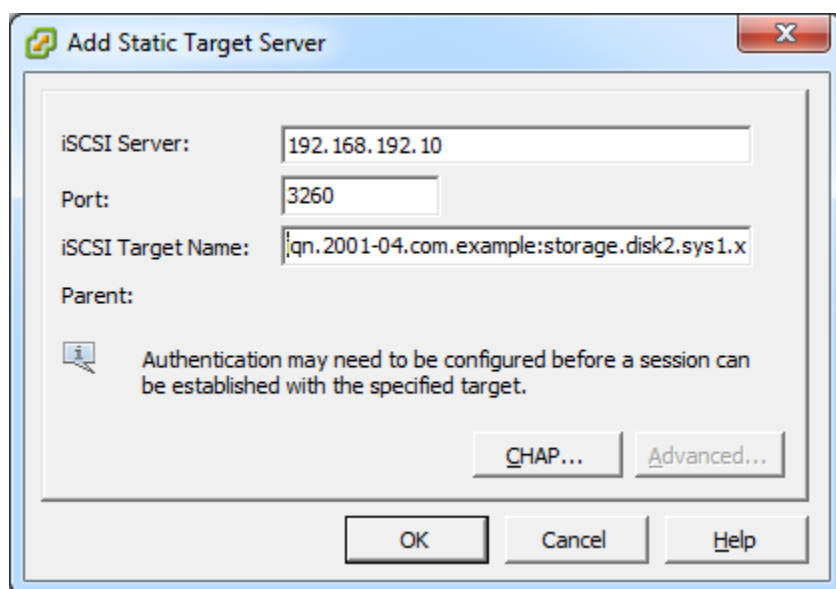
3. Click the Configure... button.



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

## Add iSCSI target

Under the properties dialog, add the iSCSI target info:



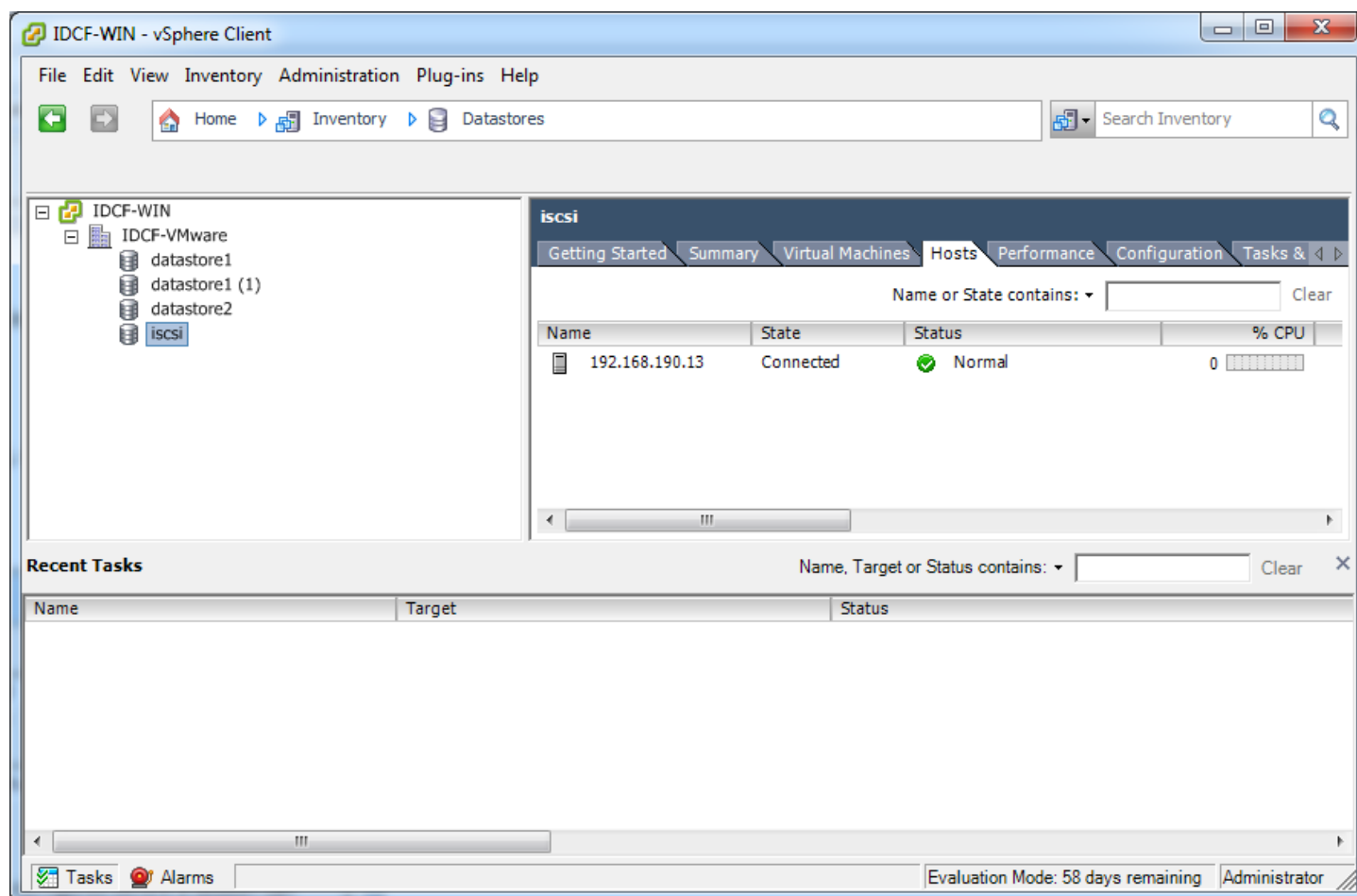
Repeat these steps for all ESXi hosts in the cluster.

## 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 CloudStack. (see Add Cluster: vSphere on page 61).



# 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 CloudStack-specific tweaks.

## Supported Operating Systems

KVM is included with a variety of Linux-based operating systems. Those supported for use with CloudStack 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>

The following are also available for community use. We do not guarantee access to CloudStack support personnel for users of these versions:

- RHEL versions 5.5 – 5.x: <https://access.redhat.com/downloads>
- CentOS versions 5.5 – 5.x: <http://www.centos.org/modules/tinycontent/index.php?id=15>
- CentOS 6.0: <http://www.centos.org/modules/tinycontent/index.php?id=15>
- Ubuntu 10.04: <http://releases.ubuntu.com/lucid/>
- Fedora 16: <https://mirrors.fedoraproject.org/publiclist/Fedora/14/>

## 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

### WARNING

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

as possible after they are released. CloudStack 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.

## KVM Installation Steps

1. Download one of the operating systems that includes KVM (see System Requirements for KVM Hosts on page 97) 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 CloudStack agent on the host (p. 98) | Primary storage setup (p. 100) |
| Physical network configuration (p. 99)           |                                |
| Time synchronization (p. 100)                    |                                |

## Installing the CloudStack Agent on a KVM Host

Each KVM host must have the CloudStack Agent installed on it. Install the CloudStack 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`. CloudStack provides a patched version.

On RHEL:

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

On Ubuntu:

```
# apt-get remove 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 CloudStack 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.

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

```
> A
```

6. (Not applicable to Ubuntu) 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 CloudStack 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, CloudStack will use the device that is used for the default route. This device will be placed in a CloudStack-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.

On RHEL or CentOS:

```
# yum install ntp
```

On Ubuntu:

```
# apt-get install ntp
```

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

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

You can use the NTP servers provided by Citrix:

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

**3.** Restart the NTP client.

On RHEL or CentOS:

```
# service ntpd restart
```

On Ubuntu:

```
# service ntp restart
```

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

On RHEL or CentOS:

```
# chkconfig ntpd on
```

On Ubuntu:

```
# chkconfig ntp on
```

## Primary Storage Setup for KVM (Optional)

---

CloudStack 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 CloudStack 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 CloudStack.

# 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

---

CloudStack 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. CloudStack 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 CloudStack 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 CloudStack 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 CloudStack 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

---

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

4. 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 CloudStack on page 73
  - VMware vSphere Installation and Configuration on page 84
  - KVM Installation and Configuration on page 97
5. 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.

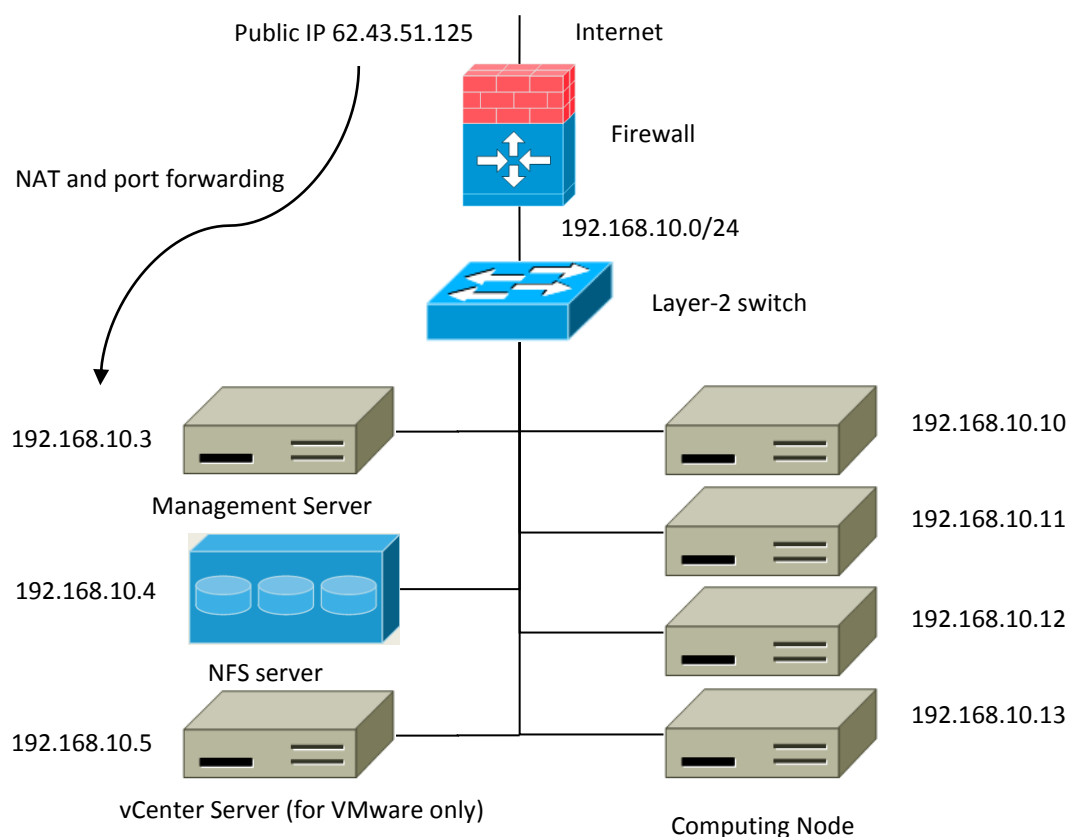
# Choosing a Deployment Architecture

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 a CloudStack work together in different scenarios, this section is for you.

## Small-Scale Deployment



Small-Scale Deployment

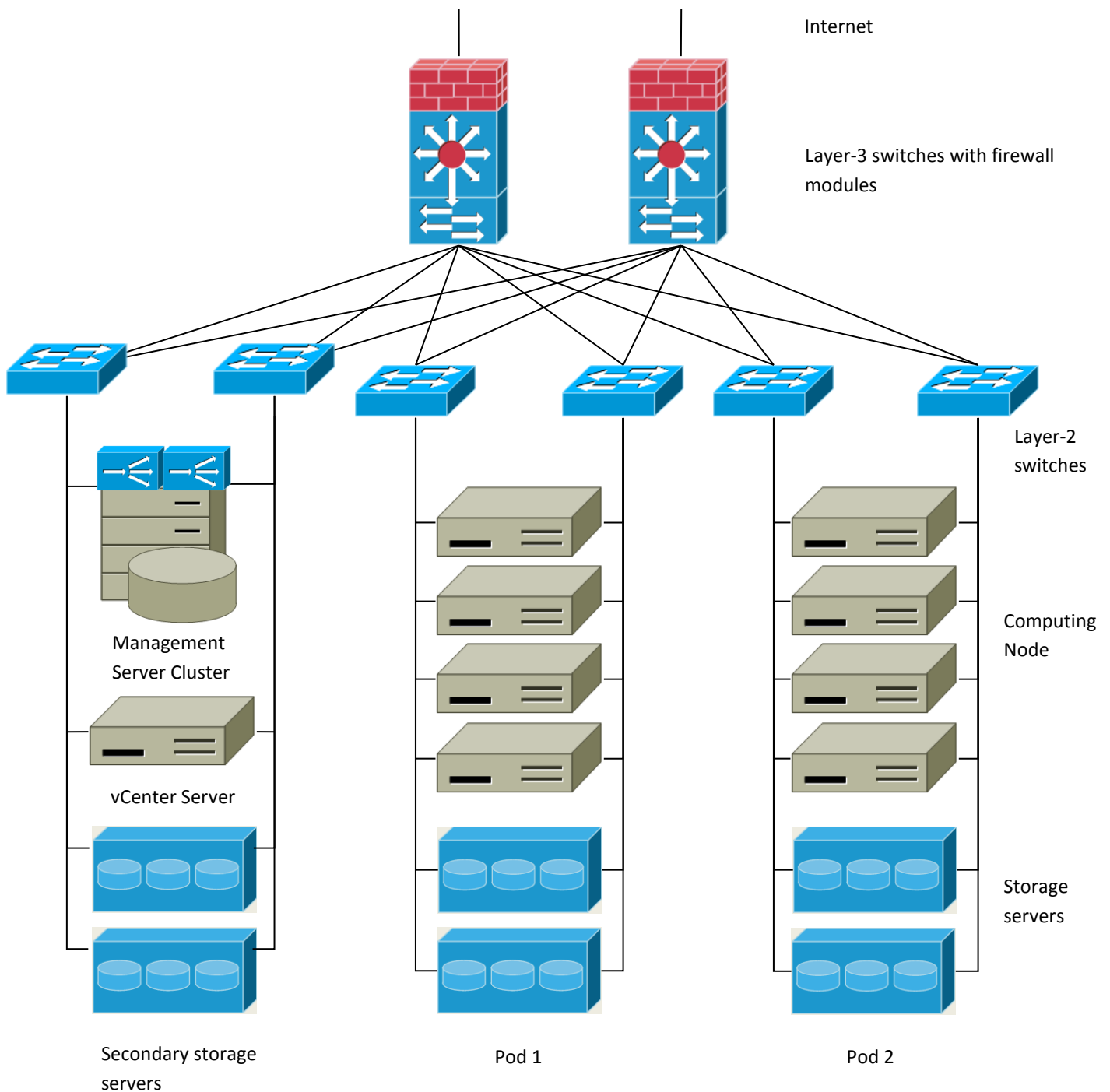
This diagram illustrates the network architecture of a small-scale CloudStack deployment.

- 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 CloudStack 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

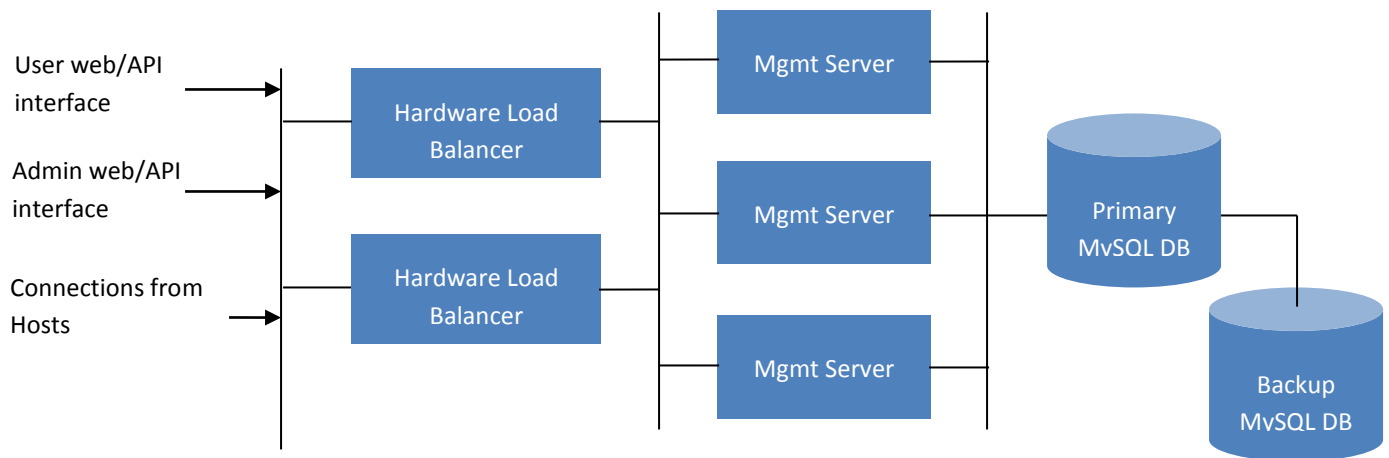
---

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 CloudStack 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.

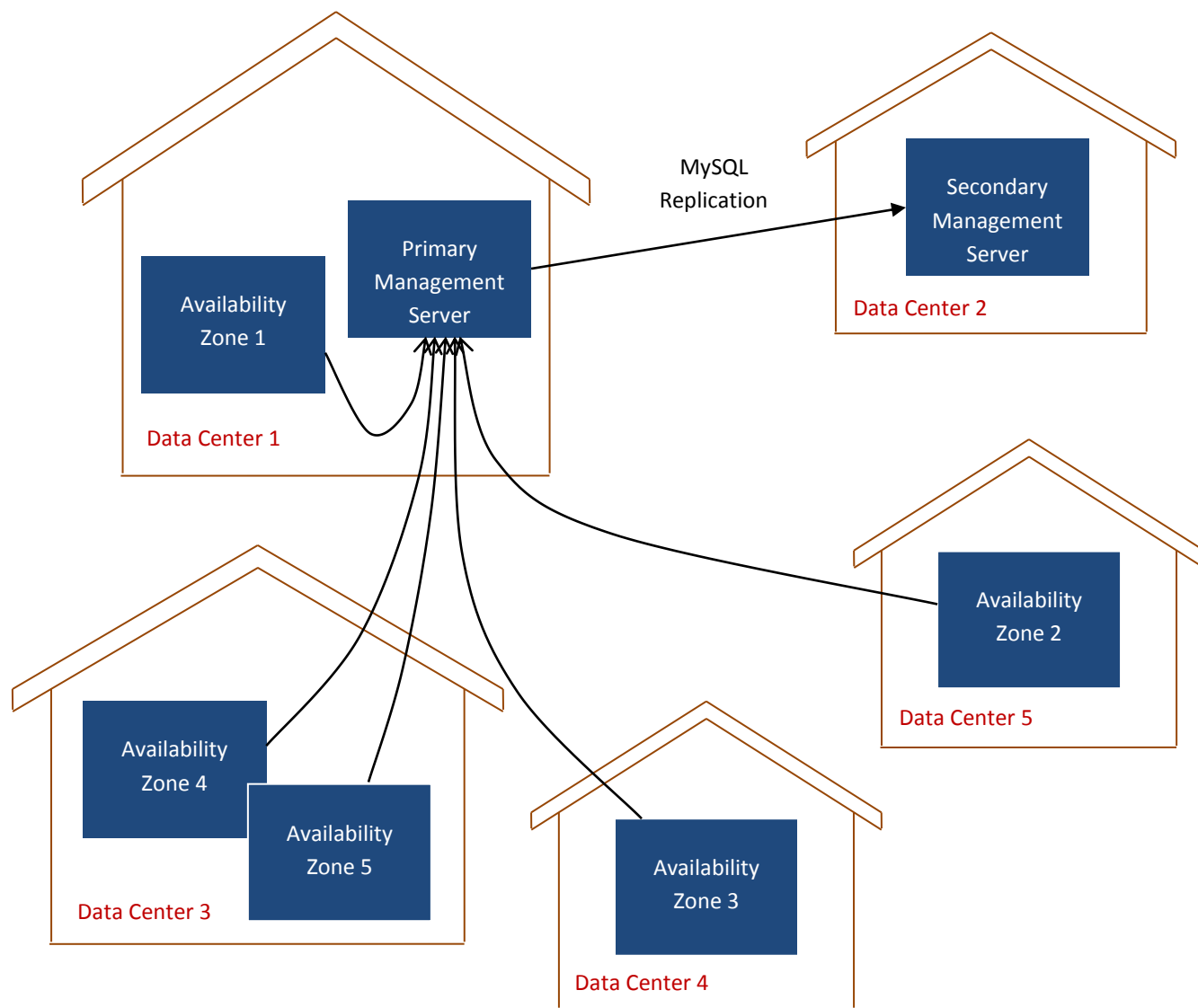


The administrator must decide the following.

- 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.

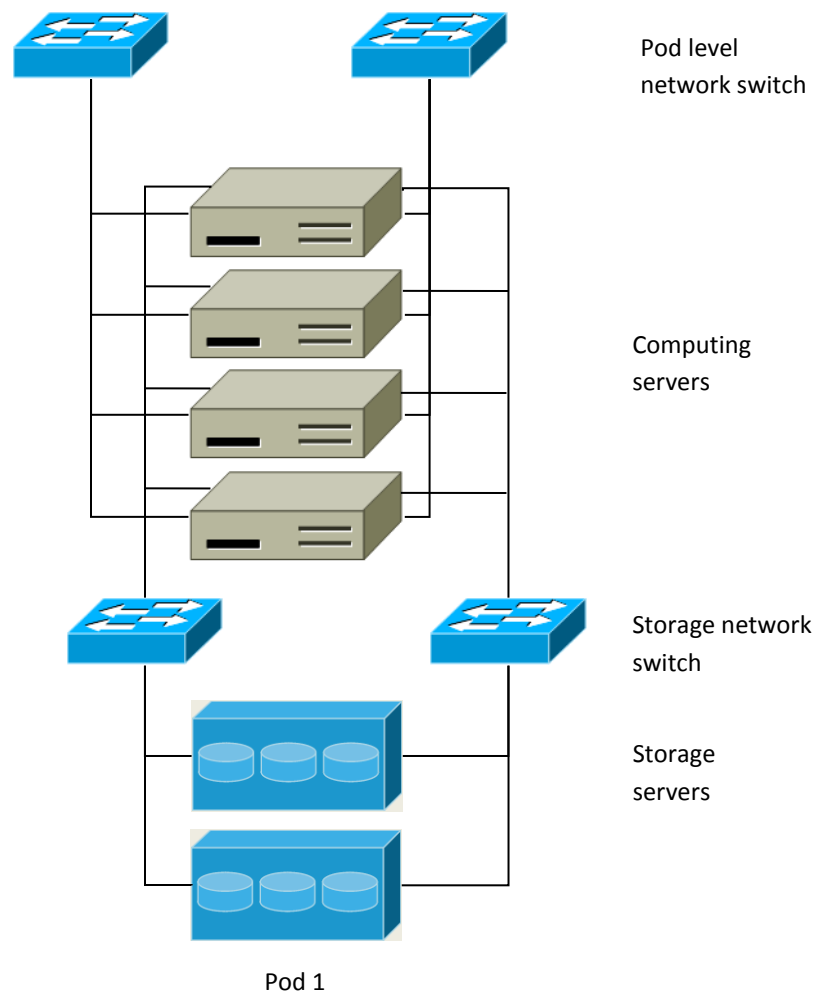
## Multi-Site Deployment

The CloudStack 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.

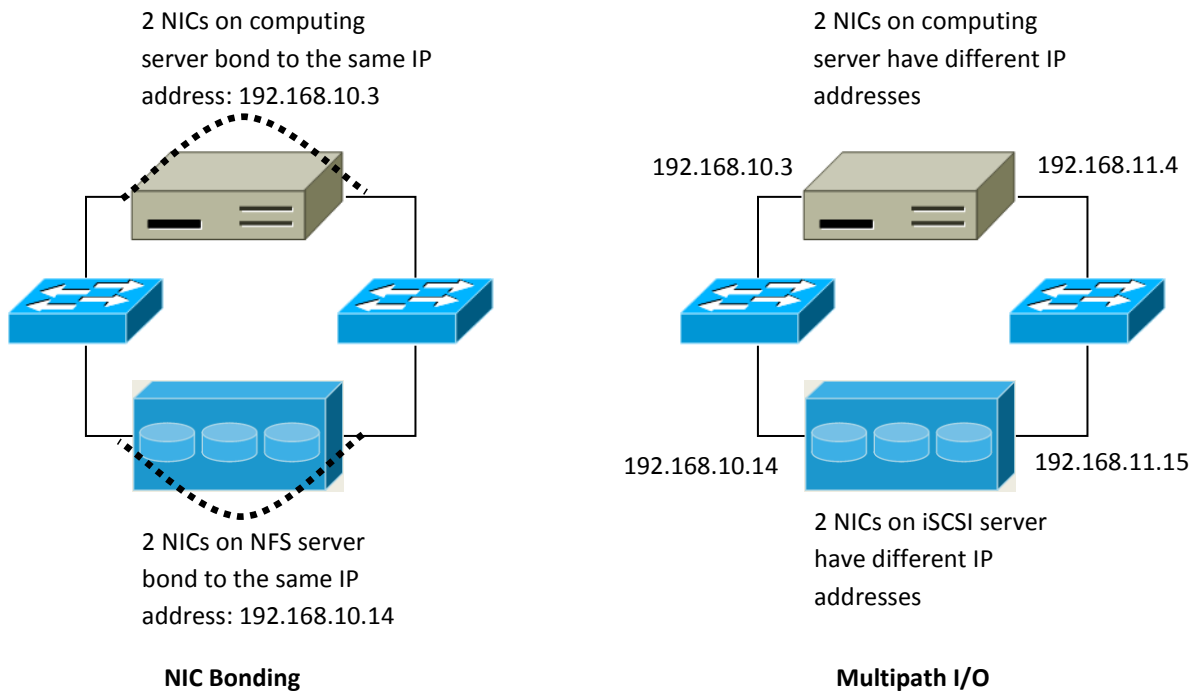


#### Separate Storage Network

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

---

CloudStack 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 CloudStack. 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 CloudStack 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

CloudStack 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 CloudStack, 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 | CloudStack software can access this, hypervisors, system VMs.                                    |
| 500-599  | VLAN carrying public traffic.                            | CloudStack accounts.   |
| 600-799  | VLANs carrying guest traffic:                            | CloudStack accounts. Account-specific VLAN is chosen from this pool.                             |
| 800-899  | VLANs carrying guest traffic                             | CloudStack accounts. Account-specific VLAN chosen by CloudStack admin to assign to that account. |
| 900-999  | VLAN carrying guest traffic                              | CloudStack 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)

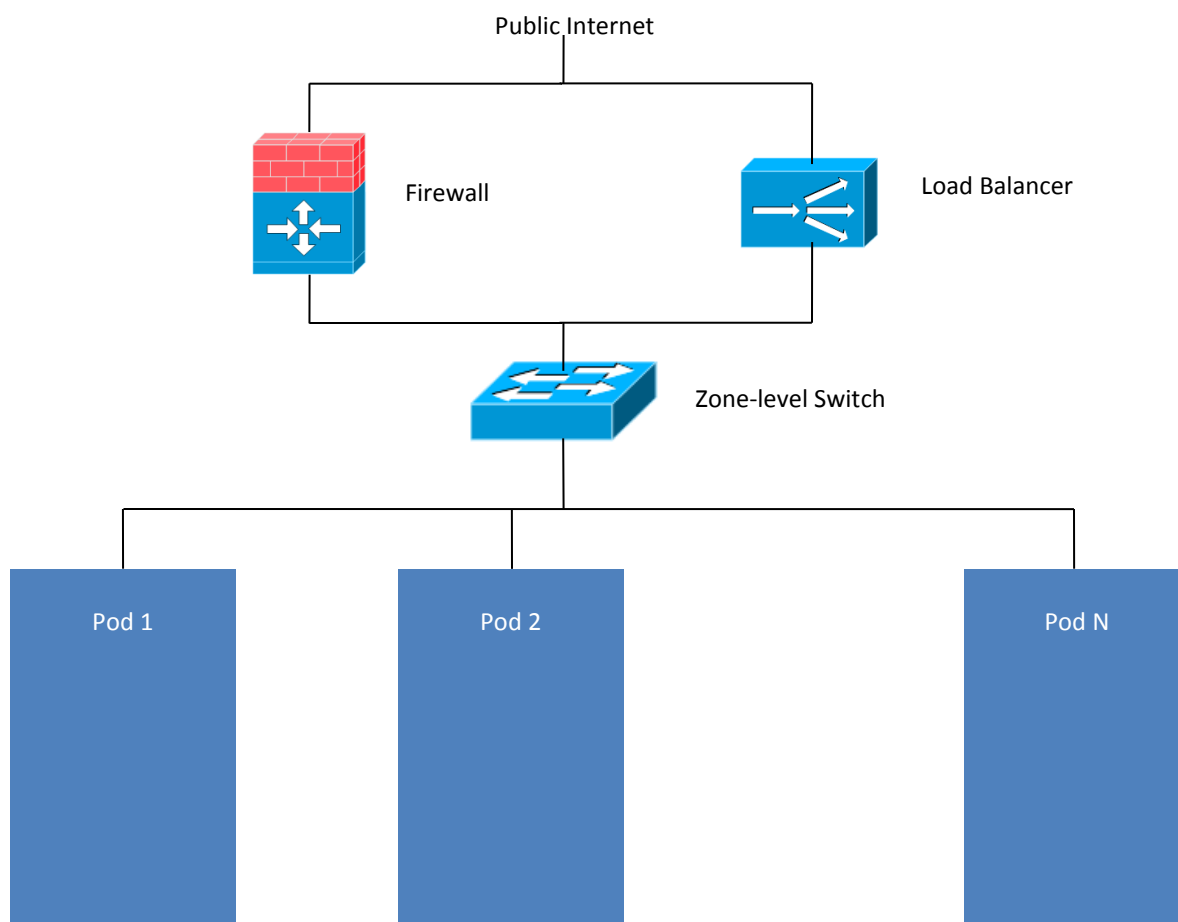
#### Available only for guests using advanced networking

CloudStack provides for direct management of the Juniper SRX series of firewalls. This enables CloudStack 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, CloudStack 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.



CloudStack 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 CloudStack 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 CloudStack 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 CloudStack Management Server is installed, log in to the CloudStack 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 CloudStack 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 CloudStack 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

---

CloudStack 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)

---

CloudStack can optionally use a Citrix NetScaler or BigIP F5 load balancer to provide load balancing services to guests. If this is not enabled, CloudStack will use the software load balancer in the virtual router.

To install and enable an external load balancer for CloudStack 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 CloudStack Management Server is installed, log in as administrator to the CloudStack 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. CloudStack 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 CloudStack 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, CloudStack needs to pull the data from an external network statistics collector installed on the network. Metering statistics for guest networks are available through CloudStack's integration with inMon Traffic Sentinel™.

Traffic Sentinel is a network traffic usage data collection package. CloudStack 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 CloudStack queries the Traffic Sentinel database to obtain this information.

To construct the query, CloudStack 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. CloudStack queries Traffic Sentinel for network statistics that apply to these IPs during the time period they remained allocated in CloudStack. 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 CloudStack. When the Usage Server runs, it collects this data.

To set up the integration between CloudStack 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. CloudStack 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 CloudStack, add the Traffic Sentinel host by calling the CloudStack 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 CloudStack API, see the Developer's Guide at [http://docs.cloud.com/CloudStack\\_Documentation/Developer's\\_Guide%3A\\_CloudStack](http://docs.cloud.com/CloudStack_Documentation/Developer's_Guide%3A_CloudStack).

4. Log in to the CloudStack UI as administrator.
5. Click Configuration – Global Settings. Set the following:
  - `direct.network.stats.interval` – how often you want CloudStack 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 CloudStack 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 CloudStack 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 129 and restart the Management Server.

# Storage Setup

CloudStack 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 CloudStack 3.0.x.

## 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

CloudStack 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 with CloudStack 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_TCP_PORT=32803
LOCKD_UDP_PORT=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 CloudStack features above and beyond the basic deployment options.

## Edit the Global Configuration Settings (Optional)

Once your Management Server is running, you might need to set some global configuration parameters, depending on what optional features you are setting up. The documentation for each CloudStack feature should direct you to the names of the applicable parameters. Many of them are discussed in the CloudStack 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               | <p>For XenServer nodes, this is a true/false variable that instructs CloudStack to enable iSCSI multipath on the XenServer Hosts when they are added. This defaults to false. Set it to true if you would like CloudStack to enable multipath.</p> <p>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.</p>   |
| 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 CloudStack will use storage that is local to the Host for VHDs. By default CloudStack 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 CloudStack 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 CloudStack 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)

---

CloudStack 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 CloudStack to expose HTTP under the assumption that a site will implement its typical practice.

CloudStack uses Tomcat as its servlet container. For sites that would like CloudStack 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)

---

CloudStack 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. Restart the MySQL service:

On RHEL or CentOS:

```
# service mysqld restart
```

On Ubuntu:

```
# service mysql restart
```

3. 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;
```

4. Leave the current MySQL session running.
5. In a new shell start a second MySQL session.
6. 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 |              |                  |
+-----+-----+-----+-----+
```

7. Note the file and the position that are returned by your instance.
8. Exit from this session.
9. Complete the master setup. Returning to your first session on the master, release the locks and exit MySQL.

```
mysql> unlock tables;
```

10. Install and configure the slave. On the slave server, run the following commands.

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

11. 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
```

12. Restart MySQL.

On RHEL or CentOS:

```
# service mysqld restart
```

On Ubuntu:

```
# service mysql restart
```

13. 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;
```

14. Then start replication on the slave.

```
mysql> start slave;
```

15. 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. CloudStack 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
```

# Best Practices

---

Deploying a cloud is challenging. There are many different technology choices to make, and CloudStack 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 CloudStack.
- 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 CloudStack sales team, you can contact your representative to discuss the options for obtaining help and training. CloudStack also offers a variety of ways to submit support requests and get help from fellow users; see [Contacting Support](#) on page 142.

## Setup Best Practices

---

- Each host should be configured to accept connections only from well-known entities such as the CloudStack 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 125 or "Linux NFS on iSCSI" on page 127.
- 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 CloudStack 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 CloudStack 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. CloudStack 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 CloudStack 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 CloudStack 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.

## 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.

On RHEL or CentOS:

```
# service mysqld restart
```

On Ubuntu:

```
# service mysql 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            |  | CloudStack 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                    |  | CloudStack 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

CloudStack 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 CloudStack 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 CloudStack. |

# Contacting Support

---

## Open-source community

A variety of channels are available for getting help with CloudStack, from forums to IRC chat and more. For details, see <http://cloudstack.org/discuss/>.

## Commercial customers

The CloudStack support team is available to help commercial customers plan and execute their installations. To contact the support team, log in to the support portal at <https://na6.salesforce.com/sserv/login.jsp?orgId=00D80000000LWom> using the account credentials you received when you purchased your support contract.