Cloud.com CloudStack Installation Guide

Version 2.2.8

Revised June 27, 2011

Contents

1 Overview

Cloud.com™ CloudStack™ Version 2.2 is designed to work with a wide variety of enterprise-grade and commodity network and storage infrastructure including the following:

- Layer-3 switching at the core and layer-2 switching at the edge. With layer-3 switching at the core, there is no limit on the number of physical servers that can be managed in a cloud.

- 1-GbE and 10-GbE Ethernet NICs and switches

- Redundant network setup with bonded NICs

- NFS and iSCSI storage

CloudStack consists of two types of nodes:

- **CloudStack Management Server**: The server in this node is the resource manager in the system. It controls allocation of virtual machines to servers in the Host and assigns storage and IP addresses to the virtual machine instances.

- **CloudStack Host**: The servers in this node run the virtual machine instances. Servers are grouped into Zones, Pods, and Clusters.

    - **Zone**: A Zone consists of multiple Pods. Typically a Zone is a datacenter.

    - **Pod**: A Pod is usually one rack of hardware and includes one or more clusters, and a layer-2 switch. The Pod is defined by a network subnet.

    - **Cluster**: A Cluster consists of one or more Hosts and Primary Storage.

A small installation may consist of one Management Server and several Hosts. Additional Hosts can be added after the initial installation. The CloudStack Management Server is installed on a RHEL/CentOS 5.4+ system or RHEL6. It can be a VM or a dedicated server.

This guide contains detailed information about the following recommended steps for installing CloudStack.

1. Choose a deployment architecture

2. Set up networking

3. Set up storage

4. Install Citrix XenServer/VMware vSphere/KVM

5. Install the CloudStack Management Server

6. Prepare secondary storage

7. Describe the deployment

8. Test the deployment

2 Prerequisites

CloudStack has the following hardware and software requirements.

	Description	Minimum Requirements
Management Server	Hosts the Cloud.com CloudStack Management Server software.	• 64-bit x86 CPU (more cores results in better performance) • 2 GB of memory • 80 GB of local disk • At least 1 NIC • RHEL/CentOS 5.4+ 64-bit or RHEL6 64-bit • Statically allocated IP address • Fully qualified domain name as returned by the hostname command
Host	Provides all the CPU and memory resource for allocated guest virtual machines.	• 64-bit x86 CPU (more cores results in better performance) • Hardware virtualization support required • 4 GB of memory • 30 GB of local disk • At least 1 NIC • Statically allocated IP Address • Citrix XenServer 5.6, 5.6 FP1, or 5.6 FP2; VMware vSphere 4.1; or RHEL6. **Important: The computing server should be certified as compatible by the hypervisor vendor. You can view the Citrix Hardware Compatibility Guide at** http://hcl.xensource.com/**. You can view the VMware Hardware Compatibility Guide at** http://www.vmware.com/resources/compatibility/search.php**. You can view the RHEL Hardware Compatibility Guide at** https://hardware.redhat.com/**.**
vCenter Server	Run VMware vCenter software	• 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.
Primary Storage	Used for storing the guest VM root disks as well as additional data disk volumes.	• 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. For more information, see Storage Setup on page 29.
Secondary Storage	Provides storage for templates and snapshots	• NFS storage appliance or Linux NFS server • 100GB minimum capacity
Database Node		• May be co-located with the Management Server • Otherwise requirements identical to Management Server

 June 27, 2011

3   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.

3.1   Small-Scale Deployment
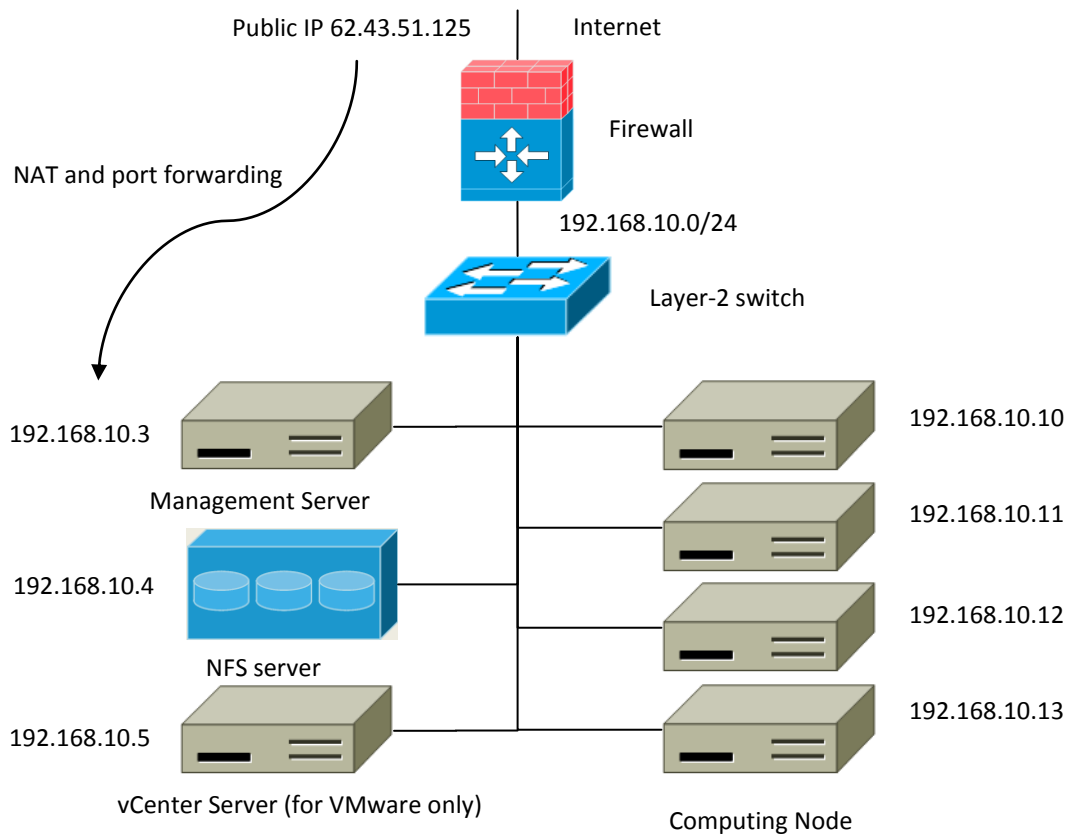
Figure 1 Small-Scale Deployment

Figure 1 illustrates the network architecture of a small-scale Cloud.com CloudStack deployment.

1. 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 private network.

2. A layer-2 switch connects all physical servers and storage.

3. A single NFS server functions as both the primary and secondary storage.

4. The Management Server is connected to the private network.

3.2 Large-Scale Redundant Setup
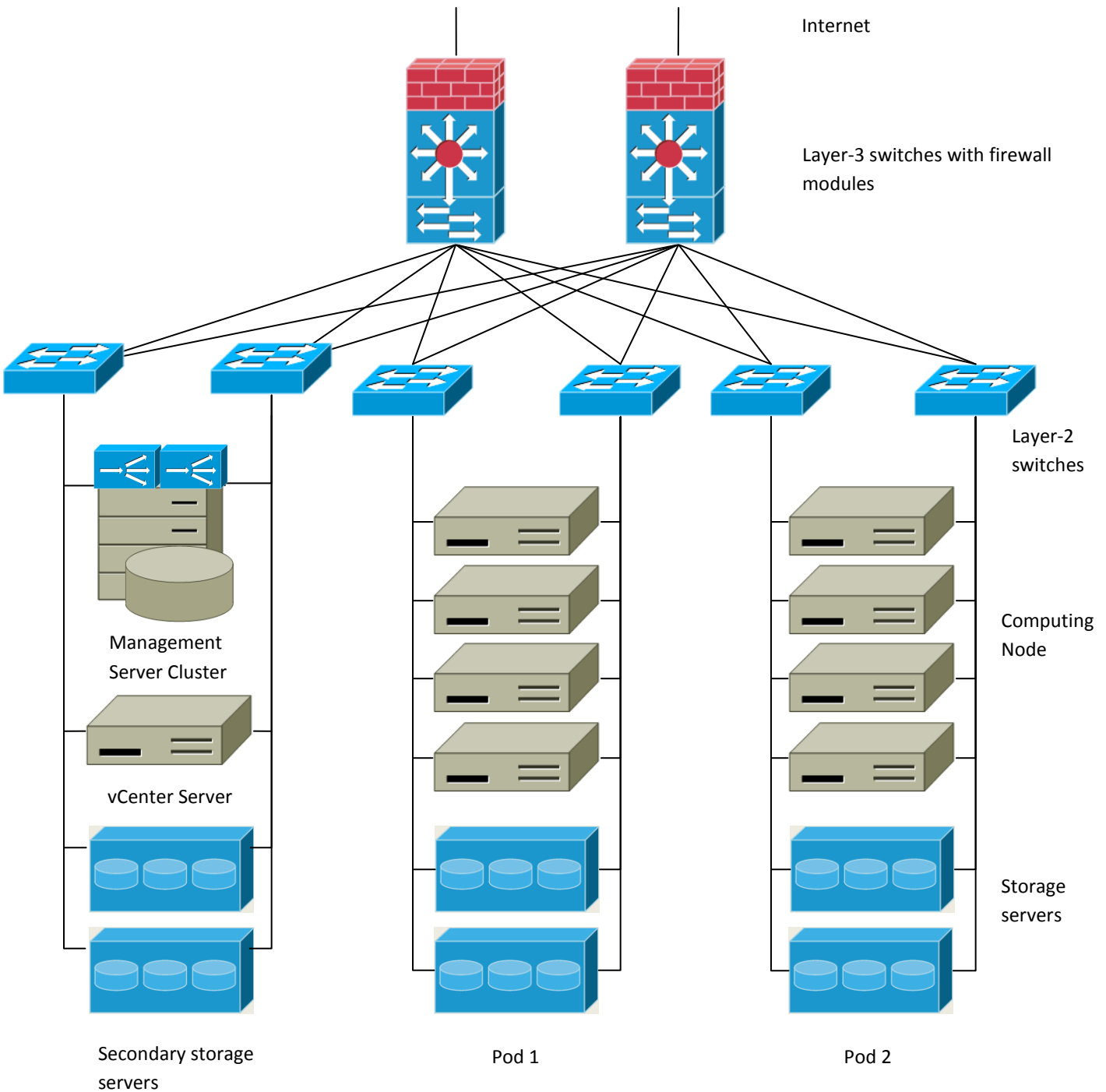
Figure 2 Large-Scale Deployment Architecture

Figure 2 illustrates the network architecture of a large-scale Cloud.com CloudStack deployment.

1. 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:

    a.   Forwards HTTP requests and API calls from the Internet to the Management Server. The Management Server resides on the private network.

    b.   When the cloud spans multiple availability Zones, the firewalls should enable site-to-site VPN such that servers in different availability Zones can directly reach each other.

2.   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.

3.   The Management Server cluster (including front-end load balancers, Management Server nodes, and the MySQL database) is connected to the private network through a pair of load balancers.

4.   Secondary storage servers are connected to the private network.

5.   Each Pod contains storage and computing servers. Each storage and computing server should have redundant NICs connected to separate layer-2 access switches.

3.3 Separate Storage Network

In the Large-Scale Redundant setup described in the previous section, storage traffic can overload the private 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.
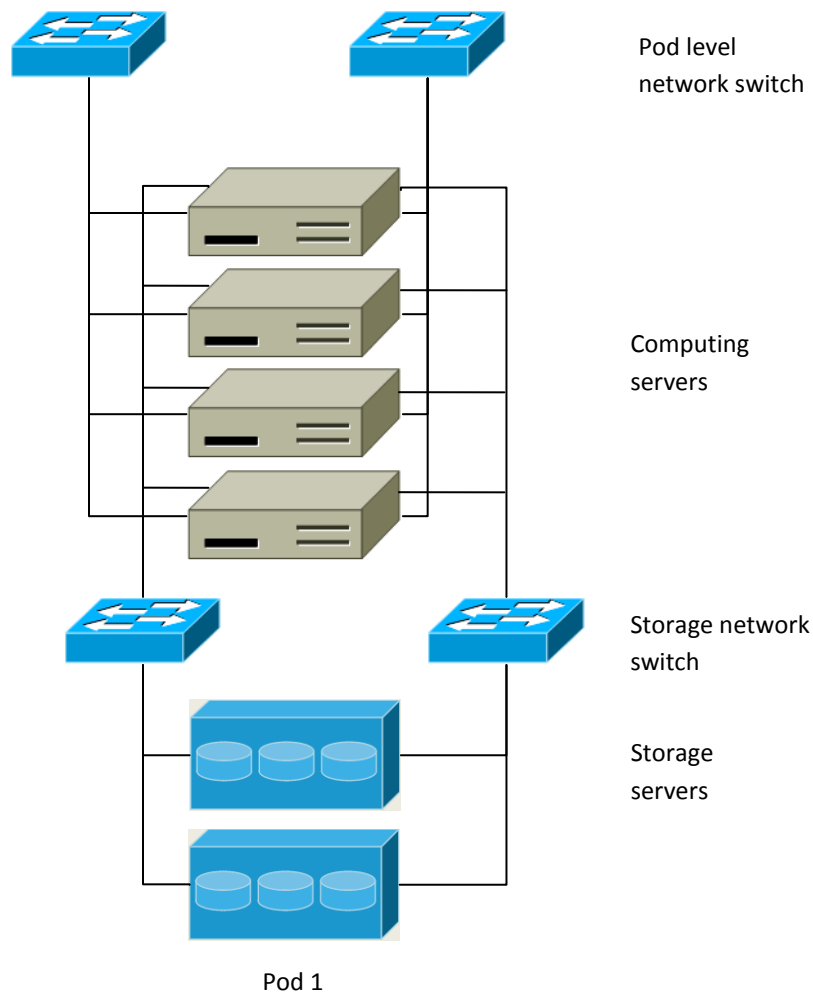
Figure 3 Separate Storage Network

Figure 3 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.

 June 27, 2011

2 NICs on computing
server bond to the same IP
address: 192.168.10.3

2 NICs on computing
server have different IP
addresses

192.168.10.3   192.168.11.4

192.168.10.14   192.168.11.15

2 NICs on NFS server
bond to the same IP
address: 192.168.10.14

2 NICs on iSCSI server
have different IP
addresses

NIC Bonding
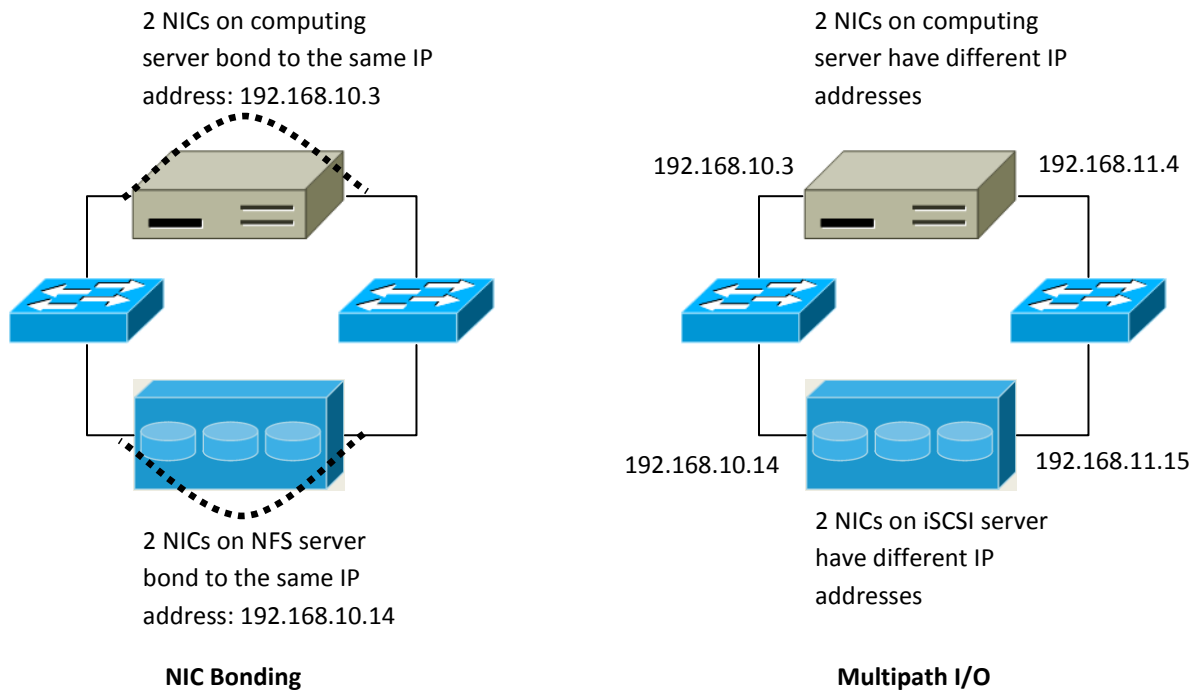
Multipath I/O

Figure 4 NIC Bonding and Multipath I/O

Figure 4 illustrates the differences between NIC bonding and Multipath I/O (MPIO). NIC bonding configuration involves only one network. MPIO involves two separate networks.

3.4 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.

3.4.1 Required Practices

- For XenServer and vSphere, do not put more than 8 hosts in a Cluster. For KVM, do not put more than 16 hosts in a cluster.
- For XenServer, install PV drivers / Xen tools on each template that you create. This will enable live migration and clean guest shutdown.
- For vSphere, install VMware Tools on each template that you create. This will enable console view to work properly.

3.4.2 Suggested Practices

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.

- 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 29 or "Linux NFS on iSCSI" on page 31.

- 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.

- A staging system that models the production environment is strongly advised. It is critical if customizations have been applied to the CloudStack.

- Monitor host disk space. Many host failures occur because the host's root disk fills up from logs that were not rotated adequately.

- Allow adequate time for installation, a beta, and learning the system. Installs with Basic Networking can be done in a day or two. Installs with Advanced Networking usually take several days for the first attempt, with complicated installations taking longer. Allow at least 4-8 weeks for a beta to work through all of the integration issues. It takes months to gain confidence with the CloudStack and related technologies. You may want to contact our sales team about training sessions to help accelerate this.

4 Network Setup

The CloudStack provides two primary networking modes:

- Advanced. Advanced mode uses VLANs for isolation and consists of two types of guest networks:

    o   Virtual networks

    o   Direct attached with tagged VLANs ("Direct tagged")

- Basic. Basic mode does not use VLANs for isolation. It is also known as "Direct Untagged".

The following table highlights the differences between the three types of guest networks.

	Basic	Advanced - Virtual	Advanced - Direct
Uses VLANs for Isolation	No	Yes	Yes
Uses untagged VLAN	Yes	No	No
Uses Security Groups for Isolation	Yes	No	No
Virtual Router is Gateway	No	Yes	No
VPN available	No	Yes	No
Load Balancer available	No	Yes	No
DHCP and DNS available	Yes	Yes	Yes
1:1 NAT available	Coming Soon	Yes	No
Public IP Addresses Required	No	Yes	No
Metering data available	No	Yes	No

The three types of networking may be in use in the same cloud. However, a given Zone must use either Basic Networking or Advanced Networking.

The style of networking that a particular guest receives is determined by a combination of the networks that the administrator has made available and the network that is chosen by the user at guest creation. An administrator configures Basic or Advanced Networking for a Zone. In Advanced networking, the administrator can add VLANs to the CloudStack to create one or more networks that are available for use by the users of that Zone. Virtual networks use "Zone VLANs" and direct tagged networks uses "Direct VLANs".

This chapter discusses network setup that is common to all modes as well as network setup that is specific to one or two of the modes.

4.1 VLAN Allocation

Important: CloudStack networking enables many different deployment styles. Your deployment may not need one or more of the types of VLANs. You should decide what services you want to offer to your users before provisioning VLANs.

VLAN allocation must be considered if Advanced Mode is used for a Zone.

Cloud.com CloudStack is designed to utilize hardware VLANs to isolate guest virtual network traffic. There are three types of VLANs in the CloudStack.

1. **Public VLAN**. A range of VLAN IDs will be reserved for public IP addresses. These VLANs are trunked into every Pod.

2. **Zone VLAN**. A range of VLAN IDs will be reserved for guest virtual networks. These VLANs are trunked into every Pod. One VLAN is allocated per guest virtual network that has active instances.

3. **Direct VLAN.** A range of VLAN IDs will be reserved for direct tagged networks. These networks may either be Zone wide, meaning guests from multiple account can use them, or account-specific, where the entire VLAN is reserved for use by a single account. These VLANs are trunked into every Pod. The administrator provisions these VLANs in the CloudStack one at a time; a range is not given to the CloudStack to manage as is the case with Zone VLANs.

Figure 5 illustrates VLAN allocation in an Availability Zone:
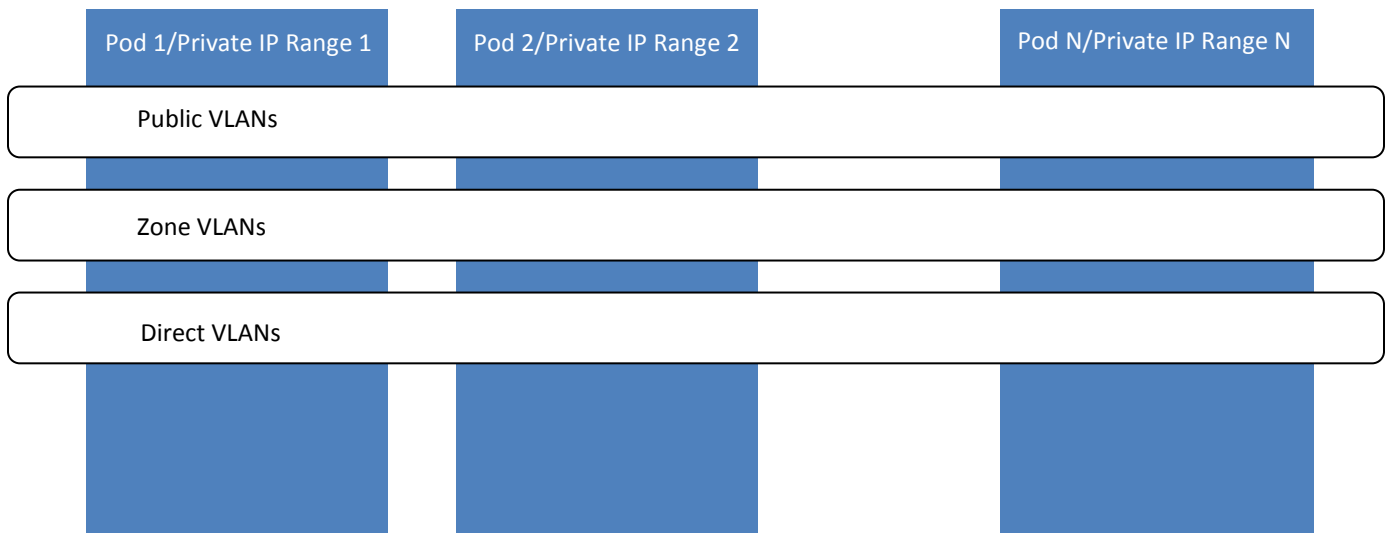
Figure 5 VLAN Allocation in an Availability Zone

The hosts and storage servers reside on an Untagged Private Network. The untagged private network in each Pod is mapped to a unique VLAN and private IP range in the layer-3 switch. The layer-3 switch serves as the default gateway for each private network and ensures a packet can be routed from one host to any other host in the same Zone.

 June 27, 2011

4.1.1 VLAN Allocation with Virtual Networking

With Virtual Networking, VLANs are required for the guests at the Zone level. The following is an example of a VLAN allocation scheme when Virtual Networking is used:

VLAN IDs	Use
< 500	Reserved for administrative purposes and untagged private network for each pod
500-599	Public VLANs
600-999	Zone VLANs
> 1000	Reserved for future use

4.1.2 VLAN Allocation with Direct Tagged

With Direct Tagged networking, there is no need for Public VLANs nor Zone VLANs. There is a new need for a VLAN range for the Direct Attached guests.

VLAN IDs	Use
< 300	Reserved for administrative purposes and untagged private network for each pod
300-499	Directed Attached VLANs
> 500	Reserved for future use

4.1.3 VLAN Allocation with Virtual Networking and Direct Tagged Networking

CloudStack supports deployments that have both Virtual Networking and Direct Tagged guests. In this case it will be necessary to allocate VLANs for both types of guests.

VLAN IDs	Use
< 300	Reserved for administrative purposes and untagged private network for each pod
300-499	Direct Tagged VLANs
500-599	Public VLANs
600-999	Zone VLANs
> 1000	Reserved for future use

4.2 IP Address Allocation

The CloudStack requires several types of IP addresses to be provisioned in it. The required types depend on the networking mode that is in use.

4.2.1 Public IP Addresses

The CloudStack provisions one public IP address per account for use as the source NAT IP address when Advanced Mode is enabled. Users may request additional public IP addresses for their accounts. The administrator must configure one or more ranges of public IP addresses for use by the CloudStack. These IP addresses could be RFC1918 addresses in private clouds.

4.2.2 Private IP Addresses

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.

The administrator should provide private IPs for the system in each Pod and provision them in CloudStack.

- For vSphere with advanced virtual networking, the recommended typical number of private IPs is one per 1 GB of RAM. If you define smaller service offerings, you might need more private IPs. If you have larger service offerings, you might need fewer private IPs.
- 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.

When Advanced Virtual 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

 June 27, 2011

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 when Advanced Virtual networking is enabled, 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.

4.2.3 Direct IP Addresses

In Basic Mode, the 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 untagged VLAN as the Hosts.

In Advanced Mode, the administrator can create additional networks for use by the guests. These networks can be Zone wide, in which case they are available to all guests, or account-specific, 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.

4.2.4 Guest IP Addresses - Virtual Networking

With virtual networking, the CloudStack manages the IP address assignment for the guests in an account. The administrator should set a global configuration parameter to name the CIDR, but there is no need to manage the CIDR on a per-account basis. All virtual networks in the Cloud will use the same CIDR for DHCP and IP address allocation.

4.3 Layer-3 Switch

The layer-3 switch is the core switching layer at the Availability Zone level. The layer-3 switch should be programmed as follows:

- If direct tagged or virtual networking is in use, the layer-3 switch trunks public VLANs, Zone VLANs, and Direct Attached VLANs into each Pod.
- The layer-3 switch functions as the gateway for the untagged private network. A separate VLAN is created in the layer-3 switch for each private IP address range. The layer-3 switch should allow packets to flow between private IP ranges.

The "Virtual Network and Direct Tagged" VLAN allocation in this section is used in the configurations described for layer 2 and layer 3 switches. You can adjust VLAN allocation according to your specific needs.

4.3.1 Example 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.

4.3.1.1 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.

Important: Dell 62xx Series switch only 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.

- Public VLANs (500-599) and Zone VLANs (600-999) and Direct Attached VLANs (300-499) are passed to all the Pod-level layer-2 switches.

4.3.1.2 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 Public VLANs (500-599), Zone VLANs (600-999), and Direct Attached VLANs (300-499) are passed to all the Pod-level layer-2 switches.

4.4 Layer-2 Switch

The layer-2 switch is the access switching layer inside the Pod.

- It should trunk Public VLANs, Zone VLANs, and Direct Attached VLANs into every computing host.
- It should switch untagged traffic for the private network containing computing and storage hosts. The layer-3 switch will serve as the gateway for the private network.

4.4.1 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.

4.4.1.1 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.
- Public VLANs (500-599) , Zone VLANs (600-999) and Direct Attached VLANs (300-499) are passed through all the ports of the layer-2 switch.

4.4.1.2 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 of 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.

4.5 Hardware Firewall

All deployments should have a firewall protecting the management server. This is described in the "Generic Firewall" section. Optionally, some deployments may also have a Juniper firewall that will be the default gateway for the guest virtual networks. This is described in the "External Guest Firewall" section.

4.5.1 Generic Firewall Provisions

The hardware firewall is required to serve two purposes:

- Protect the Management Server farm. NAT and port forwarding should be configured to direct traffic from the public Internet to the Management Server farm.
- Route private network traffic between multiple Availability Zones. Site-to-site VPN should be configured between multiple Availability 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.

4.5.2 External Guest Firewall Integration for Juniper (optional)

Available only for guests using virtual networking (in Advanced Mode)

CloudStack provides for direct management of the Juniper SRX series of firewalls. This enables the 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. This feature is optional. If Juniper integration is not provisioned the CloudStack will use the virtual router for these services.

The Juniper SRX can optionally be used in conjunction with an external load balancer.

CloudStack assumes that External Network elements will be deployed in a side-by-side configuration.

 June 27, 2011
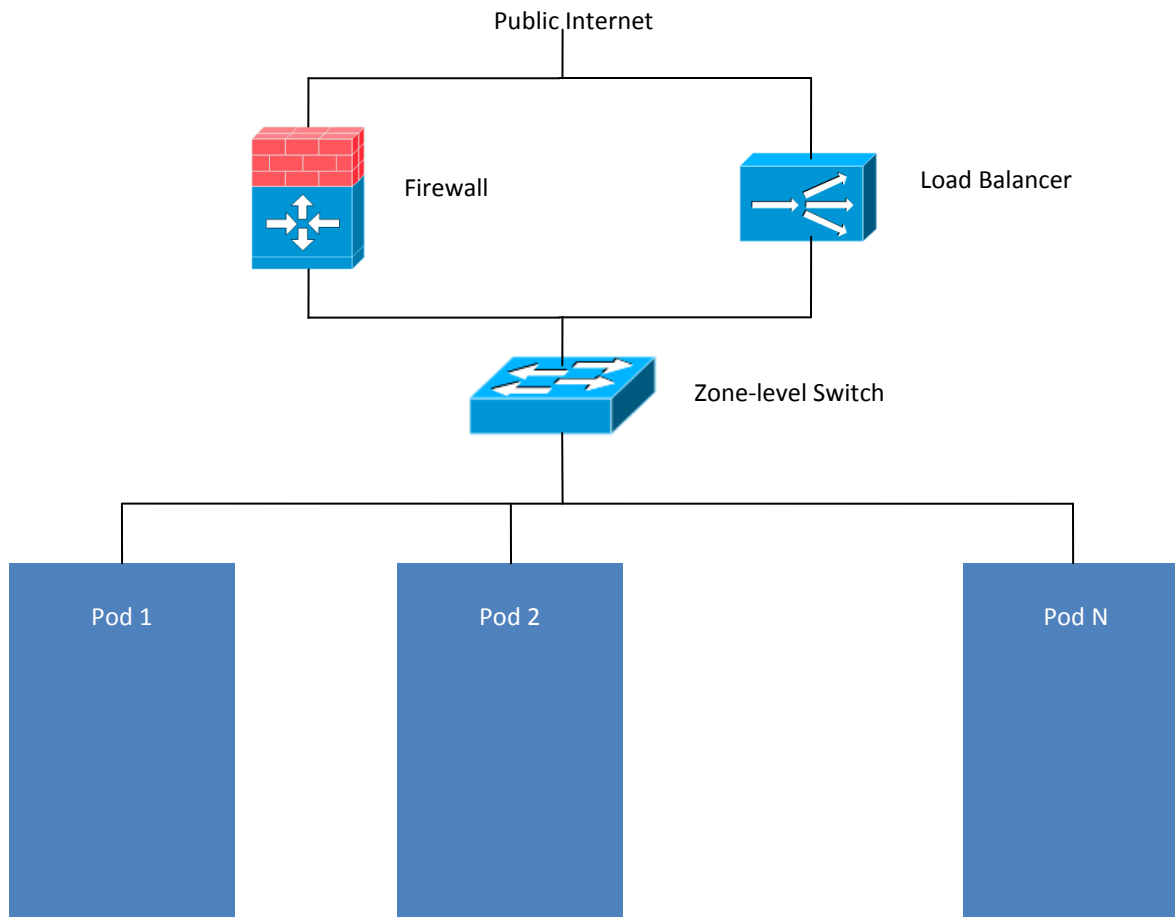
CloudStack requires a Juniper configuration as follows.

1. Install your SRX appliance according to the vendor's instructions.

    Important: The SRX software version must be at least 10.3. Earlier versions will not work.

2. Connect one interface to the private network and one interface to the public network. Alternatively, you can connect the same interface to both networks and a 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 fe-0/0/3 for your public interface and VLAN tag 301, your public interface name would be "fe-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, 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;
}
```

10. If traffic metering is desired, add the firewall filters to your public interface. For example, a sample configuration output (for public interface fe-0/0/3.0, public security zone untrust, and private security zone trust) is:

```
fe-0/0/3 {
    unit 0 {
        family inet {
            filter {
                input untrust;
                output trust;
            }
            address 172.25.0.252/16;
        }
    }
}
```

11. Make sure all Zone VLANs are brought to the private interface of the SRX.

12. The CloudStack will be configured with the Juniper information after the Management Server is installed.

Important: All accounts with guests in a given Zone will use the external firewall if it is configured. It is not currently possible to have some guests or some accounts in a Zone use the external firewall and others use the virtual router.

4.6 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.

Important: Persistence may still be enabled on source ports which do not require it.

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

4.7 External Guest Load Balancer Integration for F5 (optional)

CloudStack can optionally use an 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.

This service is available only to guests using virtual networking (Advanced Mode).

To install and enable your F5 for CloudStack management:

1. Set up your F5 BigIp appliance according to the vendor's directions.
2. Connect it to the public network and the private 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 Zone VLANs are trunked to the private network interface.
5. The CloudStack will be configured with the F5 information after the Management Server is installed.

Important: if an external load balancer is used an external firewall must also be used.

4.8 Direct Network Usage Integration for Traffic Sentinel

To collect usage data for a direct network, CloudStack needs to pull the data from an external network statistics collector installed on the network. Metering statistics for Direct Networking 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 Direct Networked 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. For more information about the Usage Server, see Installing the Usage Server (Optional) on page 90.

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. Click File – Users – Access Control – Reports Script, then select Guest from the dropdown list. CloudStack will be the guest user performing the remote queries to gather network usage for one or more IP addresses.

3. On CloudStack, add the Traffic Sentinel host. In the CloudStack admin UI, click System -> Physical Resources -> Zone in the admin UI, select the pod and cluster, then click Add Host. In the Host Name field, enter the configured IP address of the hardware module where Traffic Sentinel is installed.

4. In the CloudStack admin UI, click Configuration – Global Settings. Set direct.network.stats.interval to the length of time you would like to pass between queries to Traffic Sentinel.

4.9 Additional Topology Requirements

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. Note that you must not expose port 8250 to the public Internet. The secondary storage VM can be located on any Host in the Zone. It uses the private network for its communication.

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 console proxy VMs connect to all hosts in the Zone over the private network. Therefore the private network of any given Pod in the Zone must have connectivity to the private network of all other Pods in the Zone.

The secondary storage NFS export is mounted by the secondary storage VM. Secondary storage traffic goes over the private 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 private network to the storage network.

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 and Console Proxy VMs.

The Management Servers communicate with each other to coordinate tasks amongst themselves. This communication uses TCP on ports 8250 and 9090.

With Advanced Networking, separate subnets must be used for private and public networks.

The public internet must not be able to access port 8096 on the Management Server.

The Management Servers communicate with the XenServers on ports 22 (ssh) and 80 (HTTP).

The Management Servers communicate with VMware vCenter servers on port 443 (HTTPs).

The Management Servers communicate with the KVM servers on port 22 (ssh).

5   Storage Setup

CloudStack is designed to work with a wide variety of commodity and enterprise-grade storage. Local disk may be used as well. 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

5.1   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.

5.2   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.

5.3   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.

5.3.1   Linux NFS on Local Disks and DAS

This section describes how to configure an NFS export on a standard Linux installation. Instructions in this section specifically apply to RHEL/CentOS 5. Steps to setup other distributions may vary.

1.   Install the RHEL/CentOS distribution on the storage server.

    Important: 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.

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 <your.subnet.mask>(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 private 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 CIDR's:

```
/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_TCPPORT=32803
LOCKD_UDPPORT=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.

5.3.2 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.

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 private 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 CIDR's:

```
/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 Citrix XenServer Installation and Configuration

Citrix XenServer 5.6 GA must be installed on the Hosts. Citrix XenServer can be downloaded from the Citrix Website (http://www.citrix.com/lang/English/lp/lp_1688615.asp) and installed using the Citrix XenServer Installation Guide.

Important: 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. See http://docs.vmd.citrix.com/XenServer/4.0.1/reference/ch02.html for more information on homogenous XenServer hosts.

Important: You must re-install Citrix XenServer if you are going to re-use a host from a previous install.

Important: CloudStack requires XenServer 5.6, 5.6 FP1, or 5.6 FP2.

Following installation, CloudStack requires the following configuration.

- Username and password
- Time synchronization
- Licensing
- Network Setup
  - Configuring public network with a dedicated NIC (optional)
  - NIC bonding (optional)
- iSCSI Multipath Setup (optional)

The following sections contain information about configuring the XenServer.

6.1 Username and Password

All XenServers in a Cluster must have the same username and password as configured in the CloudStack.

6.2 Time Synchronization

The XenServer host must be set to use NTP or another clock synchronization mechanism. All Hosts in a Pod must have the same time. 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
```

6.3 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.

6.3.1 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 on **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.

6.4 Physical Networking Setup

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 private network interface must be static. It can be set on the host itself or obtained via static DHCP.

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

Important: If a single NIC is your desired NIC configuration there is no need for further configuration. Continue to the next section, Management Server Installation.

6.4.1 Configuring Public Network with a Dedicated NIC (optional)

The CloudStack supports the use of a second NIC (or bonded pair of NICs, described later) 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 Installation.

When a dedicated NIC is present for the public network, the public network can be implemented using a tagged or untagged VLAN.

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 the 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>
```

 June 27, 2011

6.4.2 Separate Storage Network (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 private network NIC, `ping –I eth0 <primary storage device IP>` must fail. In all deployments, secondary storage devices must be pingable from the private 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 bonding is done, you should follow the procedure described in the private network section to set up the bond on the first host in the cluster as well as second and subsequent hosts in the cluster.

If no bonding is done the administrator must setup 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
```

6.4.3 NIC Bonding (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 private network

- 2 NICs on private, 2 NICs on public, storage uses private 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 private network for added slave hosts.

6.4.3.1 Private Network Bonding

The administrator must bond the private network NICs prior to adding the host to the CloudStack.

6.4.3.2 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".

Important: This label is significant as the 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 private 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 the CloudStack as the private network.

6.4.3.3 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 private network.

6.4.3.4 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.

 June 27, 2011

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

Important: This label is significant as the 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 the CloudStack as the public network.

6.4.3.5 Adding Additional Hosts to the Cluster

With the bonds (if any) established on the master you should add additional, slave hosts. For all additional hosts to be added to the Cluster execute this step. 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]
```

6.4.3.6 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.

6.5 Primary Storage Setup

The 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=lvmohba shared=true
      device-config:SCSIid=360a98000503365344e6f6177615a516b
      name-label="e6849e96-86c3-4f2c-8fcc-350cc711be3d"
    ```

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

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

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

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

    Make note of the values you will need when you add this storage to the CloudStack later (see Add Primary Storage on page 85). 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.

6.6 iSCSI Multipath Setup (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 85). 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.

 June 27, 2011

If you encounter difficulty, address the support team for the SAN provided by your vendor. If they are not able to solve your issue, contact cloud.com support.

6.7 Security Groups Setup (optional)

CloudStack supports the use of security groups in Basic Networking with XenServer 5.6 FP1.

NOTE: Security groups are not supported with XenServer 5.6 or XenServer 5.6 FP2.

Each XenServer 5.6 FP1 host must have the Citrix XenServer Cloud Supplemental Pack installed plus additional software from Cloud.com. Follow these steps to enable the use of security groups.

1. Install Citrix XenServer Cloud Supplemental Pack (CSP). This is obtained from Citrix. This should include the CSP kernel as well as ebtables-2.0.9. After installation confirm that the kernel name as returned by "uname -a" includes "csp" in its name.

2. Get and install the Cloud.com additional components. The following code assumes XenServer 5.6 FP2.

```
# yum -y erase iptables
# wget http://download.cloud.com/support/security.groups/fp1/iptables-1.4.7-
1.i386.rpm
# wget http://download.cloud.com/support/security.groups/fp1/iptables-ipv6-1.4.7-
1.i386.rpm
# wget http://download.cloud.com/support/security.groups/fp1/ipset-4.5-4.i386.rpm
# rpm -ivvh iptables-1.4.7-1.i386.rpm
# rpm -ivvh iptables-ipv6-1.4.7-1.i386.rpm
# rpm -ivvh ipset-4.5-4.i386.rpm
# sed -i 's/net.bridge.bridge-nf-call-iptables = 0/net.bridge.bridge-nf-call-
iptables = 1/' /etc/sysctl.conf
# sed -i 's/net.bridge.bridge-nf-call-arptables = 0/net.bridge.bridge-nf-call-
arptables = 1/' /etc/sysctl.conf
```

3. Reboot the XenServer host

```
# reboot
```

Now go on to Management Server Installation on page 64.

7   VMware vSphere Installation and Configuration

VMware vSphere must be installed on the Hosts. VMware vSphere can be downloaded and purchased from the VMware Website (https://www.vmware.com/tryvmware/index.php?p=vmware-vsphere&lp=1) and installed by following the VMware vSphere Installation Guide.

Following installation, CloudStack requires the following configuration.

- ESXi Host Setup
- Configure Host Networking
    - Configure Virtual Switch
    - Configure vCenter Management Network
    - Configure NIC Bonding (optional)
- Configure Multipath Storage (optional)
- Configure clusters in vCenter and add hosts to them, or add hosts without clusters to vCenter

The following sections contain information about configuring the VMware vSphere.

7.1   Prerequisites and Constraints

The following requirements must be met in order for the VMware vSphere installation to work properly.

- VMware vCenter Standard Edition 4.1 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.
- The CloudStack requires VMware vSphere 4.1. 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 private network **must not** be configured as a separate tagged virtual network. The CloudStack private network is the same as the vCenter management network, and will inherit its configuration. See Configure vCenter Management Network on page 47.
- CloudStack requires ESXi. ESX is not supported.
- All resources used for CloudStack must be used for CloudStack only. CloudStack cannot shares 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 product 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 the ESXi hypervisor hosts. These would include the VLANS for Management, Storage, vMotion, and guest VLANs. The guest VLAN (used in Advanced Networking; see **Error! Reference source not found.** on page **Error! Bookmark not defined.**) is a contiguous range of VLANs that will be managed by the CloudStack Product. CloudStack does not support Distributed vSwitches in VMware.

 June 27, 2011

7.2   Licensing

CloudStack requires vSphere and vCenter, both version 4.1.

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 and discuss with your VMware sales representative.

vCenter Server Standard is recommended.

7.3   Preparation Checklist

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

7.3.1   Management Server Checklist

You can either install a single instance of the CloudStack Management server or multiple Management Servers in a cluster with a load balancer. For optional Clustering setup and replication setup, see Multi-Node Install (Multiple Management Servers) on page 66.

You will need the following information for each Management Server.

	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 5.4 (or later) or CentOS 5.4 (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.

7.3.2 Database Checklist

For a single-node database setup, you will need the following information.

	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 5.4 (or later) or CentOS 5.4 (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.

7.3.3 vCenter Checklist

You will need the following information about vCenter.

	Value	Notes
vCenter User		This user must have admin privileges.
vCenter User Password		Password for the above user.

 June 27, 2011

vCenter Datacenter Name		Name of the datacenter.
vCenter Cluster Name		Name of the cluster.

7.3.4 Networking Checklist

You will need the following information about the VLAN.

	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 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.
Public VLAN Gateway		
Public VLAN Netmask		
VLAN Range for Customer use		A contiguous range of non-routable VLANs. One VLAN will be assigned for each customer.

7.3.5 Storage Checklist

CloudStack requires two types of storage: Primary (NFS, iSCSI, local and FC) and Secondary Storage (NFS only). The volumes used for Primary and Secondary storage should be accessible from Management Server and the ESXi 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.

	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.

7.4 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.

7.5 Physical Host Networking

You should have a plan for cabling the vSphere hosts. Proper network configuration is required before adding a vSphere Host to the 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.
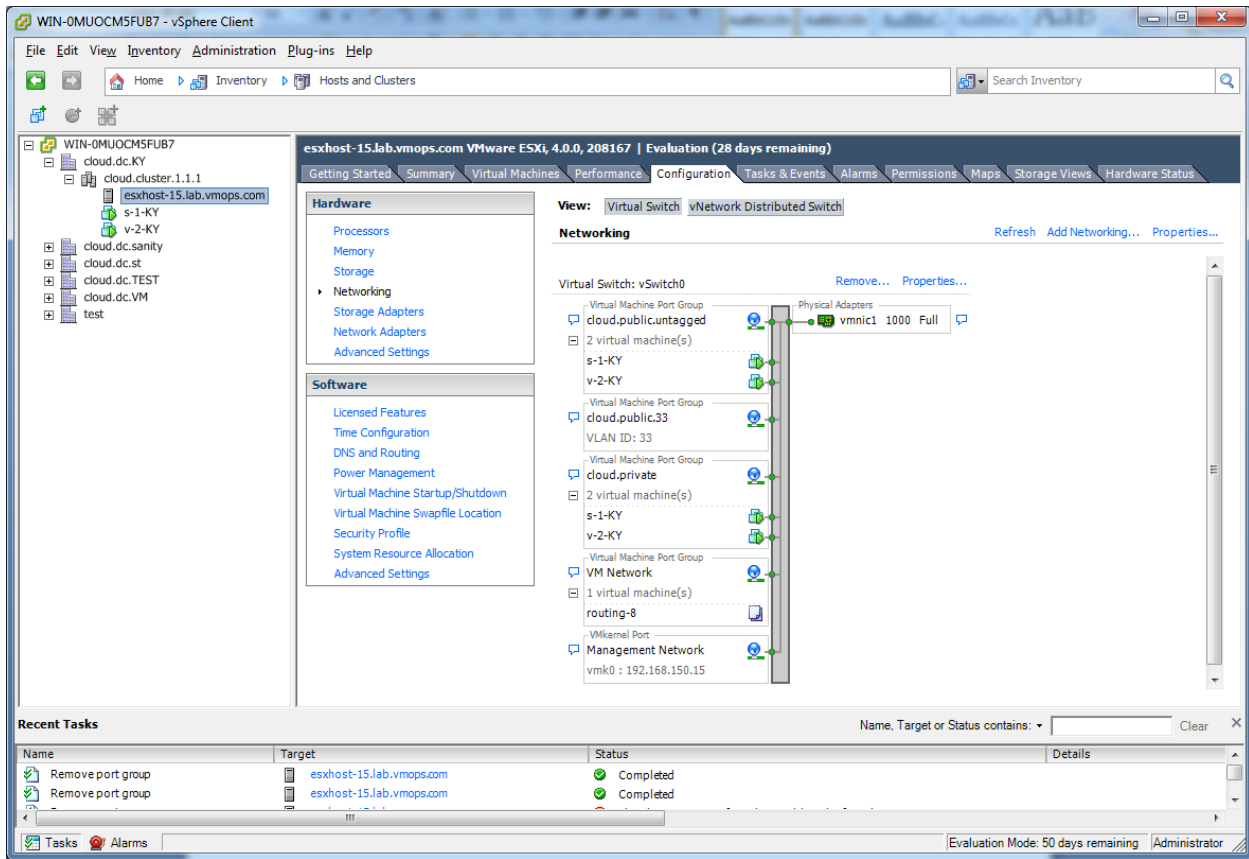
In the host configuration tab, click the "Hardware/Networking" link to bring up the networking configuration page as above.

7.5.1 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. See Describe Your Deployment on page 72.

7.5.1.1 Separating Traffic

The 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 the CloudStack to use these vSwitches as described in Describe Your Deployment on page 72.

7.5.1.2 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).
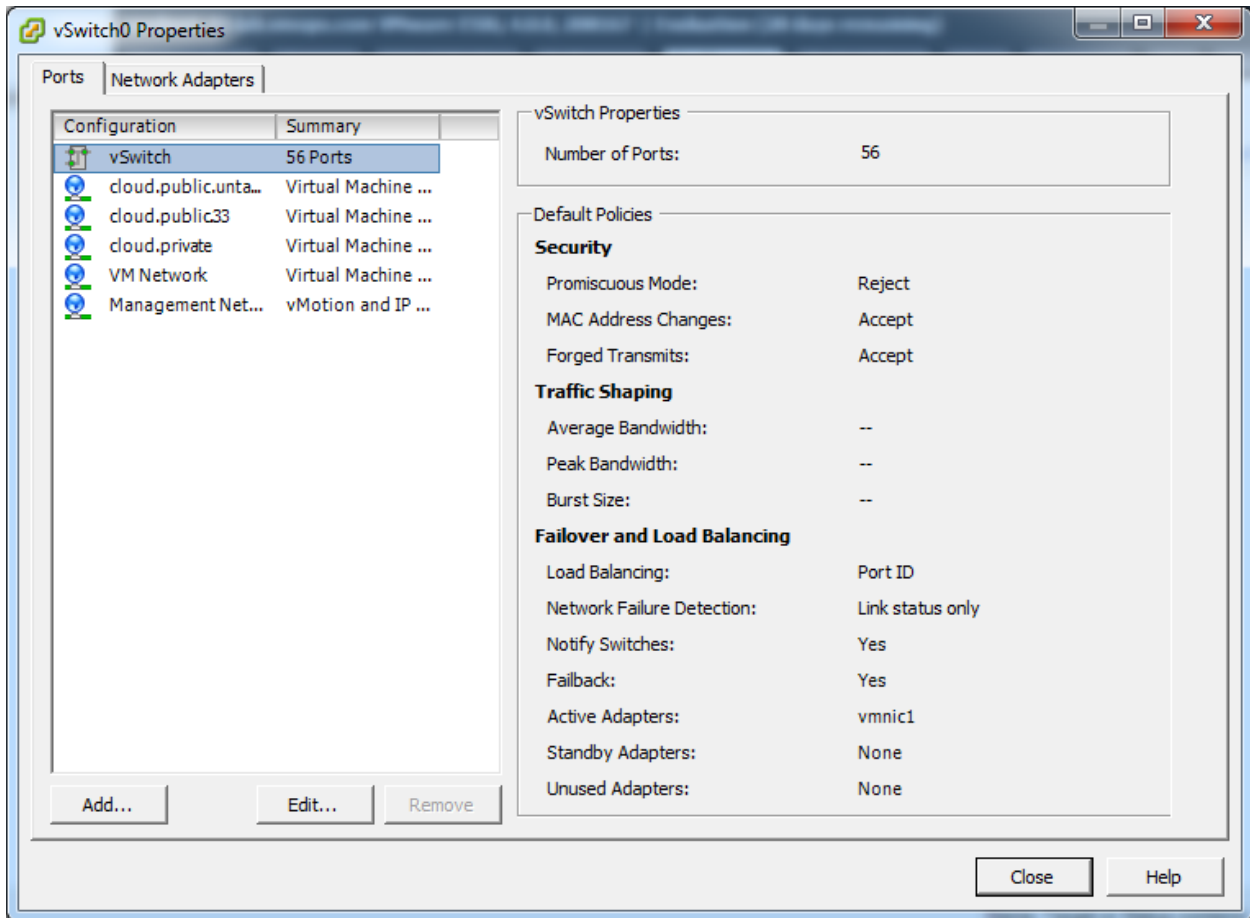
In vSwitch properties dialog, select the vSwitch and click Edit. You should see the following dialog:

                      June 27, 2011
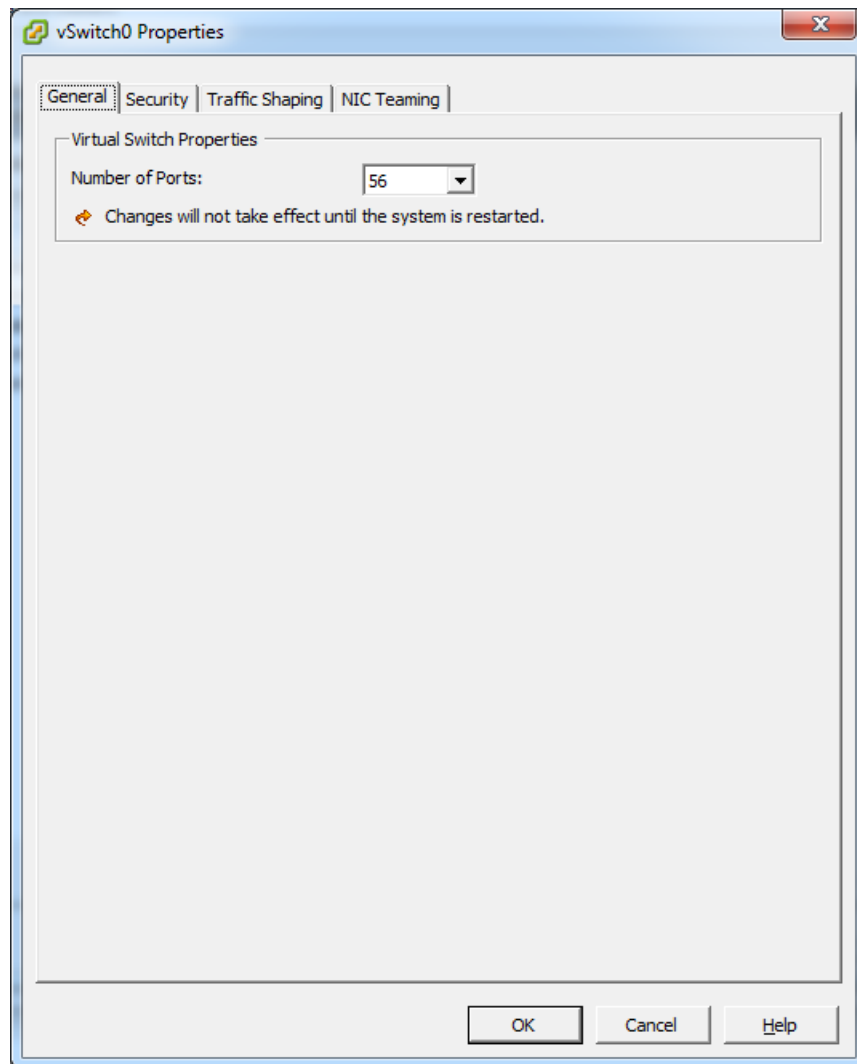
In this dialog, you can change the number of switch ports.Aafter you've done that, ESXi hosts are required to reboot in order for the setting to take effect.

7.5.2 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 private network. CloudStack requires the vCenter management network to be configured properly. Select the management network item in the dialog, then click Edit.
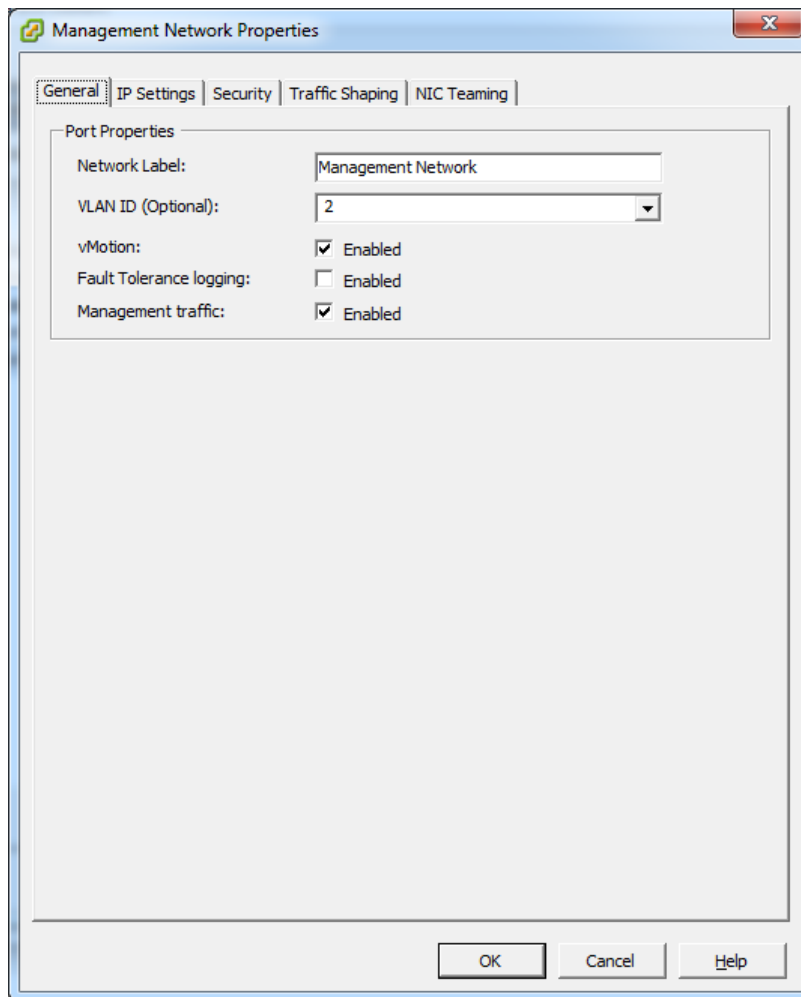
Make sure the following values are set:

- VLAN ID set to either the desired ID (for a tagged VLAN) or None (for an untagged network).

- vMotion enabled.

- Management traffic enabled.

7.5.3 Configure NIC Bonding

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

7.6 Storage Preparation

Use of iSCSI requires preparatory work in vCenter. You must add an iSCSI target and create an iSCSI datastore. This step should be skipped if NFS will be used.

7.6.1 Enable iSCSI initiator for ESXi hosts

1. In vCenter, go to Hosts and Clusters/Configuration, and click Storage Adapters link. You will see:
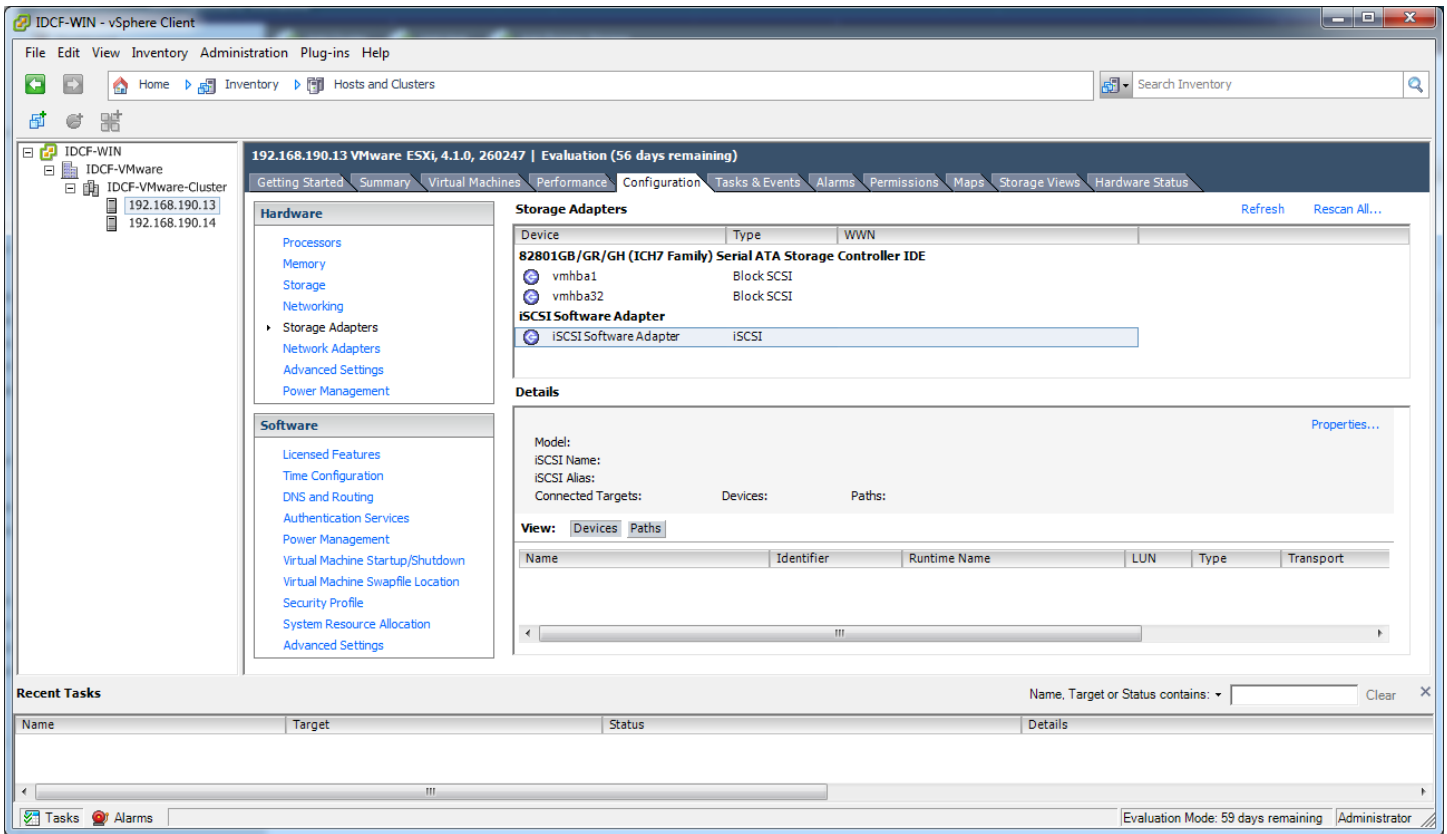
2. Select iSCSI software adapter and click Properties.
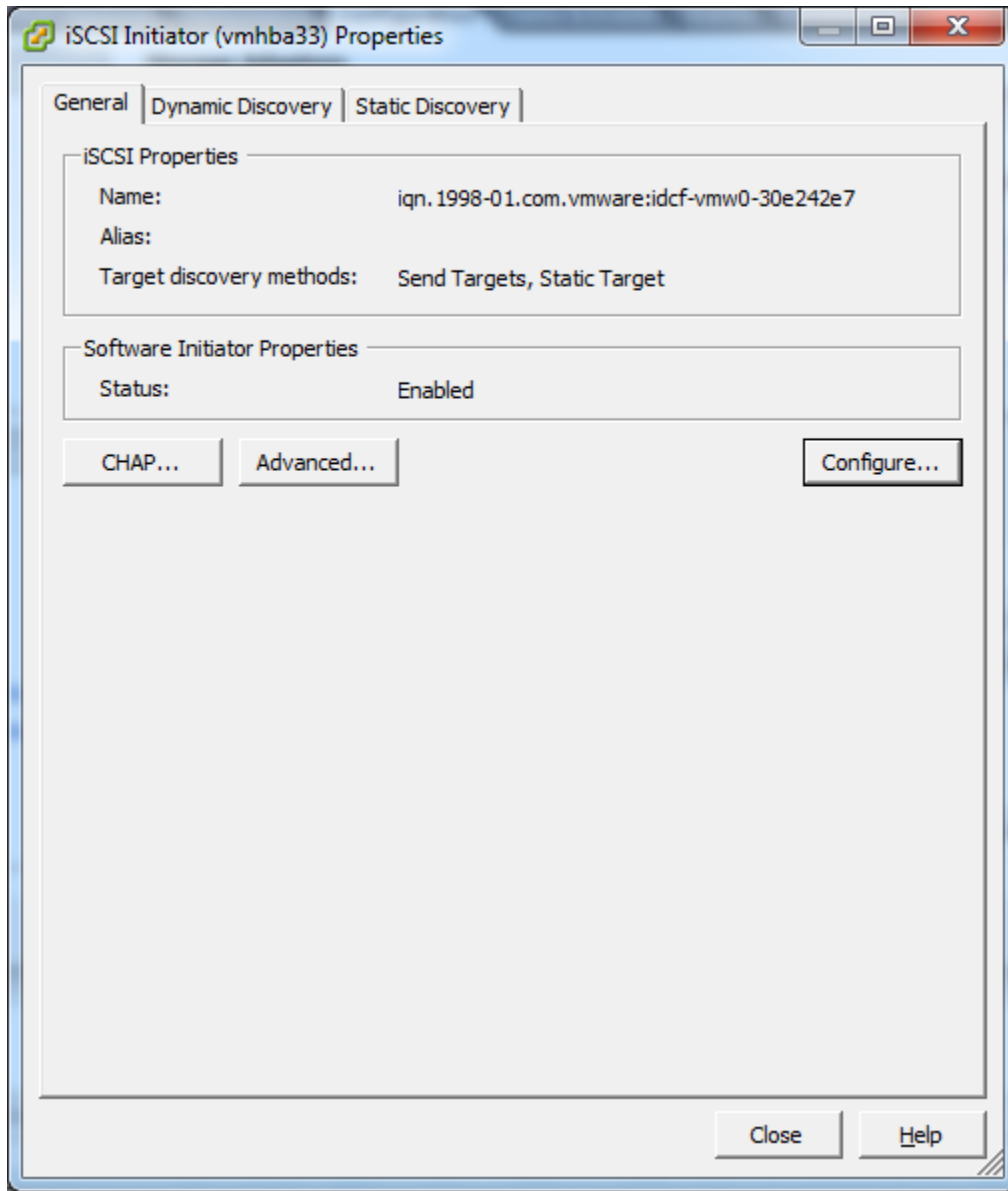
3. Click the Configure… button.

 June 27, 2011
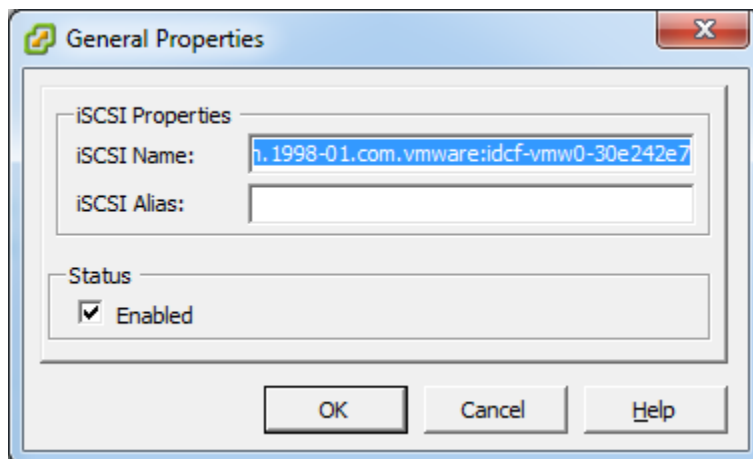
4. Check Enabled to enable the initiator.

5. Click OK to save.

7.6.2 Add iSCSI target

Under the properties dialog, add the iSCSI target info:
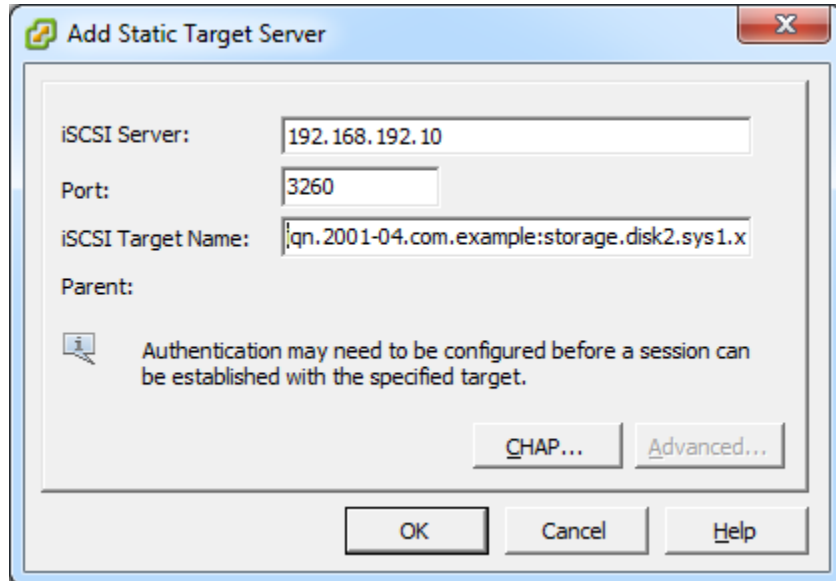
Repeat these steps for all ESXi hosts in the cluster.

7.6.3 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.
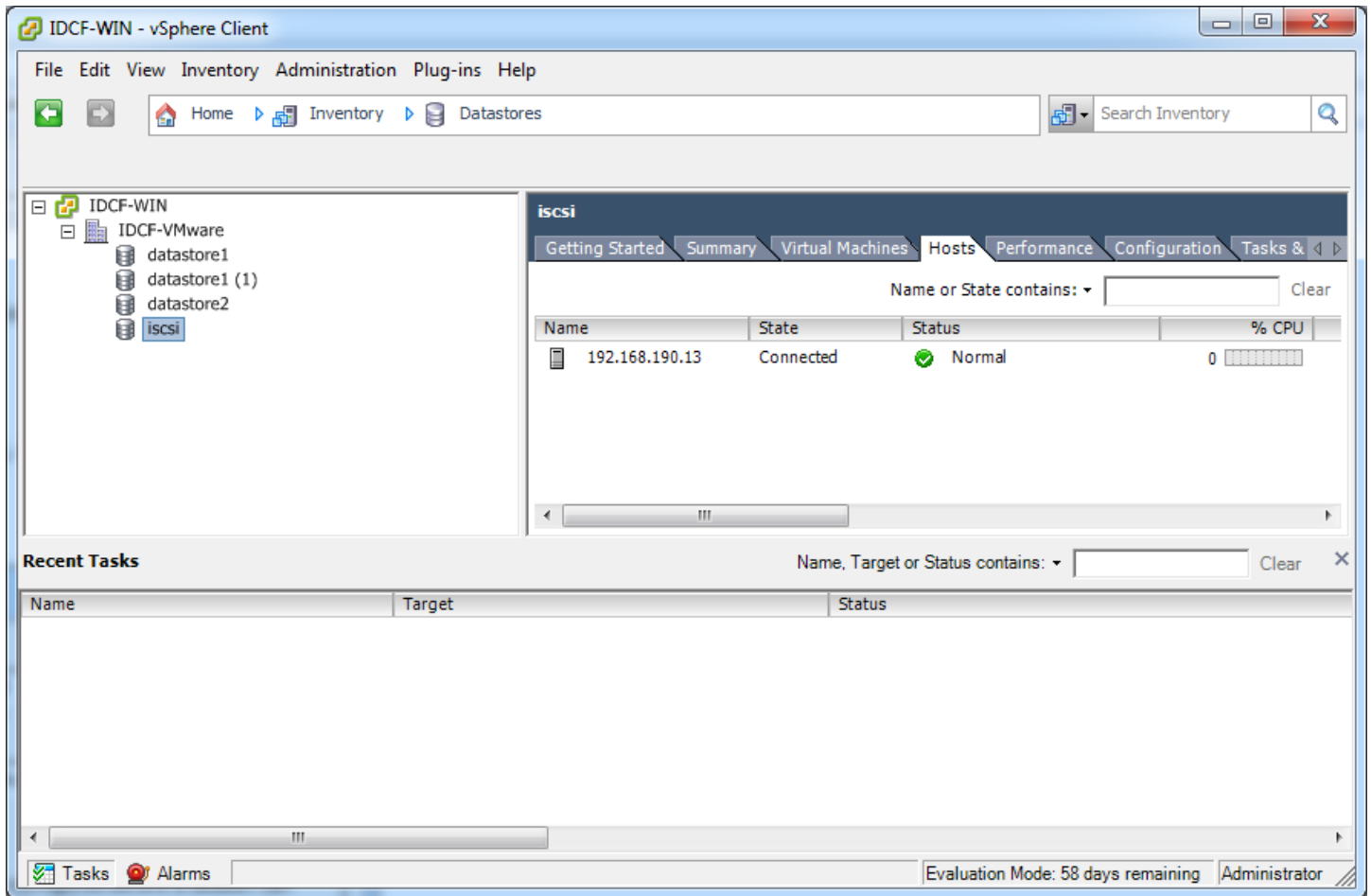
7.6.4 Multipathing

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

7.7 Add Hosts or Configure Clusters

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.

Important: the vCenter user that is provided to the CloudStack should have full administrator privileges.

7.7.1 Clusters

Use vCenter to create a vCenter cluster and add your desired hosts into the cluster. You will later add the entire cluster into the CloudStack with a single action.

Now go on to Management Server Installation on page 64.

8 KVM Installation and Configuration

Important: 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.

Important: All Hosts in the cloud must be of the same kernel version. For example, all Hosts may be RHEL6 64 bit.

Important: For Service Provider and Enterprise Edition, only RHEL 6 is supported. CentOS 6 will be supported shortly after it is available.

8.1 Installing the CloudStack Agent on a Host

Each KVM Host must have the CloudStack Agent installed on it. Install the CloudStack Agent on each Host using the following steps. All commands should be run as root. On Fedora and RHEL6 you have to make sure that the hostname resolves in DNS or /etc/hosts.

A Host's host OS must also have a fully qualified domain name. Usually you can correct the lack of a FQDN by editing /etc/hosts. You will also want to make sure that the IP address associated with the hostname is the IP address of the default route table entry (usually eth0). If the hostname resolves to 127.0.0.1 guest networking will not work.

1. 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. On RHEL6, remove qemu-kvm. The CloudStack provides a patched version.

   ```
   yum erase qemu-kvm
   ```

3. Check for quotation marks (") in any of the ifcfg-ethX files.   RHEL6 may create lines like IPADDR="192.168.21.217". To remove the quotation marks you can either run "setup" and choose to edit the network configuration or you can manually edit /etc/sysconfig/network-scripts/ifcfg-ethX. You should remove the quotation marks from all values in this file.

4. Disable SELinux.

   Set SELinux up to be permissive by default. First, set the SELINUX variable in /etc/selinux/config to "permissive". This ensures that the CloudStack Agent can run properly on system reboot. Then set SELinux to permissive until the system is rebooted:

   ```
   setenforce permissive
   ```

5. Install the CloudStack packages. You should have a file in the form of "CloudStack-NNNN.tar.gz". Untar the file and then run the install.sh script inside it:

   ```
   # tar xzf CloudStack-2.2.0-1-centos.tar.gz
   # cd CloudStack-2.2.0-1-centos
   # ./install.sh
   Setting up the temporary repository...
   Cleaning Yum cache...
   Loaded plugins: fastestmirror
   11 metadata files removed
   Welcome to the Cloud.com CloudStack Installer.  What would you like to do?

       M) Install the Management Server
       A) Install the Agent
   ```

```
    S) Install the Usage Monitor
    D) Install the database server
    Q) Quit

    > A
```

Choose "A" to install the Agent software.

6. Do one of the following:

- If this is not the first time you have installed the CloudStack agent on this machine (for example, you are upgrading from a previous version), you need to install the latest version of netcf-libs. Do steps 7 - 10.

- If this is a fresh install with release 2.2.2 or higher, the latest version of netcf-libs was installed for you. You are done!

7. Log in to the host as root.

8. Run the following commands. In the first command, use the same directory where the software was installed in step 5; your actual directory might be different than this example.

```
# cd CloudStack-2.2.0-1-centos
# rpm -Uvh ./deps/netcf-libs*.rpm --force
```

9. Open the firewall configuration file in your favorite editor:

```
# vi /etc/sysconfig/system-config-firewall
```

10. If system-config-firewall contains the line /usr/share/netcf/iptables-forward-bridged, then do these additional steps. Otherwise, you are done!

a. Remove the following line, then save and quit the file.

```
/usr/share/netcf/iptables-forward-bridged
```

b. Run this command. This puts into effect the changes from step (a) so that the new rule is live on the firewall.

```
# lokkit – update
```

c. Run this command:

```
# sed -i "/^\-A\ FORWARD\ -m\ physdev\ --physdev-is-bridged\ -j\ ACCEPT/d"
/etc/sysconfig/iptables
```

This will delete any line like "-A FORWARD –m physdev --physdev-is-bridged –j ACCEPT" in iptables. This line was inserted in iptables as a workaround for a known issue, but is no longer needed once you have installed the new netcf-libs.

d. Restart the affected services:

```
# service iptables restart
# service libvirtd restart
# service cloud-agent restart
```

The CloudStack Agent is now installed. Later in the installation, you will add this host to the CloudStack via the Management Server. This step will configure the Agent on the Host.

Important: A Host must have a statically allocated IP address; host addition will error and fail if a dynamically-assigned address is present.

8.2 Physical Network Configuration

You should have a plan for how the Hosts will be cabled and which physical NICs will carry what types of traffic. By default the 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 private network. Then the customer should edit /etc/cloud/agent/agent.properties and add values for

- 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.

8.3 Primary Storage Setup (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, and the storage is based on some clustered file system technology like OCFS2. This is called "SharedMountPoint" storage and is an alternative to NFS. 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 the CloudStack.

Now go on to Management Server Installation on page 64.

9   Bare Metal Installation

You can set up bare metal hosts in a CloudStack cloud and manage them with the Management Server. Bare metal hosts do not run hypervisor software. You do not install the operating system – that is done using PXE when an instance is created from the bare metal template (which you are going to create as part of this Installation procedure). Bare metal hosts use direct untagged networking. A cloud can contain a mix of bare metal instances and virtual machine instances.

Prepare to add bare metal instances to your cloud by performing the setup procedures in the next few sections.

1. Set Up the Firewall for Direct Untagged Networking (p. 56)   ❑

2. (Optional) Set Up External Guest Load Balancer for Bare Metal (p. 60)   ❑

3. Set Up IPMI (p. 60)   ❑

4. Enable PXE on the Bare Metal Host (p. 60)   ❑

5. Install the PXE and DHCP Servers (p. 61)   ❑

6. Set Up a CIFS File Server (p. 61)   ❑

7. Create a Bare Metal Image (p. 62)   ❑

8. Install the Management Server for Bare Metal (p. 62)   ❑

9. Add the PXE Server and DHCP Server to Your Deployment (p. 62)   ❑

10. Add a Cluster, Host, and Firewall (p. 63)   ❑

11. Add a Service Offering and Template (p. 63)   ❑

9.1   Set Up the Firewall for Direct Untagged Networking

Bare metal uses direct untagged networking. If you are using a firewall, you must set it up for this type of networking. This section gives the instructions for setting up a Juniper SRX for direct untagged networking. For more about adding the Juniper to your network, see External Guest Firewall Integration for Juniper (optional) on page 24.

1. Connect to the SRX as root.

   - It is recommended to connect using the serial port to ensure a reliable connection.

   - Connect with a 9600 baud rate.

2. Clear out factory default settings.

   a. Delete existing interfaces.

      ```
      # delete interfaces
      ```

   b. Delete VLANs.

      ```
      delete vlans
      ```

   c. Delete firewall rules.

      ```
      delete firewall
      ```

June 27, 2011

d. Delete NAT rules.

```
delete security nat
```

e. Delete security zones.

```
delete security zones
```

f. Make sure the initial security policies are correct.

```
# show security policies
```

The output should look like this:

```
from-zone trust to-zone untrust {
    policy trust-to-untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

If you do not see the above output, follow these steps to re-create the base security policy.

```
# delete security policies

# set security policies from-zone trust to-zone untrust policy trust-to-untrust
match source-address any destination-address any application any

# set security policies from-zone trust to-zone untrust policy trust-to-untrust
then permit
```

3. Set up interfaces, security zones, and the default route.

   a. Determine which SRX ports you are using. There should be one private interface and one public interface. For example, ge-0/0/1 might be private, and ge-0/0/2 might be public.

   b. Program the interfaces with correct IP addresses. Run the following command once for each interface, substituting your own values.

   ```
   # set interfaces <name> unit 0 family inet address <address>/<subnet size>
   ```

   For example:

   ```
   # set interfaces ge-0/0/1 unit 0 family inet address 192.168.10.7/24
   # set interfaces ge-0/0/2 unit 0 family inet address 192.168.10.8/24
   ```

   c. Create two security zones: one called "trust" (private zone) and the other called "untrust" (public zone).

   ```
   # set security zones security-zone trust
   # set security zones security-zone untrust
   ```

d. Add the private interface to the trust zone and the public interface to the untrust zone. Run the following command once for each interface, substituting your own values.

```
# set security zones security-zone <zone> interfaces <name>
```

For example:

```
# set security zones security-zone trust interfaces fe-0/0/1
# set security zones security-zone untrust interfaces fe-0/0/2
```

e. Allow host inbound traffic on both security zones.

```
# set security zones security-zone trust host-inbound-traffic system-services
all
# set security zones security-zone trust host-inbound-traffic protocols all
# set security zones security-zone untrust host-inbound-traffic system-services
all
# set security zones security-zone untrust host-inbound-traffic protocols all
```

f. Create a default route. This can be through the public interface. Substitute your own values for the IP addresses in this example.

```
# set routing-options static route 0.0.0.0/0 next-hop 192.168.1.1 install
```

g. Verify your interface setup. Your IP addresses should appear instead of our examples.

```
# show interfaces
  ge-0/0/1 {
     unit 0 {
        family inet {
           address 192.168.240.1/24;
        }
     }
  }
  ge-0/0/3 {
     unit 0 {
        family inet {
           address 192.168.1.91/24;
        }
     }
  }
```

                     June 27, 2011

h. Verify your zone setup. Your interface names should appear instead of our examples.

```
# show security zones
  security-zone trust {
     host-inbound-traffic {
        system-services {
           all;
        }
        protocols {
           all;
        }
     }
     interfaces {
        ge-0/0/1.0;
     }
  }
  security-zone untrust {
     host-inbound-traffic {
        system-services {
           all;
        }
        protocols {
           all;
        }
     }
     interfaces {
        ge-0/0/3.0;
     }
  }
```

i. Verify your route. Your IP addresses should appear instead of our examples.

```
# show routing-options
  static {
     route 0.0.0.0/0 {
        next-hop 192.168.1.1;
        install;
     }
  }
```

4. Set up system services and a root login.

a. Allow CloudStack to program the SRX through the API.

```
# set system services xnm-clear-text
```

b. Set a root password for the system. You will be prompted to enter and re-enter a password.

```
# set system root-authentication plain-text-password
```

5. Commit your changes.

```
# commit
```

Wait for confirmation.

9.2 (Optional) Set Up External Guest Load Balancer for Bare Metal

Support for using an F5 load balancer with bare metal is not yet implemented. Meanwhile, you can use the following technique to simulate an F5 for testing purposes.

1. Set up an F5 BIG-IP Local Traffic Manager Virtual Edition appliance according to the vendor's directions at
   http://support.f5.com/kb/en-us/products/big-ip_ltm/releasenotes/product/relnotes_ve_10_2_0.html.

2. Connect the VMware host where your virtual F5 is running to the same management network as the CloudStack Management Server.

3. Record the management IP address, username, password, public interface name, and private interface name of the F5. The interface names will be like 1.1 or 1.2.

4. Confirm that the configuration is successful:

   a. Ping the F5 management IP address from the CloudStack Management Server.

   b. Log in to https://<management server IP address> and log in with the username and password from step 3.

5. Using the Management Server UI, add the F5 virtual appliance to CloudStack.

   a. Choose System – Physical Resources, choose the desired Zone, and choose Network.

   b. Click Add Load Balancer.

   c. In the dialog box, enter the information gathered in step 3, then click Add.

9.3 Set Up IPMI

The procedure to access IPMI settings varies depending on the type of hardware. Consult your manufacturer's documentation if you do not already know how to display the IPMI settings screen.

Once you are there, set the following:

- IP address of IPMI NIC
- Netmask
- Gateway
- Username and password for IPMI NIC

9.4 Enable PXE on the Bare Metal Host

The bare metal host needs to use PXE to boot over the network. Access the BIOS setup screen (or equivalent for your hardware) and do the following:

- Set hard disk as the first priority device in the boot order.
- Make sure the connected NIC on the bare metal machine is PXE-enabled.
- Make a note of the MAC address of the PXE-enabled NIC. You will need it later.

 June 27, 2011

9.5 Install the PXE and DHCP Servers

Each bare metal host must be able to reach a PXE server and a DHCP server. Use the following steps to install the needed servers on another machine (or virtual machine). All commands should be run as root.

1. Log in as root to a host or virtual machine running CentOS 5.5.

2. You should have access to a file in the form of "CloudStack-NNNN.tar.gz." Copy that file to the machine.

3. Untar the file and then run the install.sh script inside it:

```
# tar xzf CloudStack-2.2.0-1-centos.tar.gz
# cd CloudStack-2.2.0-1-centos
# ./install.sh
Setting up the temporary repository...
Cleaning Yum cache...
Loaded plugins: fastestmirror
11 metadata files removed
Welcome to the Cloud.com CloudStack Installer.  What would you like to do?

    M) Install the Management Server
    A) Install the Agent
    B) Install BareMetal Agent
    S) Install the Usage Monitor
    D) Install the database server
    Q) Quit

    > B
```

Choose "B" to install the software that is needed for bare metal.

4. Run the bare metal setup script.

```
# cloud-setup-baremetal
```

5. Make note of the TFTP root directory that is displayed by this script. You will need it later.

9.6 Set Up a CIFS File Server

The bare metal image will be stored on a file server. We recommend using a Windows machine with its built-in CIFS file sharing functionality. If you prefer to use Linux as the file server, use the Samba Windows interoperability suite. Set up the CIFS file server using these steps:

1. On the file server, set up the following directory structure: Share\Ping_Backup. Share is the folder that will be the CIFS root directory, and Ping_Backup will store images created with the Partimage Is Not Ghost (PING) tool.

2. Share the root directory. On Windows, right-click the Share folder and choose Share with… .

9.7   Create a Bare Metal Image

Create an image which can be installed on bare metal hosts later, when bare metal instances are added to the cloud. To create the image, you will be using the Partimage Is Not Ghost (PING) tool. For information about how to use PING, see http://ping.windowsdream.com/ping/howto-2.01.html.

1. Install the desired OS on a machine with hardware identical to what you intend to use for the bare metal machines.

    Be sure the hardware is identical.

2. Use PING to create an image and store it in the Share\Ping_Backup directory on the CIFS file server you have set up.

    *   PING will prompt you for the storage location. Use <IP of CIFS server>\Share\Ping_Backup.

    *   PING will prompt you for a name for the image. Give any name you find helpful, such as win7_64bit.

9.8   Install the Management Server for Bare Metal

If you have not already installed the Management Server, do so now.

1. Follow the steps in Management Server Installation on page 64. At the end of this procedure, the Management Server should be running.

2. Then return here and continue with the next section, Add the PXE Server and DHCP Server to Your Deployment.

9.9   Add the PXE Server and DHCP Server to Your Deployment

As part of describing your deployment to CloudStack, you will need to add the PXE server and DHCP server that you created in Install the PXE and DHCP Servers on page 8.

1. Add a zone and pod using the Management Server UI. When creating the zone, in network type, choose Basic.

    Follow the steps in Add a New Zone on page 74.

2. In the left navigation tree, choose System, then Physical Resources.

3. Select your Pod.

4. Click Add Network Device. Input the following and click Save:

    *   **Type:** PxeServer

    *   **URL:** IP of PXE server

    *   **Username:** username of PXE server

    *   **Password:** password of PXE server

    *   Pxe Server Type: PING

    *   **PING Storage IP:** IP of CIFS server

    *   **PING Directory:** Share/Ping_Backup

    *   **TFTP Directory:** The directory displayed by cloud-setup-baremetal earlier. For example, /tftpboot.

    *   **PING CIFS Username:** username of CIFS server (optional)

    *   **PING CIFS Password:** password of CIFS server (optional)

5. Click Add Network Device again. Input the following and click Save:

    *   **Type:** ExternalDhcp.

 June 27, 2011

- **URL:** IP of DHCP server. This is the same value you used for PXE server in the previous step.

- **Username:** username of DHCP server

- **Password:** password of DHCP server

- **DHCP Server Type:** Dhcpd

9.10 Add a Cluster, Host, and Firewall

Add the following entities to CloudStack using the Management Server UI.

1. Add a bare metal cluster as described in Add Cluster: Bare Metal on page 83, then return here for the next step.

2. Add one or more bare metal hosts as described in Add Hosts (Bare Metal) on page 84, then return here for the next step.

3. Add the firewall as described in Advanced Networking: Adding an External Firewall (optional) on page 77. Then continue to the next section, Add a Service Offering and Template.

9.11 Add a Service Offering and Template

This is the final phase of a bare metal installation and deployment.

1. Create a bare metal service offering. In the Management Server UI, click Configuration – Service Offering – Add Service Offering. In the dialog box, fill in these values:

   - **Name.** Any desired name for the service offering.

   - **Display.** Any desired display text.

   - Storage Type. Shared.

   - **# of CPU Cores.** Use the same value as when you added the host.

   - **CPU(in MHZ).** Use the same value as when you added the host.

   - **Memory(in MB).** Use the same value as when you added the host.

   - Offer HA? No.

   - **Tags.** large

   - Public? Yes.

2. Add a bare metal template as described in Creating a Bare Metal Template in the Administrator's Guide.

Your bare metal installation is complete! Now you can create a bare metal instance from the Instances screen of the UI.

If you want to allow inbound network traffic to the bare metal instances through public IPs, set up public IPs and a port forwarding rules. Follow the steps in How to Set Up Port Forwarding in the Administrator's Guide.

10 Management Server Installation

The Cloud.com Management Server download includes everything you need to get started, except MySQL. This includes the Cloud.com software as well as dependencies. This section describes installing one or more Management Servers with one instance of MySQL, which may be on a different node from the Management Servers. The procedure for the installation is:

1. Prepare the operating system for all Management Servers.

2. Install the first Management Server.

3. Install MySQL.

4. (optional) Install additional Management Servers to create a farm for high availability.

To simplify the installation procedure this document defines two separate installation procedures: one for installing a single Management Server and one for installing multiple Management Servers in a load balanced pool. This document assumes that, in the case of multiple Management Servers, MySQL will be installed on a separate node from the Management Servers.

10.1 Operating System and OS Preparation

The Cloud.com Management Server requires RHEL/CentOS 5.4 64 bit or later. You can download CentOS 64-bit via the following link: http://isoredirect.centos.org/centos/5/isos/x86_64/. The OS must be prepared to host the Management Server using the following steps.

Important: These steps should be done on all Management Servers.

Important: NTP is recommended.

1. Edit the /etc/hosts file to make sure that every Management Server has a fully-qualified host name that resolves to an IP address. Alternatively, you can do this through DNS.

2. Log in to your OS as root. All the following commands should be run as root.

3. Ensure that the SELINUX variable in /etc/selinux/config is set to permissive. This ensures that MySQL and the Management Server can run properly on system reboot.

4. Run the following command.

```
# setenforce permissive
```

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

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

10.2 Single Node Install (One 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 Multi-Node Install (Multiple Management Servers).

1. Install the CloudStack packages. You should have a file in the form of "CloudStack-NNNN.tar.gz". Untar the file and then run the install.sh script inside it:

```
# tar xzf CloudStack-2.2.0-1-centos.tar.gz
# cd CloudStack-2.2.0-1-centos
# ./install.sh
Setting up the temporary repository...
Cleaning Yum cache...
Loaded plugins: fastestmirror
11 metadata files removed
Welcome to the Cloud.com CloudStack Installer.  What would you like to do?

    M) Install the Management Server
    A) Install the Agent
    S) Install the Usage Monitor
    D) Install the database server
    Q) Quit

    > M
```

2. Choose "M" to install the Management Server software.

10.2.1 Single Node Database Install

1. Re-run install.sh and choose "D" to install MySQL.

```
# ./install.sh
Setting up the temporary repository...
Cleaning Yum cache...
Loaded plugins: fastestmirror
11 metadata files removed
Welcome to the Cloud.com CloudStack Installer.  What would you like to do?

    A) Install the Agent
    S) Install the Usage Monitor
    D) Install the database server
    U) Upgrade the CloudStack packages installed on this computer
    R) Stop any running CloudStack services and remove the CloudStack packages from
this computer
    Q) Quit

    > D
```

2. 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 2 Management Servers.

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=700
```

3. 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 for <password>.

```
# service mysqld start
# mysql –u root
mysql> SET PASSWORD = PASSWORD(<password>);
```

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

   a. In dbpassword, specify the password to be assigned to the cloud user. You can choose to provide no password.

   b. 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.

```
# cloud-setup-databases cloud:<dbpassword>@localhost --deploy-as=root:<password>
```

5. Configure the OS for the Management Server using the following command. This command will set up iptables, sudoers, and start the Management Server.

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

This completes the single node install for the Management Server and database. Continue with Prepare Secondary Storage.

10.3 Multi-Node Install (Multiple Management Servers)

This section describes installing multiple Management Servers and installing MySQL on a node separate from the Management Servers. If you have just completed the single node install, see Prepare Secondary Storage.

The procedure to install multiple management servers is:

1. Install the first Management Server

2. Install MySQL on a separate node (referred to as the Database Node, below)

3. Set up the MySQL database

4. Install additional Management Servers

10.3.1.1 Install the First Management Server

1. Install the CloudStack packages. You should have a file in the form of "CloudStack-NNNN.tar.gz". Untar the file and then run the install.sh script inside it:

```
# tar xzf CloudStack-2.2.0-1-centos.tar.gz
# cd CloudStack-2.2.0-1-centos
# ./install.sh
```

2. Choose "M" to install the Management Server software.

10.3.2 Install the Database

1. 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
```

 June 27, 2011

2. 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.

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
```

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

```
# service mysqld start
# mysql –u root
```

4. 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>);
```

5. To grant access privileges to remote users, run the following command from the mysql prompt:

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

6. Restart the MySQL service.

```
# service mysqld restart
```

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

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

8. 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
```

10.3.3 Database Replication (Optional)

The 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.

Important: These steps assume that this is a fresh install with no data in the master.

Important: Creating a replica is not a backup solution. You should develop a backup procedure for the MySQL data that is distinct from replication.

1. Edit my.cnf on the master and add the following in the [mysqld] section below datadir.

```
log_bin=mysql-bin
server_id=1
```

For server_id a common practice is to set it to the last octet of the server's IP address. It must be unique with respect to other servers. Restart the MySQL service:

```
# service mysqld restart
```

2. 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;
```

3. Leave the current MySQL session running.

4. In a new shell start a second MySQL session.

5. 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 |              |                  |
+------------------+----------+--------------+------------------+
```

6. Note the file and the position that are returned by your instance.

7. Exit from this session.

8. Complete the master setup. Returning to your first session on the master, release the locks and exit MySQL.

```
mysql> unlock tables;
```

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

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

10. 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
```

11. Restart MySQL.

```
# service mysqld restart
```

12. 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;
```

 June 27, 2011

13. Then start replication on the slave.

```
mysql> start slave;
```

14. Optionally, open port 3306 on the slave as was done on the master earlier.

Important: 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.

10.3.3.1 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 (via service cloud-management start)

10.3.4 Creating and Initializing the Database

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

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

    a. In dbpassword, specify the password to be assigned to the cloud user. You can choose to provide no password.

    b. In dbhost, provide the hostname of the database node.

    c. 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`.

    ```
    # cloud-setup-databases cloud:<dbpassword>@<dbhost> --deploy-as=root:<password>
    ```

    Best Practice: On RHEL and CentOS, SQL does not set a root password by default. It is very strongly recommended that you set a root password as a security precaution.

10.3.5 OS Configuration for the Management Server

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
```

10.3.6 Prepare and Start Additional Management Servers

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

Important: Be sure to configure a load balancer to the Management Servers as discussed in section 4.

1. Run these commands on each additional Management Server:

```
# tar xzf CloudStack-2.2.0-1-centos.tar.gz
# cd CloudStack-2.2.0-1-centos
# ./install.sh
```

2. Choose "M" to install the Management Server.

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

```
# cloud-setup-databases cloud:<dbpassword>@<dbhost>
```

4. Configure the OS and start the Management Server:

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

The Management Server on this node should now be running.

11 Prepare Secondary Storage

Secondary storage in all Zones must be seeded with a template that is used for system VMs such as the Virtual Router. For each Secondary storage server you will need to execute the following steps.

Important: The 2.1 series system VM template will not work on 2.2. You must use the 2.2 system VM template.

1. Mount secondary storage on to your Management Server. This example assumes the path on the secondary storage server is /nfs/share.

   ```
   # mount –t nfs servername:/nfs/share /mnt/secondary
   ```

2. Retrieve and decompress the system VM template. Run the script /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt, which is installed on the Management Server. Run this for each hypervisor type that you expect end users to run in this Zone. This will give the system maximum flexibility to run system virtual machines. This process will require approximately 10 GB of free space on the local file system each time it runs.

3. The command to run depends on hypervisor type.

4. For vSphere:

   ```
   # /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt –m
   /mnt/secondary -u http://download.cloud.com/releases/2.2.0/systemvm.ova -h vmware -
   F
   ```

5. For KVM:

   ```
   # /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt –m
   /mnt/secondary -u http://download.cloud.com/releases/2.2.0/systemvm.qcow2.bz2 -h
   kvm -F
   ```

6. For XenServer:

   ```
   # /usr/lib64/cloud/agent/scripts/storage/secondary/cloud-install-sys-tmplt –m
   /mnt/secondary -u http://download.cloud.com/releases/2.2.0/systemvm.vhd.bz2 -h
   xenserver -F
   ```

   Each one of these files is large. It may take 30 minutes or more to download and uncompress.

7. Unmount secondary storage when the script has finished.

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

Repeat these steps for each secondary storage server.
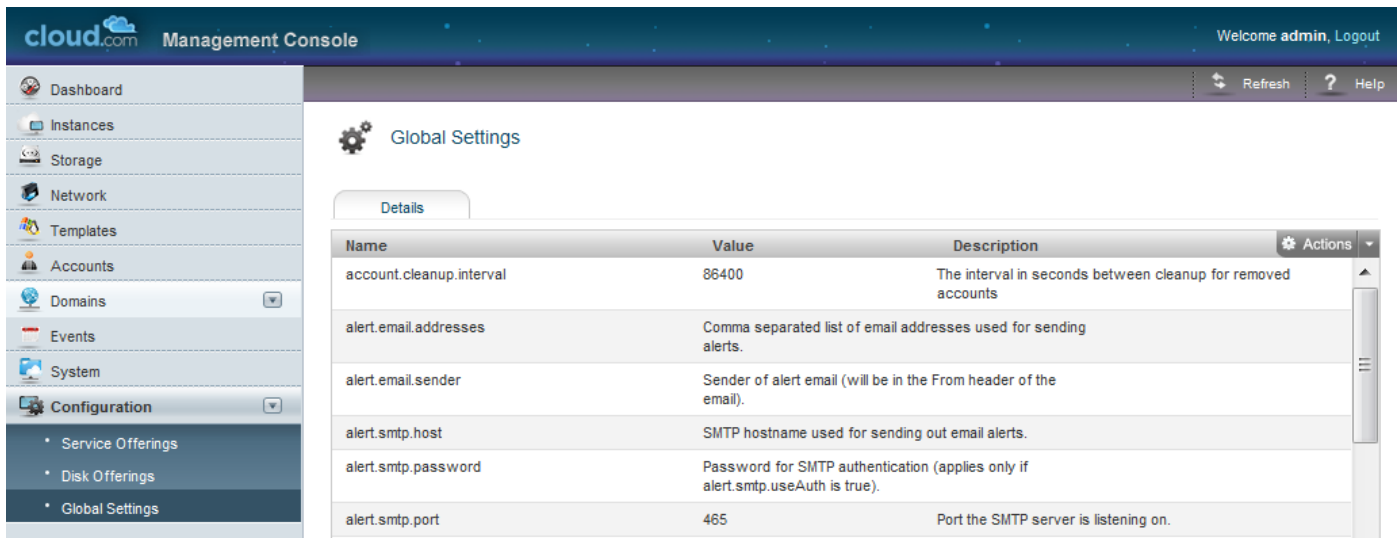
12 Describe Your Deployment

Now your Cloud.com Management Server is running. The next step is to tell it about the hosts, storage, and network configuration that you have done in the previous sections.

1. Log in to the administrator web UI.

    ```
    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. Using the left navigation tree, click on Configuration then Global Settings.

You **might** need to edit the following fields.

Field	Value
management.network.cidr	A CIDR that describes the network that the management CIDRs reside on. **This variable must be set for deployments that use vSphere.** It is recommended to be set for other deployments as well. Example: 192.168.3.0/24.
xen.public.network.device	For XenServer nodes, this is the device name with the name-label that was used for the public network. For example, "cloud-public". **This is applicable only if you have a second NIC for the public network.** In this case, set the value to the name-label used for the separate public network created in section 7.

 June 27, 2011

xen.private.network.device	For XenServer nodes, this is the device name with the name-label that was used for the public network. For example, "cloud-private".
kvm.public.network.device	For KVM nodes, this is the device that was used for the public network. For example, "cloudbr0".
kvm.private.network.device	For KVM nodes, this is the device that was used for the private network. For example, "cloudbr1".
xen.setup.multipath	For XenServer nodes, this is a true/false variable that instructs the 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 the CloudStack to enable multipath. If this is true for a NFS-based deployment multipath will still be enabled on the XenServer host. However, this does not impact NFS operation and is harmless.
secstorage.allowed.internal.sites	This is used to protect your internal network from rogue attempts to download arbitrary files using the template download feature. This is a comma-separated list of CIDRs. If a requested URL matches any of these CIDRs the Secondary Storage VM will use the private network interface to fetch the URL. Other URLs will go through the public interface. We suggest you set this to 1 or 2 hardened internal machines where you keep your templates. For example, set it to 192.168.1.66/32.
use.local.storage	This determines whether or not the CloudStack will use storage that is local to the Host for VHDs. By default the 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. **Important: local storage is available only for XenServer and vSphere. This setting has no effect on KVM.**
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.

vmware.guest.vswitch	The name of the vSwitch in vCenter that you want to carry the guest-guest traffic. Default is vSwitch0.
vmware.private.vswitch	The name of the vSwitch in vCenter that you want to carry the management and storage traffic. Default is vSwitch0.
vmware.public.vswitch	The name of the vSwitch in vCenter that you want to carry the traffic to/from the public internet. Default is vSwitch0.

There are additional configuration parameters that you may want to set. These are discussed in the Administration Guide. For an initial installation, they are not generally necessary.

3. If you changed any of these values you should restart the Management Server now.
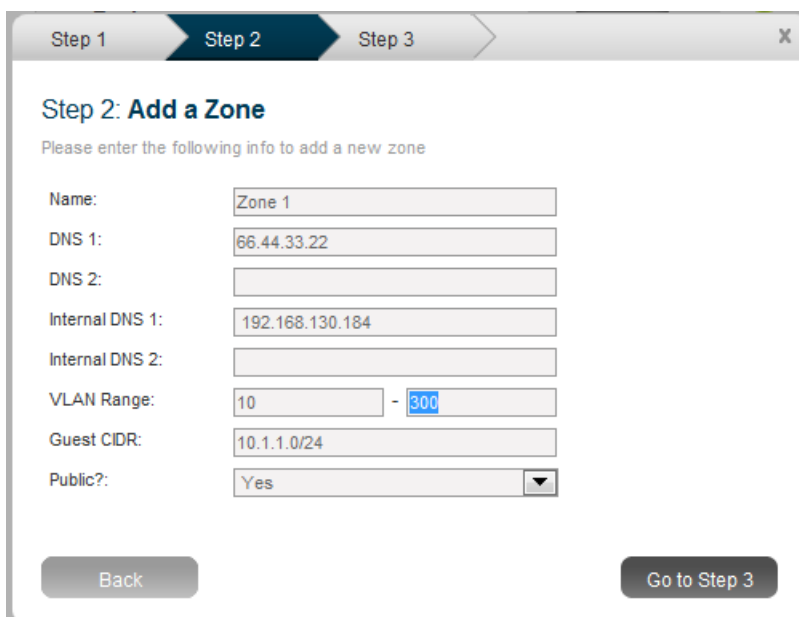
```
# service cloud-management restart
```

12.1 Add a New Zone

12.1.1 Adding a Zone and Pod

Begin by using these steps to edit the default Zone.

1. In the left navigation tree, choose System, then Physical Resources.

2. Click on the + next to the Zone to add a Zone. The Zone creation wizard will appear.

3. Choose your network type.

    a. Basic: this is for use with Direct Untagged networking.

    b. Advanced: this is for use with Direct Tagged or Virtual Networking.

4. Configure the Zone.

Important: CloudStack distinguishes between internal and public DNS. Internal DNS is assumed to be capable of resolving internal-only hostnames, such as your NFS server's DNS name. Public DNS is provided to the guest VMs for DNS resolution. You can enter the same DNS server for both types, but if you do so you must make sure that both private and public IP addresses can route to the DNS server. Note that you must provide at least one public DNS server and at least one Internal DNS server.

5. Enter the following details in the Add Zone dialog.
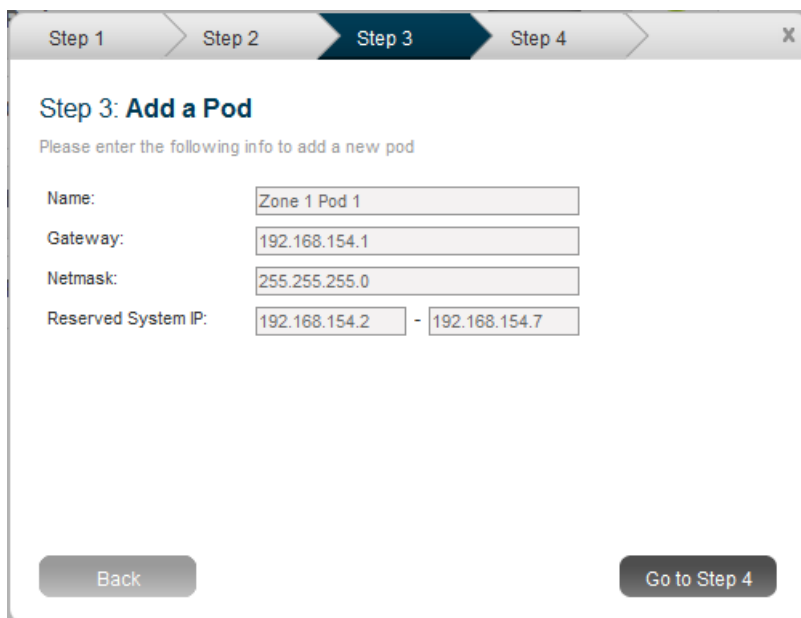
    - **Name**. The name of the Zone.

    - **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 2**. These are DNS servers for use by system VMs in the Zone. These DNS servers will be accessed via the private network interface of the System VMs. The private IP address you provide for the Pods must have a route to the DNS server named here.

    - **Zone VLAN Range (Advanced Only)**. This is the range of Zone VLANs that are used for provided VLANs to the guest networks. It is entered in the format "x-y". (E.g. 800-900). You should set the Zone VLAN fields based on your planned VLAN allocation.

    - **Guest CIDR (Advanced Only)**. 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 virtual networks in different Zones in the future.

      This field should be modified only if you are using Virtual Networking. The CloudStack uses it when VMs with Virtual Networking are created.

      Important: if using external firewall, see the external firewall section below.

    - **Public**. Choose if this Zone is public or not. A public Zone is available to all users. A non-public Zone will be assigned to a particular domain. Only users in that domain will be allowed to create Guests in this Zone.
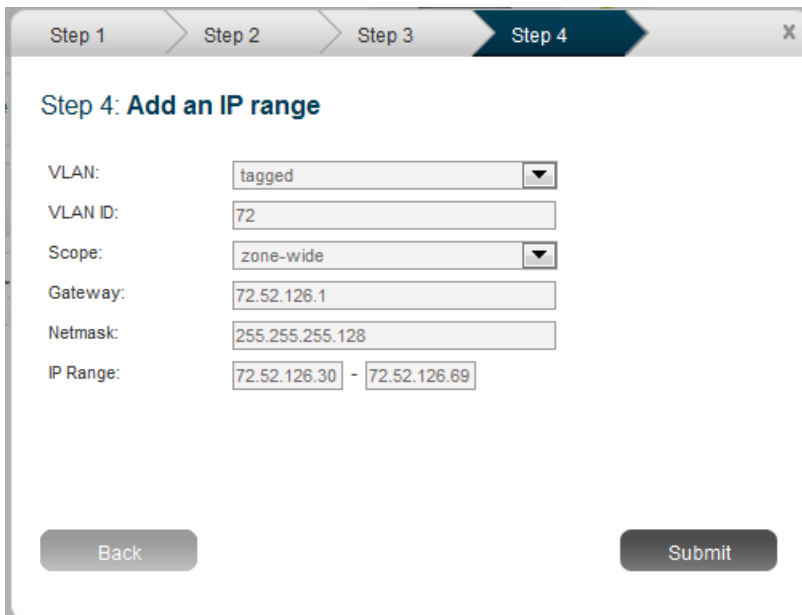
6. Add a Pod for the new Zone.

7. Enter the following details in the Add Pod dialog.

   - **Name**. The name of the Pod.

   - **Gateway**. The gateway for the hosts in that Pod.

   - **CIDR**. The CIDR that encompasses the subnet in the Pod.

   - **Reserved System IP**: This is the IP range in the private network that the CloudStack uses to manage Secondary Storage VMs and Console Proxy VMs. These IP addresses are taken from the same subnet as computing servers. You therefore need to make sure computing servers and Management Servers use IP addresses outside of this range. These two values combine to give the system control over a certain IP address range, and leave you in control of allocation for IP addresses in the CIDR but outside of the start and end range. In the screenshot we have start=192.168.154.2 and end=192.168.154.7. These computing servers and Management Servers can use IP addresses .8 to .254 and the CloudStack can use .2 to .7 for System VMs.

     The recommended number of private IPs per Pod is described in Private IP Addresses on page 20. The example above allocates ten IPs.

   - **Guest IP Range** (Basic Mode Only). The range of IP addresses that will be available for allocation to guests in this Pod. If one NIC is used these IPs should be in the same CIDR as the Pod CIDR. If multiple NICs are used they may be in a different subnet.

   - **Guest Netmask** (Basic Mode Only). The netmask in use on the subnet the guests will use.

   - **Guest Gateway** (Basic Mode Only). The gateway that the guests should use.

8. In Advanced Networking, add a Public IP Address Range. If you intend to use Virtual Networking (with our without Direct Networking) you should enter the range of public IPs you have reserved for assignment to Virtual Routers and System VMs. If you intend to use Direct Networking only, you should enter the initial VLAN for the system, whether it is for a specific account or Zone-wide.

9. Enter the following details in the Add IP Range dialog.

   - **VLAN (tagged or untagged)**. Choose whether you will be using a tagged VLAN for public network traffic or an untagged VLAN. You must choose tagged if you are using a single NIC for all traffic.

   - **VLAN ID**. The VLAN that will be used for public traffic if tagged VLAN was chosen.
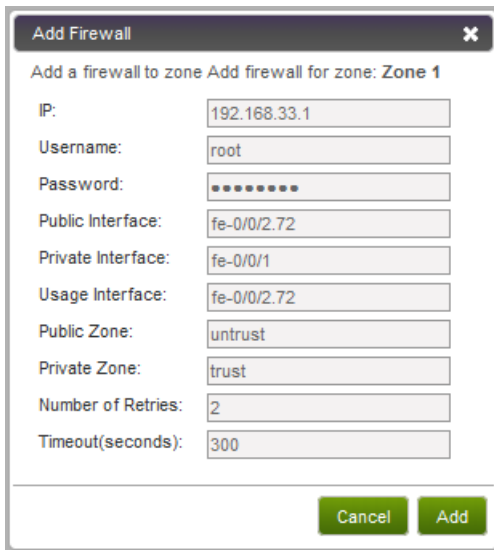
 June 27, 2011

- **Scope.** Choose if this is available to all accounts (Zone-wide) or is available for only one account (Account-specific). Almost all deployments should choose Zone-wide for the scope.

- **Gateway**. The gateway in use for these IP addresses.

- **Netmask**. The netmask associated with this IP range.

- **IP Range**. This takes a lower and an upper IP address that together form a range. These IP addresses are assumed to be accessible from the Internet and will be allocated for access to guest networks.

10. Click Submit on the dialog. Your first Zone and Pod are now added.

12.1.2 Advanced Networking: Adding an External Firewall (optional)

This step is required if you would like to add an external firewall device to the CloudStack. The Juniper SRX series is the only supported such device. In this procedure it is assumed you have already installed and configured the firewall. Before you can use it, you must add it to the CloudStack deployment.

1. Log in to the Management Server UI.

2. In the left navigation tree, choose System - Physical Resources, choose your Zone, then choose Network.

3. Click Add Firewall.

4. Input the following:

- **IP.** The IP address of the SRX.

- **Username.** The user name of the account on the SRX that the 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.

- **Public Zone.** The name of the public zone on the SRX. For example, trust.

- **Private Zone.** The name of the private zone on the SRX. For example, untrust.

- **Number of Retries.** The number of times to attempt a command on the SRX before failing. The default value is 1.

- **Timeout (seconds).** The time to wait for a command on the SRX before considering it failed. Default is 300 seconds.

5. Click Add.

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 the 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.
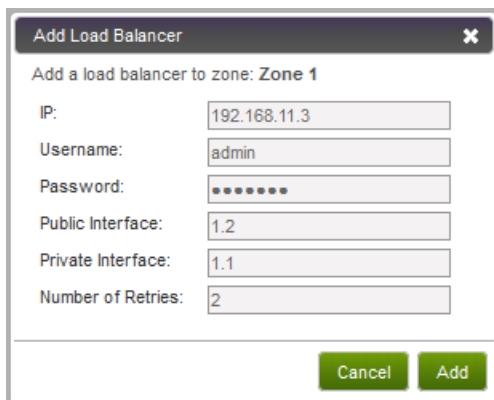
Use the following table to determine how to configure the CloudStack for your deployment.

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 that in the global configuration table as discussed in the first part of this section and restart the Management Server.

12.1.3 Advanced Networking: Adding an External Load Balancer (optional)

This step is required if you would like to add an external load balancer to the CloudStack. The BigIP F5 is the only supported external load balancing device. Add the BigIP via the UI. Go to Physical Resources -> (Select Zone) -> Network -> Add Load Balancer button.

 June 27, 2011

Parameters for this dialog include:

- **IP.** Enter the IP address of the F5.

- **User name**. Enter the user name of the account on the F5 that the CloudStack should use.

- **Password**. Enter the password of the user name above.

- **Public Interface.** Enter the name of the public interface on the F5.

- **Private Interface.** Enter the name of the private interface on the F5.

- **Number of Retries.** Number of times to attempt a command on the Load Balancer before considering the operation failed. Default is 1.

12.1.4 Additional Zones

You can add additional Zones as needed. If you choose to add additional Zones, be sure to repeat the installrtng.sh template seeding that you did for the first Zone.

12.1.5 Additional Pods

You can add additional Pods as needed now or after the system is up and running.

12.1.6 Advanced Networking: Additional Networks

The CloudStack allows the provisioning of networks in addition to the base virtual network that is always available. These networks may span the Zone and be available to all accounts or they may be scoped to a single account. Each such network requires a Direct VLAN and an IP Range; a gateway for the network is optional.
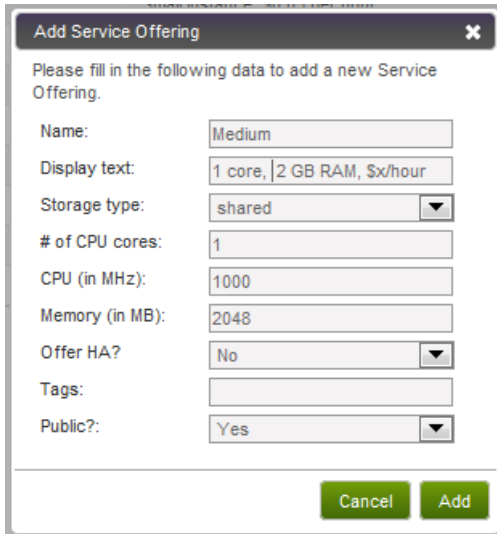
A network in the CloudStack is either eligible to the default network or ineligible to be the default network. A default network will be set as the default gateway for the guest using the DHCP response. Non-default networks will not be set to be the default gateway in the guest. Every guest must have exactly one default network. When multiple networks are present the user is required to first choose a default network. Then they are given the choice to add zero or more non-default networks to their guest. Each network on the guest will be implemented as a NIC in the guest.

Additional Networks may be added. This procedure is discussed in the Administration Guide.

12.2 Edit Service Offerings (Optional)

The service offering defines CPU and RAM for the guests. The CloudStack ships with several default service offerings. You can optionally use the following steps to edit these now or proceed with the defaults.

1. Go to the Configuration tab, and select the Service Offerings section.
2. Add or edit service offerings as needed. Select "Add Service Offering" to add one.

3. Provide the following information to define this service offering.

    *   **Name**. Any desired name for the service offering.

    *   **Display text**. A short description of the offering.

    *   **Storage type**. The type of disk that should be allocated to the guest. Local allocates from storage attached to XenServer directly. Shared allocates from storage accessible via NFS.

    *   **# of CPU cores**. The number of cores which should be allocated to an instance with this offering.

    *   **CPU (in MHz)**. The CPU speed of the cores that the instance is allocated. For example, "2000" would provide for a 2 GHz clock.

    *   **Memory (in MB)**. The amount of memory in megabytes that the instance should be allocated. For example, "2048" would provide for a 2 GB RAM allocation.

    *   **Offer HA**. If yes, the user will be able to choose a VM to be monitored and as highly available as possible.

    *   **Tags**. The tags that should be associated with the primary storage for this root disk.

    *   **Public**. Should the service offering be available all domains or only some domains. Chooes Yes to make it available to all domains. Choose No to limit the scope to a subdomain; the CloudStack will then prompt for the subdomain's name.

12.3 Edit Disk Offerings (Optional)

The disk offering defines the size and characteristics of data disks attached to the guests. The CloudStack ships with several default disk offerings.

1. Go to the Configuration tab, and select the Disk Offerings section. This is located next to the Zones section.

2. Add or edit disk offerings as needed. Select "Add Disk Offering" to add one.

 June 27, 2011

3.   Provide the following information to define this disk offering.

- **Name**. Name of the disk offering (E.g. extra large)

- **Description**. A short description of the disk offering

- **Disk size (in GB)**. The size of the disk offering in GB (E.g. 10 is a 10 GB offering)

- **Tags**. Tags are a comma separated list of attributes of the storage. For example "ssd,blue". Tags are optional. They are also added on Primary Storage. The CloudStack matches tags on a disk offering to tags on the storage. If a tag is present on a disk offering that tag (or tags) must also be present on Primary Storage for the volume to be provisioned. If no such primary storage exists allocation from the disk offering will fail.

12.4 Add Cluster

Now that the offerings are defined, you need to tell the CloudStack about the hosts that it should manage.   You can add hosts by themselves or in the case of VMware add an existing cluster (as configured in vCenter).

A Cluster is a XenServer server pool, a set of KVM servers, or a VMware vCenter cluster. Within a Cluster the Hosts may live migrate VMs to and from each other, and all access the same shared storage. We expect that most deployments will have a single Cluster per Pod, although the CloudStack supports multiple Clusters per Pod.

Most deployments will want to use clusters of more than one host because of the benefits of live migration. However, you may create a cluster with only one host.

12.4.1 Add Cluster: KVM and XenServer

To add a Cluster to a Pod for KVM and XenServer:

1.   Navigate to System -> Physical Resources -> (Select Zone) -> (Select Pod).

2.   Choose "Add Cluster" in the upper left.

3.   The Add Cluster dialog will appear.

4. Choose the hypervisor type for this Cluster.

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

6. Complete the addition by clicking "Add".

12.4.2 Add Cluster: vSphere

For vSphere servers we recommend creating the cluster in vCenter and then adding the entire cluster to the CloudStack. Following that recommendation:

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.
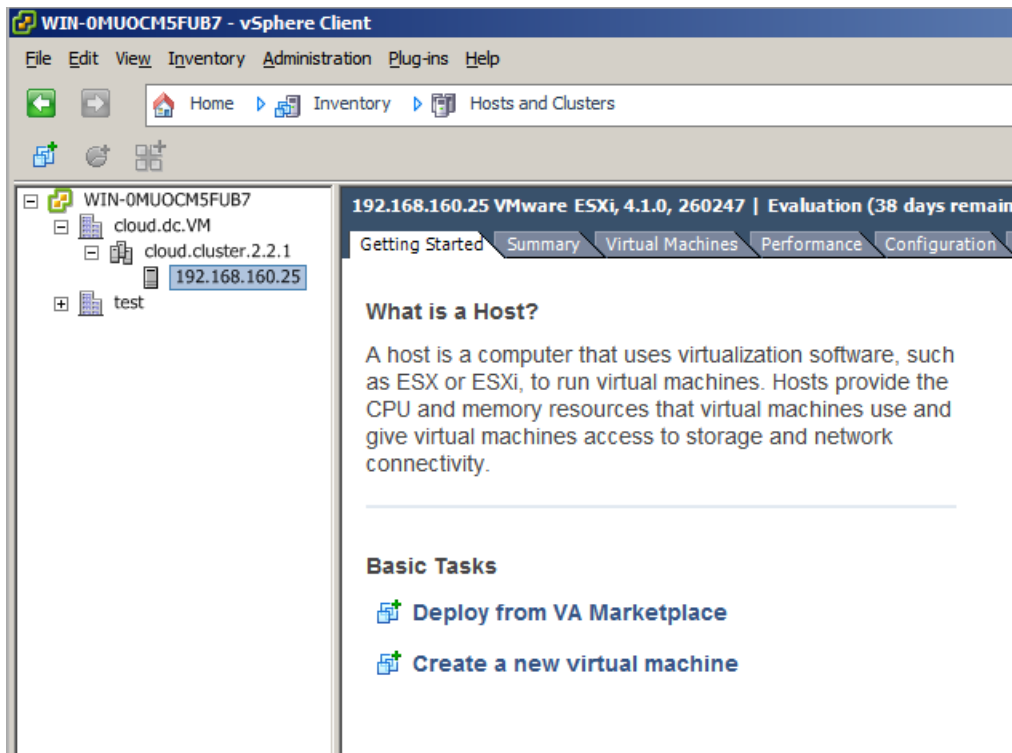
2. Go to System -> Physical Resources -> (Select Zone) -> (Select Pod) -> Add Cluster. The Add Cluster dialog displays.
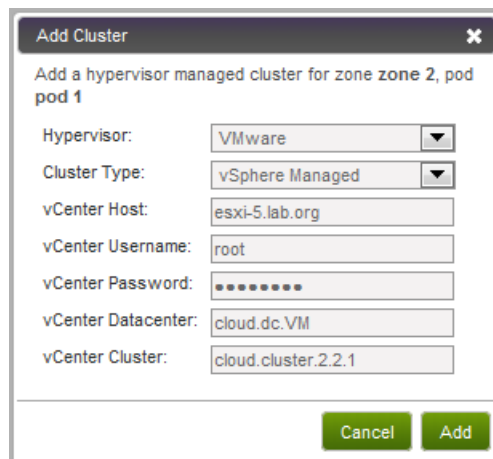
3. Provide the following information in the Add New Computing Host dialog. The fields below make reference to values from vCenter as shown in

- **Hypervisor**. Choose VMware.

- **Cluster Type**. Choose vSphere Managed.

- **vCenter Server**. Enter the hostname or IP address of the vCenter server.

- **vCenter Username**. Enter the username that the 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".

- **vCenter Cluster**. Enter the name of the cluster you created in vCenter. For example, "cloud.cluster.2.2.1"

It may take a minute for the cluster to be provisioned. It will automatically display in the UI.

12.4.3 Add Cluster: Bare Metal

To add a Cluster to a Pod for bare metal hosts:

1. Before you can add a bare metal Cluster, you must have performed several other installation and setup steps to create a bare metal environment. See Bare Metal Installation on page 56.

2. Navigate to System -> Physical Resources -> (Select Zone) -> (Select Pod).

3. Choose "Add Cluster" in the upper left.
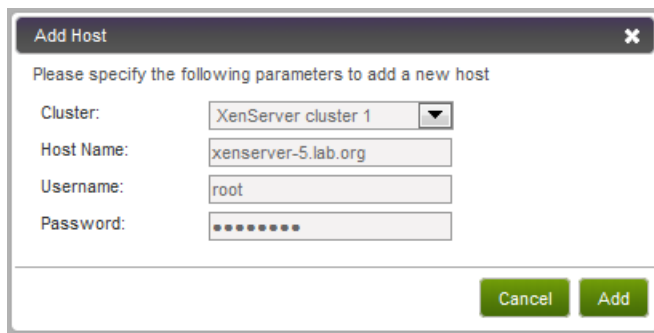
4. The Add Cluster dialog will appear.
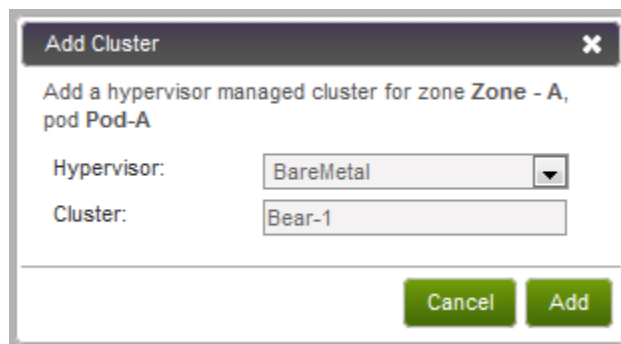
5. In Hypervisor, choose BareMetal.

6. In Cluster, enter a name for the Cluster. This can be any text you like.

7. Click Add.

12.5 Add Hosts (KVM and XenServer)

KVM and XenServer hosts can be added to a Cluster as discussed previously. To add a Host follow these steps:

1. Go to System -> Physical Resources -> Zone -> Pod -> Add Host. The Add Host dialog displays.

2. Provide the following information in the Add Host dialog.

- **Hypervisor**. The Hypervisor type for this Host.

- **Cluster**. The Cluster to which this host will be added. If you skipped adding a Cluster then this dropdown will show "", which will cause the Host to add as a Standalone host.

- **Host Name**. For Xen and KVM this is the DNS name or IP address of the XenServer host or KVM host.

- **Username**. Usually the root user.

- **Password**. This is the password for the user named above (from your Citrix XenServer or KVM install).

It may take a minute for the host to be provisioned. It should automatically display in the UI.

Repeat for additional Hosts.

12.6 Add Hosts (Bare Metal)

To add a bare metal Host follow these steps:

1. Before you can add a bare metal Host, you must have performed several other installation and setup steps to create a bare metal cluster and environment. See Bare Metal Installation on page 56.

2. Go to System -> Physical Resources -> Zone -> Pod -> Add Host.

3. Provide the following information in the Add Host dialog.

- **Hypervisor**. Choose BareMetal.

- **Cluster**. The Cluster to which this host will be added. Give the name of a bare metal cluster that you created earlier (see Add Cluster: Bare Metal on page 83).

- **Host Name**. The IPMI IP address of the machine.

- **Username**. User name you set for IPMI.

- **Password**. Password you set for IPMI.

- **# of CPU Cores**. Number of CPUs on the machine.

- **CPU(in MHZ).** Frequency of CPU.

- **Memory(in MB).** Memory capacity of the new host.

- **Host MAC.** MAC address of the PXE NIC.

- **Tags.** Set to large. You will use this tag later when you create the service offering.

It may take a minute for the host to be provisioned. It should automatically display in the UI.

 June 27, 2011

Repeat for additional bare metal Hosts.

12.7 Add Primary Storage

Next you will need to tell the system about the primary and secondary storage devices that are available. You can add multiple primary storage servers to a Cluster. At least one is required. If you intend to use only local disk for your installation, you can skip to Add Secondary Storage on page 86.

> **Important: Primary storage cannot be added until a Host has been added to the Cluster.**
>
> **Important: if you do not provision shared storage for primary storage, you will not be able to create additional volumes (via Storage > Volumes > Add Volume). Also, if you do not provision shared primary storage, you must have set system.vm.local.storage.required to true in the first part of this section or else you will not be able to start VMs.**

1. To display the CloudStack cluster to which you want to add storage, click System, then click the triangles to expand Physical Resources, then the desired Zone, Pod, and Cluster.
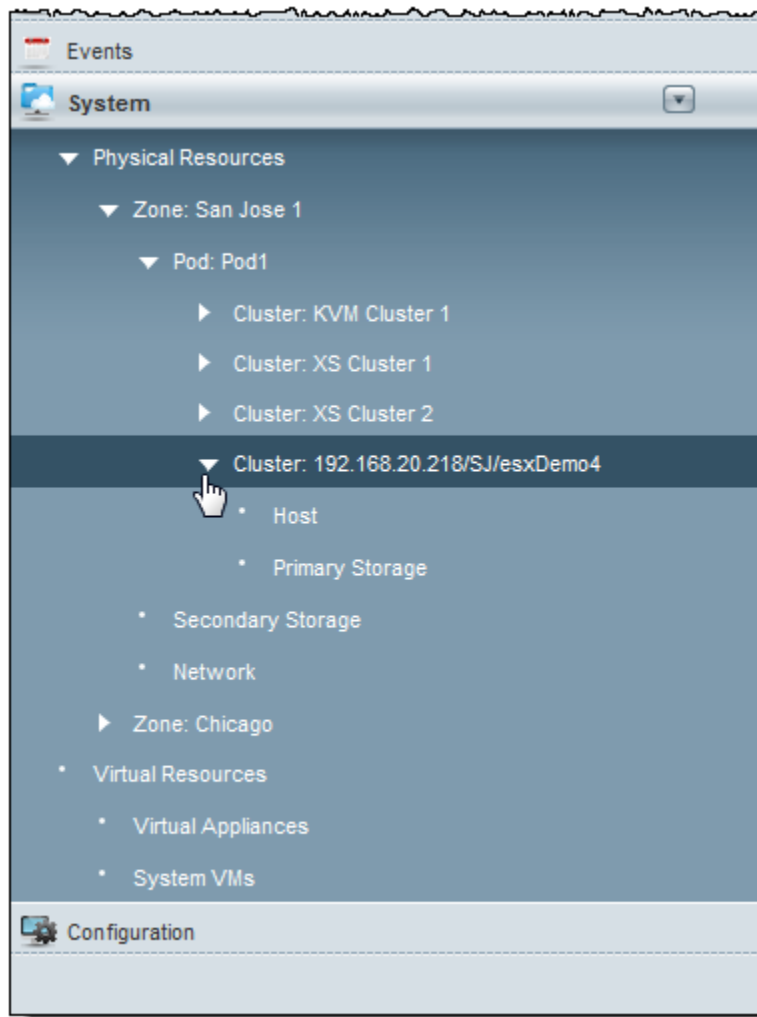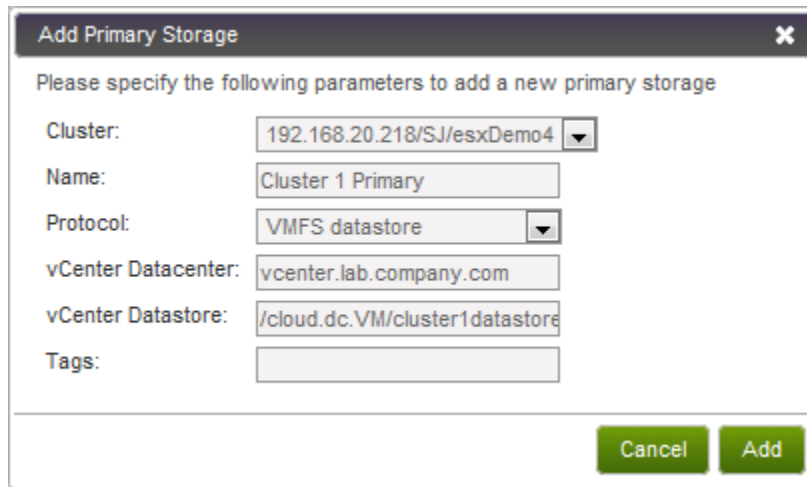

2. Click Add Primary Storage.
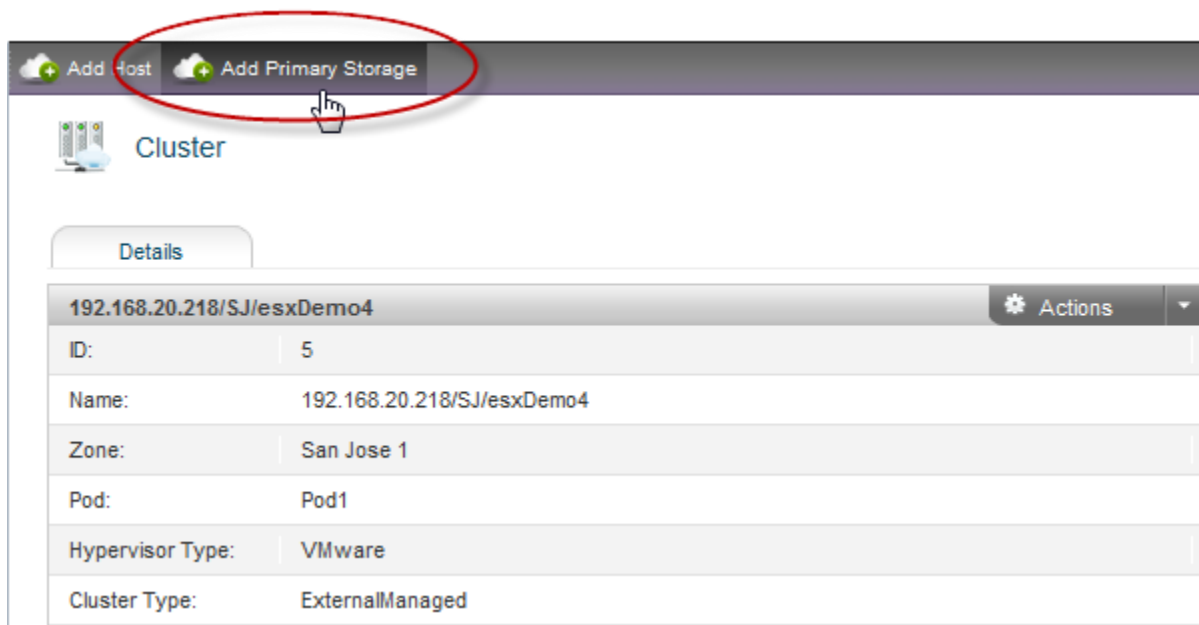
The Add Primary Storage dialog displays.

3. Provide the following information in the Add Primary Storage dialog. The information required varies depending on your choice in Protocol.

- **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 setup outside the 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**. 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. It is an optional field and may be left blank.

- **IMPORTANT**: 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.

Here are some sample dialogs.

Figure 5 Adding VMFS Primary Storage

Figure 6 Adding Primary Storage That Was Set Up Manually (PreSetup)
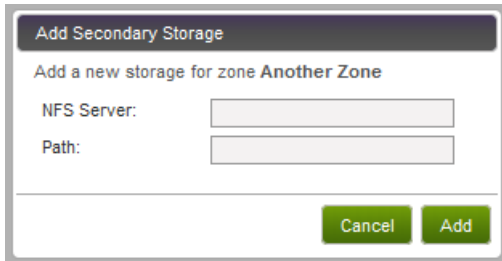
4. Click Add.

12.8 Add Secondary Storage

You will need to add secondary storage.   Secondary Storage is used to store templates, ISOs, and snapshots.

Important: Secondary Storage is always accessed via NFS.

1. Navigate to the Zone you are building. Choose System -> Physical Resources and then click on your Zone.

2. Select "Add Secondary Storage".

3. Provide the details for Secondary Storage server:

    -   **Server**. The IP address of the server.

    -   **Path**. The exported path from the server.

4. Repeat these steps to add more Secondary Storage servers to the zone.

12.9 SSL

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

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

13 Initialization and Testing

You should have one Java process running the Cloud.com software on each Management Server. This is the Management Server process.

After everything is configured the CloudStack will perform its initialization. This can take 30 minutes or more depending on the speed of your network. During this initialization process several things happen:

- The CloudStack will start the Secondary Storage VM and Console Proxy VM from the system VM template downloaded into each Zone. In the System Section, Virtual Resources, System VMs section you will see the status of these VMs listed first as Creating, then as Starting, then as Running. You can click on Refresh is the upper right to update the status.

- After the Secondary Storage VM is running the Management Server will initiate downloads of the CentOS templates. One is downloaded for each hypervisor type. The Management Server requests that the Secondary Storage VM perform this download. You can go to the Templates tab to check the status of this download. Go to Templates then My Templates when logged in as admin. The status will show "Storage agent or storage VM disconnected" until the Secondary Storage VM is running. Then the status will change to show that the download is in progress. You can click Refresh to update the download percentages.

- Once the CentOS templates are downloaded they will be uncompressed by the Secondary Storage VM. This is a large file and this operation will take several minutes. The Management Server will then update each template's status to Ready.

If these steps do not work you should see the Troubleshooting section below, or contact support for assistance.

Important: If these steps do not work further testing will not be successful. You must resolve the above issues before proceeding.

Once the CloudStack has performed initialization, use the following steps to try creating a new virtual machine.

1. Create a new user account. Click on Accounts and then My Accounts. Click "Add Account" at the top.

   This tool allows you to create end user accounts, domain administrators, and global administrators, as well new domains. Follow the steps to create a new user.

2. Optionally logout and login as the new user. To log in as an end user account, go to http://<ManagementServerHostOrIP>:8080/client. This URL displays the end user UI or the admin UI based on the access level of the authenticated account.

3. Go to the Instances tab. Click on My Instances.

4. Click Add Instance and follow the steps in the wizard.

   a. The template selection screen requires selecting a template. At this point you likely have only the provided CentOS template available.

   b. Select a service offering. Be sure that the hardware you have allows starting the selected service offering.

   c. Add any additional "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.

   d. Choose the primary network for the guest. Most likely you have only one option here. But if you entered additional networks as in the direct tagged case you may have more than one option. You must pick exactly one.

   e. Optionally give your VM a name and a group. The group is text that may be whatever you would like. Click Submit and your VM will be created and started.

If you decide to grow your deployment, you can add more Hosts, Primary Storage, Zones, Pods, and Clusters. As needed, repeat the procedures in Describe Your Deployment starting on page 72.

Cloud.com CloudStack 2.2.8 Installation Guide

14 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.

Important: 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.

Use the following steps to install the Usage Server.

1. Run ./install.sh.

```
# ./install.sh
Setting up the temporary repository...
Cleaning Yum cache...
Loaded plugins: fastestmirror
11 metadata files removed
Welcome to the Cloud.com CloudStack Installer.  What would you like to do?

    A) Install the Agent
    S) Install the Usage Monitor
    U) Upgrade the CloudStack packages installed on this computer
    R) Stop any running CloudStack services and remove the CloudStack packages from
this computer
    E) Remove the MySQL server (will not remove the MySQL databases)
    Q) Quit

    > S
```

2. Choose "S" to install the Usage Server.

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.

 June 27, 2011

15 Troubleshooting

A quick step to look for errors in the management server log is this:

```
# grep -i -E 'exc|unable|fail|invalid|leak|invalid|warn'
/var/log/cloud/management/management-server.log
```

15.1 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.

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.

Important: 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.

15.1.1 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 System -> 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 Host using your known user and password.

4. ssh into the private IP of the SSVM with the following.

   ```
   # ssh -i /root/.ssh/id_rsa.cloud -p 3922 root@private-ip
   ```

5. 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.

15.1.2 Checking the Log File

You can also check the log file /var/log/cloud/cloud.log for any error messages.

15.2 VLAN Issues

A common installation issue is that your VLANs are not set up correctly. They are not trunked into every host in the Zone.

15.3 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 these things:

- 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

15.4 Troubleshooting Bare Metal Instances

Symptom

Creating an instance from a bare metal template results in an endless loop.

Cause

If PXE is first in the boot order, the host gets stuck in an infinite PXE boot loop when creating an instance from the CloudStack UI.

Solution

Make sure hard disk is the preferred boot option. See Enable PXE on the Bare Metal Host on page 60.

 June 27, 2011

16 Contacting Support

Cloud.com support is available to help you plan and execute your installation. The support team is available at support@cloud.com or via the support portal at http://cloud.com/community/support.