Cloud.com CloudStack Administration Guide

Version 2.1

July 19, 2010

© 2010 Cloud.com Inc. All rights reserved. Specifications are subject to change without notice. The Cloud.com logo, Cloud.com, Hypervisor Attached Storage, HAS, Hypervisor Aware Network, HAN, and VMSync are trademarks or registered trademarks of Cloud.com, Inc. All other brands or products are trademarks or registered trademarks of their respective holders.

Contents

[1 About the CloudStack 7](#_Toc266745774)

[1.1 Service Offerings, Disk Offerings, and Templates 7](#_Toc266745775)

[1.2 Accounts and Domains 7](#_Toc266745776)

[1.3 Server Types 7](#_Toc266745777)

[1.3.1 Management Server 7](#_Toc266745778)

[1.3.2 Computing Nodes 8](#_Toc266745779)

[1.4 Networking Features and Virtualization 8](#_Toc266745780)

[1.5 Storage Features and Virtualization 9](#_Toc266745781)

[1.6 Administrator Controlled Allocation 9](#_Toc266745782)

[1.7 Guest VM Management 10](#_Toc266745783)

[1.8 Manageability 10](#_Toc266745784)

[1.9 API and Extensibility 10](#_Toc266745785)

[1.10 Scalability and Availability 10](#_Toc266745786)

[2 Selecting Hardware and Software 11](#_Toc266745787)

[2.1 Computing Nodes 11](#_Toc266745788)

[2.2 Management Servers 11](#_Toc266745789)

[2.3 Storage 11](#_Toc266745790)

[2.4 Network 11](#_Toc266745791)

[2.5 Hypervisor Support 11](#_Toc266745792)

[2.6 Guest OS and Software Support 12](#_Toc266745793)

[3 Planning a Deployment 13](#_Toc266745794)

[3.1 Management Server Farm 13](#_Toc266745795)

[3.2 Scaling Concepts 13](#_Toc266745796)

[3.2.1 Computing Nodes 13](#_Toc266745797)

[3.2.2 Clusters 13](#_Toc266745798)

[3.2.3 Pods 14](#_Toc266745799)

[3.2.4 Availability Zones 14](#_Toc266745800)

[3.3 Multi-Site Deployment 14](#_Toc266745801)

[4 Defining Your Service Offering 16](#_Toc266745802)

[5 Understanding Network Types and Network Virtualization 17](#_Toc266745803)

[5.1 Guest Network 17](#_Toc266745804)

[5.2 Network Virtualization within One Pod 18](#_Toc266745805)

[5.3 Network Virtualization within One Availability Zone 19](#_Toc266745806)

[5.4 Types of Network Virtualization 21](#_Toc266745807)

[5.4.1 Software-based Network Virtualization 21](#_Toc266745808)

[5.4.2 Hardware-based Network Virtualization 21](#_Toc266745809)

[5.5 Private Address Allocation 22](#_Toc266745810)

[5.6 Public Address Allocation 22](#_Toc266745811)

[6 Storage Features and Types 23](#_Toc266745812)

[6.1 Primary Storage 23](#_Toc266745813)

[6.1.1 Tags 23](#_Toc266745814)

[6.2 Secondary Storage 24](#_Toc266745815)

[6.3 Working with Volumes 24](#_Toc266745816)

[6.4 Working with ISO Images 24](#_Toc266745817)

[6.5 Working with Blank VMs 24](#_Toc266745818)

[6.6 Working with Templates 24](#_Toc266745819)

[6.6.1 The Default Template 24](#_Toc266745820)

[6.6.2 Creating Templates 25](#_Toc266745821)

[6.6.3 Running Sysprep for Windows Templates 26](#_Toc266745822)

[6.6.4 Importing AMI’s 30](#_Toc266745823)

[6.6.5 Adding Password Management to Your Templates 33](#_Toc266745824)

[6.6.6 Uploading Templates 33](#_Toc266745825)

[6.6.7 Public Templates 33](#_Toc266745826)

[6.6.8 Private Templates 34](#_Toc266745827)

[6.6.9 Published Templates 34](#_Toc266745828)

[6.6.10 Deleting Templates 34](#_Toc266745829)

[6.7 Working with Snapshots (Service Provider and Enterprise Editions) 34](#_Toc266745830)

[6.7.1 Automatic Snapshot Creation and Retention 34](#_Toc266745831)

[6.7.2 Incremental Snapshots and Backup 34](#_Toc266745832)

[6.7.3 Volume Status 35](#_Toc266745833)

[6.7.4 Snapshot Restore 35](#_Toc266745834)

[6.7.5 Performance Considerations 35](#_Toc266745835)

[7 Network Features 36](#_Toc266745836)

[7.1 Guest Virtual Networks 36](#_Toc266745837)

[7.2 IP Forwarding and Firewalling 36](#_Toc266745838)

[7.3 IP Load Balancing 36](#_Toc266745839)

[7.4 Port Forwards 36](#_Toc266745840)

[7.5 DNS and DHCP 36](#_Toc266745841)

[8 Working with System Virtual Machines 37](#_Toc266745842)

[8.1 Console Proxy (Premium Edition only) 37](#_Toc266745843)

[8.2 Virtual Router 37](#_Toc266745844)

[8.3 Secondary Storage VM (Premium Edition Only) 37](#_Toc266745845)

[9 System Reliability and HA 38](#_Toc266745846)

[9.1 Management Server 38](#_Toc266745847)

[9.2 Computing Node 38](#_Toc266745848)

[9.3 Primary Storage Outage and Data Loss 38](#_Toc266745849)

[9.4 Secondary Storage Outage and Data Loss 38](#_Toc266745850)

[9.5 HA-Enabled VM (Service Provider and Enterprise Edition) 38](#_Toc266745851)

[10 Management Features 40](#_Toc266745852)

[10.1 Users, Administrators, and Domains 40](#_Toc266745853)

[10.1.1 Root Administrators 40](#_Toc266745854)

[10.1.2 Domain Administrators 40](#_Toc266745855)

[10.2 Provisioning 40](#_Toc266745856)

[10.2.1 Register 40](#_Toc266745857)

[10.3 VM Lifecycle Management 40](#_Toc266745858)

[10.3.1 VM Creation 40](#_Toc266745859)

[10.3.2 VM Deletion 40](#_Toc266745860)

[10.3.3 VM Lifecycle 41](#_Toc266745861)

[10.3.4 Remote Access 41](#_Toc266745862)

[10.4 PV Drivers 41](#_Toc266745863)

[10.5 Administrator Alerts 42](#_Toc266745864)

[10.6 Event Logs 42](#_Toc266745865)

[10.7 Working with Server Logs 43](#_Toc266745866)

[10.8 Limits 43](#_Toc266745867)

[10.8.1 Configuration Limits 43](#_Toc266745868)

[10.8.2 ROOT Domain Limits 43](#_Toc266745869)

[11 Working with Computing Nodes 45](#_Toc266745870)

[11.1 Adding Computing Nodes with Community Edition 45](#_Toc266745871)

[11.2 Adding Computing Nodes with Service Provider and Enterprise Edition 45](#_Toc266745872)

[11.3 Scheduled Maintenance and Maintenance Mode 45](#_Toc266745873)

[11.4 Removing Computing Nodes 45](#_Toc266745874)

[11.5 Computing Node Allocation 45](#_Toc266745875)

[11.5.1 OS Preferences 45](#_Toc266745876)

[11.5.2 Over-Provisioning 45](#_Toc266745877)

[12 Working with Usage 46](#_Toc266745878)

[13 User Interface and API 47](#_Toc266745879)

[13.1 User Interface 47](#_Toc266745880)

[13.1.1 Admin User Interface 47](#_Toc266745881)

[13.1.2 End User Interface 47](#_Toc266745882)

[13.2 API 47](#_Toc266745883)

[13.2.1 Provisioning and Authentication API 48](#_Toc266745884)

[13.2.2 Allocators 48](#_Toc266745885)

[13.2.3 User Data and Meta Data 48](#_Toc266745886)

[14 Appendix A—Time Zones 49](#_Toc266745887)

# About the CloudStack

The Cloud.com™ CloudStack™ platform is a complete software suite used to create Infrastructure as a Service (IaaS) clouds. Target customers include service providers and enterprises.

* The Cloud.com CloudStack platform enables service providers to set up an on-demand, elastic cloud computing service that competes with the Amazon EC2™ service. It enables a utility computing service by allowing service providers to sell self‑service virtual machine instances over the Internet.
* The Cloud.com CloudStack platform enables enterprises to set up an on-premise private cloud for use by their own employees. The current generation of virtualization infrastructure shipped by VMware®, Citrix®, and Microsoft® targets enterprise IT departments who manage virtual machines in the same way as they would manage physical machines. The Cloud.com CloudStack platform, on the other hand, enables self service of virtual machines by users outside of IT departments.

The Cloud.com CloudStack platform includes the Management Server and extensions to industry-standard hypervisor software (E.g. XenServer®, VMware, KVM) installed on Computing Nodes running in the cloud. The Management Server is deployed on a farm of management servers. The administrator provisions resources (Computing Nodes, storage devices, IP addresses, etc.) into the Management Server and the Management Server manages those resources. The Management server presents web interfaces to end users and administrators that enable them to take actions on some or all of their instances in the IaaS cloud.

## Service Offerings, Disk Offerings, and Templates

The CloudStack platform allows the administrator to define Service Offerings and Disk Offerings. These allow the administrator to define the virtual hardware (CPU speed and count, RAM size, and disk size) that the user can select when creating a new instance.

The administrator can also provision templates in the system. Templates are the base OS images that the user can select when creating a new instance. For example, the CloudStack platform includes CentOS 5.3 as a template. All popular Linux and Windows OS versions are supported.

## Accounts and Domains

CloudStack platform users are assigned accounts. An account is typically a customer of the service provider or a department in a large organization. Accounts are the unit of isolation in the cloud. Accounts are grouped by domains. Domains usually contain accounts that have some logical relationship to each other and a set of delegated administrators with some authority over the domain and its subdomains. For example, a service provider with several resellers could create a domain for each reseller.

## Server Types

There are two required types of servers in the CloudStack platform: Management Servers and Computing Nodes.

### Management Server

The CloudStack Management Server runs in a Tomcat container and requires MySQL for persistence. The MySQL database required by the Management Server may optionally be placed on a separate system from the Management Server itself. This type of server is called a “Database Server”. Replication is also supported.

The Management Server:

* Provides the web user interfaces for the administrator and end users.
* Provides the APIs for the CloudStack platform.
* Manages the assignment of guest VMs to particular Computing Nodes.
* Manages the assignment of public and private IP addresses to particular accounts.
* Manages the allocation of storage to guests’ virtual disk images.
* Manages snapshots, templates, and ISO images, possibly replicating them across data centers.
* Provides a single point of configuration for the cloud.

### Computing Nodes

Computing Nodes are the resource in the cloud that hosts the guest virtual machines. For example, a Linux KVM-enabled host and a Citrix XenServer host are Computing Nodes.

Computing Nodes:

* Provide all the CPU, memory, storage, and networking resources needed to host the virtual machines.
* Interconnect using a high bandwidth TCP/IP network and connect to the Internet.
* May reside in multiple data centers across different geographic locations.
* May have different capacities (E.g. Different CPU speeds, different amounts of RAM, etc.).
* Are high-quality commodity hardware, ;and are reliable individually, but can fail frequently when a large number of servers are involved.

## Networking Features and Virtualization

The CloudStack platform manages the allocation of private, direct, and public IP addresses. The administrator configures the system with available public, direct, and private IP addresses. There are two primary types of networks that can be created: "Direct Attached" and "Virtual".

### Direct Attached Networking

With Direct Attached networks the guest VMs are directly assigned IP addresses on the local subnet. They access the internet directly, and are not NATed by any components of the CloudStack. Their packets do not travel through a virtual router. Consequently they cannot take advantage of software load balancing, firewalling, and port forwarding features in the CloudStack.

Direct Attached guests may be isolated from other Direct Attached guests or not. With "Tagged Direct", the administrator assigns a specific Zone-wide VLAN ID and IP range to an account. Direct Attached guests created by that account use that VLAN for guest-guest traffic and are isolated from other accounts' guests. Direct Attached guests receive their IP address from the virtual router, whose function is only for DHCP in this case. Tagged Direct is useful for linking guests with other systems, such as managed servers.

Untagged direct networking is a Pod-level concept. In this model there is no isolation. The guests can receive their IP addresses from an external DHCP server or a CloudStack virtual router. Untagged Direct is useful for private cloud deployments where account security is not a concern.

### Virtual Networking

With Virtual Networking, the virtual router acts as a firewall for all guests of an account. Every account is assigned a virtual router. All public IP addresses acquired by the account are assigned to the virtual router. The virtual router is a system-owned VM that provides a hardened barrier between the guest VMs and the Internet. The virtual router is the gateway for guest VM traffic to and from the Internet, and it provides DNS and DHCP services to the guests. It also NATs all Internet traffic. The virtual router’s presence in traffic enables the CloudStack platform to present several networking features to the end user. The virtual router can be configured by the user to port forward traffic from a public IP to a port on a particular guest VM. The port’s traffic can also be load balanced across multiple guest VMs, providing for increased availability of a service behind the public IP address.

Inter-guest traffic travels via a zone-wide VLAN and not through the virtual router. The use of VLANs provides isolation: the guests of different accounts are on different VLANs.

In this style of networking every account is given an initial public IP address. The user may acquire additional public IP addresses. Public IP addresses are routable from the Internet.

### Combining Virtual Networking and Direct Attached Networking

A single account may have guest VMs that have virtual networking and guest VMs that have tagged, direct attached networking. In this case there are two virtual routers for the account. One virtual router is responsible for the Zone VLAN used for the guests; the second virtual router is responsible for the tagged, direct attached VLAN assigned to the account.

Untagged, direct attached guests may not be combined with other networking types.

## Storage Features and Virtualization

Templates define the base OS image that will be used when a guest is first booted. For example, a template might be 64-bit CentOS 5.3. Every template has a privacy level associated with it. Privacy levels include:

* **Public**. The template is available to all users.
* **Published**. The template is available to its owner and select accounts to which the owner published the template.
* **Private**. The template is available to only its owner.

Administrators and end users can add templates to the system. Users can see the template owner when viewing the template.

The CloudStack platform defines a volume as a unit of storage available to a guest VM. Volumes are either root disks or data disks. The root disk has “/” in the file system and is usually the boot device. Data disks provide for additional storage (E.g. As “/opt” or “D:”). Every guest VM has a root disk and a data disk. End users can mount multiple data disks to guest VMs. Users choose data disks from the disk offerings created by administrators. The user can create a template from a volume as well; this is the standard procedure for private template creation.

ISO images may be stored in the system and made available with a privacy level similar to templates. ISO images are classified as either bootable or not bootable. A bootable ISO image is one that contains an OS image (E.g. An Ubuntu 10.04 installation CD). The CloudStack platform allows a user to boot a guest VM off of an ISO image. Users can also attach ISO images to guest VMs. For example, this enables installing PV drivers into Windows.

In the Service Provider Edition and Enterprise Edition, snapshots may be taken for volumes, including both root and data disks. The administrator places a limit on the number of stored snapshots per user. Users can create new volumes from the snapshot for recovery of particular files and they can create templates from snapshots to boot from a restored disk. Snapshots may be set to occur on a recurring schedule. A completed snapshot is copied from primary storage to secondary storage, where it is stored until deleted or purged by newer snapshots.

The administrator provisions primary and secondary storage in the CloudStack platform. Both primary and secondary storage can be accessible via either iSCSI or NFS. Primary storage stores the guest VM virtual disk image. It is typically located close to the Computing Nodes. Secondary storage stores the templates, ISO images, and snapshot data. There is usually one instance of secondary storage for hundreds of Computing Nodes. The CloudStack platform manages the allocation of guest virtual disks to particular primary storage devices.

## Administrator Controlled Allocation

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

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

## Guest VM Management

The CloudStack platform provides several guest management operations for end users and administrators. VMs may be stopped, started, rebooted, and destroyed.

Guests have a name and group. Guest names and groups are opaque to the CloudStack platform and are available for end users to organize their VMs.

Guests can be configured to be Highly Available (HA). An HA-enabled guest is monitored by the system. If the system detects that the guest is down, it will attempt to restart the guest, possibly on a different Computing Node.

The CloudStack platform cannot distinguish a guest VM that was shut down by the user (E.g. Via the “shutdown” command in Linux) from a VM that exited unexpectedly. If an HA-enabled guest is shut down inside the VM, the CloudStack platform will restart it. The user must go through the CloudStack UI or API to shut down an HA-enabled guest.

## Manageability

The system provides alerts and events to help with the management of the cloud. Alerts are notices to an administrator, generally delivered by e-mail, notifying the administrator that an error has occurred in the cloud. Alert behavior is configurable.

Events track all of the user and administrator actions in the cloud. For example, every guest VM start creates an associated event. Events are stored in the Management Server’s database.

The CloudStack platform allows administrators to place a Computing Node into maintenance mode. When maintenance mode is activated the node is first removed from the pool of nodes available to receive new guest VMs. Then, the guest VMs currently running on the node are seamlessly migrated to another Computing Node not in maintenance mode. This migration uses live migration technology and does not interrupt the execution of the guest.

Host and guest performance monitoring is available to end users and administrators. This allows the user to monitor their utilization of resources and determine when it is appropriate to choose a more powerful service offering or larger disk.

## API and Extensibility

The CloudStack platform end user and administrator web interfaces are built on the same HTTP query interface that is available for integration. This simple interface enables the creation of command line tools and new user interfaces to suit particular needs.

The CloudStack platform pluggable allocation architecture allows the creation of new types of allocators for the selection of storage and Computing Nodes.

## Scalability and Availability

The CloudStack platform has been designed to support thousands of Computing Nodes located in multiple data centers. Administrators define a Pod as the unit of scale. Typically a Pod would be a rack of hardware. Scaling out the cloud becomes the process of adding new Pods and provisioning the added resources with the Management Server.

The CloudStack platform has a number of features to increase the availability of the system. The Management Server itself may be deployed in a farm where the servers are load balanced. MySQL may be configured to use replication to provide for a manual failover in the event of database loss. For the Computing Nodes, the CloudStack platform supports NIC bonding and the use of separate networks for storage as well as iSCSI Multipath.

# Selecting Hardware and Software

The CloudStack platform has been designed to support a wide variety of hardware for Computing Nodes, storage, and network devices. The following sections describe the requirements and in some cases provide statements on models that have been certified.

## Computing Nodes

For 64-bit x86 machines with processors supporting either AMD-V or Intel VT virtualization, extensions are required.

Citrix provides a hardware compatibility list for XenServer at <http://hcl.xensource.com/>,for those customers using the Citrix XenServer as their hypervisor.

RedHat provides a hardware compatibility list for RHEL at <https://hardware.redhat.com/>; however, it does not appear possible to do a search to constrain results to hardware that supports KVM.

Each machine should have at minimum 36 GB local disk storage and one or more Gigabit Ethernet (GbE) cards. We recommend 10 Gbps cards for best performance.

The CloudStack platform automatically detects the amount of CPU and memory resources provided by the Computing Nodes.

## Management Servers

The Management Server requires a 64-bit version of Linux. CentOS 5.3 and later are supported. For the Community Edition, Ubuntu 10.04 and Fedora 13 are supported. The Management Server may be placed on a virtual machine.

A load balancer (such as NetScaler) may be used to load balance traffic from the web and connections from the Computing Nodes.

## Storage

The CloudStack platform has been certified with popular storage, including:

* Dell EqualLogic™ for iSCSI
* Network Appliances filers for NFS
* Scale Computing for NFS

## Network

The CloudStack platform has been certified with popular networking equipment including:

* **Network switch**: Cisco™ 3750-E or compatible Gigabit Ethernet switch
* **Ethernet switch**: Dell™ 6224 Gigabit Ethernet switch

Additional hardware configurations can be certified as professional service engagements based on individual customer needs.

## Hypervisor Support

For the Community Edition, the version of Ubuntu, Fedora, or CentOS used on the Computing Nodes defines the Hypervisor version. This has been specified in the Computing Nodes section.

For the Service Provider and Enterprise Editions, Citrix XenServer 5.6 is required on the Computing Nodes.

## Guest OS and Software Support

The CloudStack platform works with all operating systems supported by the underlying hypervisor.

# Planning a Deployment

## Management Server Farm

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

Hardware Load Balancer

User web/API interface

Admin web/API interface

Connections from Computing Nodes

Mgmt Server

Hardware Load Balancer

Mgmt Server

Mgmt Server

Backup MySQL DB

Primary MySQL DB

The administrator must decide the following.

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

## Scaling Concepts

### Computing Nodes

Computing Nodes are the basic physical scaling block of the CloudStack platform. Additional Computing Nodes can be added at any time to provide more capacity for guest VMs.

Computing Nodes are not visible to the end user. An end user cannot determine which Computing Node their guest has been assigned to.

### Clusters (Service Provider and Enterprise Editions)

Clusters are the second level of physical scaling in the CloudStack platform. A Cluster is a collection of Compute Nodes that have access to shared Primary Storage. Nodes in the same Cluster can live migrate instances to and from each other. A Cluster has at most 16 XenServer nodes.

Computing Nodes that are in the same Cluster are in the same subnet.

Clusters are not applicable to deployments that use local storage.

Clusters are not visible to the end user.

### Pods

Pods are the third level of physical scaling in the CloudStack platform.

With XenServer and shared Primary Storage a Pod is a collection of clusters. It may be exactly one Cluster establishing a 1:1 mapping between Cluster and Pod. Multiple Clusters per Pod are supported; currently CloudStack has been tested with up to two Clusters per Pod.

With XenServer and local storage a Pod is a collection of Compute Nodes. There are no practical limits to the number of Compute Nodes in a Pod in this case.

With KVM a Pod is a collection of Compute Nodes. In this case there are no practical limits to the number of Compute Nodes in a Pod.

The Management Server is used to add and remove Computing Nodes and primary storage from Clusters and Pods.

A Pod is frequently mapped to a single rack with a layer-2 switch. Computing Nodes in the same Pod are in the same subnet.

Pods are not visible to the end user.

### Availability Zones

Availability Zones are the fourth level of physical scaling in the CloudStack platform. An Availability Zone is a collection of Pods and secondary storage. An Availability Zone will include one or more layer-3 switches. The Availability Zone implies some form of physical isolation and redundancy (E.g. Separate power supply and network uplink) from other Availability Zones. It does not necessarily mean geographic distribution, and there may be one or more Availability Zones in a data center.

Availability Zones are visible to the end user. They must select an Availability Zone for their guest when started. They may also be required to copy their private templates to additional Availability Zones to enable creation of guest VMs in those zones from their templates.

Computing Nodes in the same Availability Zone are directly accessible to each other without having to go through a firewall. Nodes in different Availability Zones can access each other through statically configured VPN tunnels.

The administrator must decide the following.

* How many Computing Nodes to place in a Pod.
* How many primary storage servers to place in a Pod and total capacity for the storage servers.
* How many Pods to place in an Availability Zone.
* How many Clusters to have per Pod
* How much secondary storage to deploy in an Availability Zone.

## Multi-Site Deployment

The CloudStack platform scales well into multiple sites through the use of Availability Zones. Figure 2 is an example of a multi-site deployment.

Primary Management Server

Availability Zone 1

Secondary Management Server

Availability Zone 4

Availability Zone 5

Availability Zone 3

Availability Zone 2

Data Center 1

Data Center 2

Data Center 3

Data Center 4

Data Center 5

MySQL Replication

Figure 2 Example of a Multi-Site Deployment

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

# Defining Your Service Offering

The service offering defines the virtual hardware that the end users will be able to choose from. This includes CPU core count and speed, memory, and disk size. Here is an example of a service offering:

A virtual machine instance that is equivalent to a 1 GHz Intel® Core™ 2 CPU, with 1 GB memory at $0.20/hour. Network traffic metered at $0.10/GB.

The users expect that a service offering includes the following elements:

* CPU, memory, and network resource guarantees.
* How resources are metered.
* How the resource usage is charged.
* How often the charges are generated.

The CloudStack platform allows the administrator to configure the resource guarantee. It then emits usage records that the administrator can integrate with their billing system.

Service offerings cannot be changed once created.

A service offering that is no longer in use by any virtual machines can be permanently deleted.

A service offering that is still in use can be deleted by the administrator. However it will remain in the database until all the virtual machines referencing it have been deleted. After deletion by the administrator, a service offering will not be available to end users that are creating new instances.

The CloudStack platform separates service offerings into computing service offerings and storage service offerings. The computing service offering specifies:

* Guest CPU
* Guest RAM
* Guest Networking type (virtual or direct)
* Tags on the root disk

The disk offering specifies:

* Disk size
* Tags on the data disk

# Understanding Network Types and Network Virtualization

In the CloudStack platform there are several types of networks, some real and some virtual. These include:

* **Guest Network**. The virtual network that the guest virtual machines connect to. It provides the isolation discussed previously.
* **Private Network**. The physical network that carries guest-guest traffic between Computing Nodes when virtual networking is used.
* **Public Network**. The physical network that provides the guests with access to the Internet. This network also carries guest-guest traffic when Direct Attached networking is used.
* **Management Network**. The physical network that provides the link between the Management Servers, hypervisors, and storage devices.
* **Storage Network**. An optional physical network that provides the link between the hypervisors and storage devices.

There need not be a physical separation between these network types. For example, the CloudStack platform can run successfully on a single node installation that has a single NIC. Further, in all cases the private network and the management network are the same network.

Optionally, with the Premium Edition, a NIC may be dedicated to the public network. This can be used to isolate the public network traffic from the private network.

Optionally, a NIC may be dedicated to a separate Storage Network. This can be used to isolate storage traffic from other types of traffic. For example, a 1 Gbps NIC could be used for the private network while a 10 Gbps NIC is used for storage access.

See the Install Guide for instructions on procedures for these configurations.

Network virtualization is the process of creating a network for use by guest virtual machines. This virtual network has the characteristics of a LAN from the viewpoint of the guests. The resources used to create the virtual network may come from many sources and may rely on software-based components to a greater extent than is common in physical networks.

## Guest Network

Each account that has a guest with a virtual network Service Offering is assigned a virtual network in its Availability Zone. A guest virtual network can be configured to any private address space. This document uses a Class A network in 10.0.0.0/8 private address space for its examples. The guest virtual network is an overlay network on top of the private network and is managed by the CloudStack platform.

A guest virtual network is valid within only one Availability Zone. Therefore virtual machines in different Availability Zones cannot communicate with each other using their IP addresses in the guest virtual network. Virtual machines in different Availability Zones must communicate with each other by routing through a public IP address.

Figure 1 illustrates a typical guest virtual network setup.

Routing Domain

Account 1 Guest 1

Account 1 Guest 2

Account 1 Guest 3

Account 1 Guest 4

Internet

Public Network (65.37.\*.\*)

Guest Virtual Network 10.0.0.0/8

Gateway address 10.1.1.1

NAT  
Load Balancing

65.37.141.24  
65.37.141.27

65.37.\*.\*

10.1.1.2

10.1.1.3

10.1.1.4

10.1.1.5

Private Network (192.168.\*.\*)

Figure Guest Virtual Network Setup

The Management Server automatically creates a Virtual Router for each guest virtual network. A virtual router is a special virtual machine that runs on the Computing Nodes. Each virtual router has three network interfaces. Its eth0 interface serves as the gateway for the guest virtual network and has the IP address of 10.1.1.1. Its eth1 interface resides on the private/management network and is used by the system to configure the virtual router. Its eth2 interface is assigned a public IP address on the public network.

The virtual router provides DHCP and will automatically assign an IP address for each guest VM in the 10.0.0.0/8 network. The user can manually reconfigure guest VMs to assume different IP addresses.

Source NAT is automatically configured in the virtual router to forward outbound traffic for all guest VMs.

## Network Virtualization within One Pod

Figure 2 illustrates network setup within a single Pod. The Computing Nodes are connected to a Pod-level switch. At a minimum the Computing Nodes should have one physical uplink to each switch. Bonded NICs are supported as well. The Pod-level switch is a pair of redundant gigabit switches with 10 G uplinks.

Pod-Level Switch (layer-2 switch)

Computing Node 3

Computing Node 1

Storage Device 1

Computing Node 2

Computing Node 4

Computing Node 5

Storage Device 2

Computing Node 6

Public Network (65.37.\*.\*)

Private/Management Network (192.168.\*.\*)



Guest Networks (10.\*.\*.\*)

Figure Network Setup within a Single Pod – Logical View

Servers are connected to the private/management and public networks as follows:

* Storage devices are connected to only the private/management network.
* Computing Nodes are connected to both the management network and the public network.

**Note: If there is no virtual router executing on a Computing Node, then that Computing Node will not have a NIC bound to an IP address on the management network.**

* The Computing Nodes are connected to one or more guest networks.

We recommend the use of multiple physical Ethernet cards to implement each network interface as well as redundant switch fabric in order to maximize throughput and improve reliability.

## Network Virtualization within One Availability Zone

Figure 3 illustrates the network setup within a single Availability Zone.



Layer-2 switch



Internet

Layer-3 switch w/ firewall modules

Pod 2

Pod 1

Primary storage servers



Management Server farm with MySQL



Computing Nodes



Secondary storage servers



Figure Network Setup within a Single Availability Zone

The private/management network carries traffic in the guest virtual networks.

A firewall for the private/management network operates in the NAT mode. The private/management network typically is assigned IP addresses in the 192.168.0.0/16 Class B private address space. Each Pod is assigned IP addresses in the 192.168.\*.0/24 Class C private address space.

Each Availability Zone has its own set of public IP addresses. Public IP addresses from different Availability Zones do not overlap.

The private/management network addresses must be unique across the cloud. You cannot, for example, have a Computing Node in one Availability Zone which has the same private IP address as a Computing Node in another Availability Zone.

## Network Virtualization

Network virtualization uses tagged VLANs to provide isolation between guest virtual networks. There is one tagged VLAN per guest virtual network with active instances in a Zone.

With network virtualization there are two base VLANs that are present within every Availability Zone.

* **The Private/Management VLAN**. This is for the private/management network as defined above.
* **The Public VLAN**. This is for the public network as defined above.

There are 4094 available VLANs according to the 802.1q standard. The administrator should determine a segmentation of the VLAN namespace that matches their requirements. Here is an example of such a segmentation:

|  |  |
| --- | --- |
| **VLAN IDs** | **Use** |
| < 100 | Reserved for administrative purposes |
| 100-199 | Public VLANs |
| 200-499 | Untagged private IPs for each Pod |
| 500-1999 | Zone VLANs |
| > 2000 | Reserved for future use |

## Private Address Allocation

The CloudStack platform allocates a private IP address to each virtual router. The administrator is responsible for allocating private IP addresses to the hypervisors. The administrator configures the CloudStack platform with the range of IP addresses available for virtual router private IP address allocation.

## Public Address Allocation

Each virtual router is assigned at least one public IP addresses. The user may request additional public IP addresses.

The administrator configures the available public IP address pools on a per-Availability Zone basis. Distinct public IP ranges can be added as separate VLANs incrementally. Each public IP range can be used by any Pod inside the same Availability Zone.

# Storage Features and Types

The CloudStack platform defines two types of storage: primary and secondary. Primary storage can be accessed by either iSCSI or NFS. Additionally, direct attached storage may be used for primary storage. Secondary storage is always accessed using NFS.

A site’s policies and administrative preferences combined with the advantages and disadvantages of each access protocol should be considered in deciding between NFS, iSCSI, and direct attached storage for primary storage.

In the Service Provider Edition and Enterprise Edition the virtual disk image format is VHD. QCOW is used for the Community Edition.

In contrast to some other cloud offerings, there is no ephemeral storage in the CloudStack platform. All volumes on all nodes are persistent.

## Primary Storage

Primary Storage is used for storing the guest VM root disks as well as additional data disk volumes. It is located in the same Pod as the Computing Nodes for maximum speed and throughput and is always assigned to a Pod. Volumes are created automatically when a virtual machine is created. The volumes are deleted when the VM is destroyed.

The speed of primary storage will impact guest performance. If possible administrators should choose smaller, higher RPM drives for primary storage.

Primary Storage can be added at any time via the administrator UI. Administrators should monitor the capacity of primary storage devices and add additional primary storage as needed.

When the hypervisor is XenServer, the XenServer nodes are added in a Xen Storage Pool. This provides for Live Migration of the guests from one Computing Node to another in the same Pod. The CloudStack platform will automatically create the Xen Storage Pools as Computing Nodes are added. The administrator may configure the Storage Pools themselves; if this is done the CloudStack platform will add all Computing Nodes in the Storage Pool when one Node is added.

Thin provisioning is used for the guest virtual disk images. This greatly increases the number of guests that can be allocated per TB of storage.

Local storage is an option for primary storage. To use local storage for the System Virtual Machines (E.g. the Virtual Router), set system.vm.use.local.storage to true in global configuration.

The system supports multiple Primary Storage pools. For example, you could provision 2 NFS servers in primary storage. Or you could provision 1 iSCSI LUN initially and then add a second iSCSI LUN when the first approaches capacity.

### Tags

Storage may be "tagged". A tag is a text string attribute associated with Primary Storage, a Disk Offering, or a Service Offering. Tags allow administrators to provide additional information about the storage. For example, that is a "SSD" or it is "slow". Tags are not interpreted by the CloudStack. They are matched against tags placed on service and disk offerings. Service and disk offering tags are used to identify the requirements of the storage that those offerings have. For example, the high end service offering may require "fast" for its root disk volume.

The interaction between tags, allocation, and volume copying across Clusters and Pods is complex. As a simplification the CloudStack currently requires that all Clusters in a Zone have the same set of tags present on their Primary Storage. Different devices can be used to present those tags, but the set of exposed tags must be the same.

## Secondary Storage

Secondary Storage is used for storing templates, saved snapshots of guest VMs, and ISO images. The secondary storage has a high read:write ratio and is expected to consist of larger drives with lower I/OpS than the primary store. The secondary storage device must be located in the same Availability Zone as the guest VMs it serves.

There must be exactly one secondary storage device per Availability Zone.

Submissions to secondary storage go through the Management Server. The Management Server can retrieve templates and ISO images from URLs using a variety of protocols.

## Working with Volumes

A volume provides storage to a guest VM. The volume can provide for a root disk or an additional data disk. The CloudStack platform supports additional volumes for guest VMs.

## Working with ISO Images

The CloudStack platform supports ISOs and their attachment to guest VMs. An ISO is a read-only file that has an ISO/CD-ROM style file system. Users can upload their own ISOs and mount them on their guest VMs.

ISOs are uploaded based on a URL. HTTP is the supported protocol. Once the ISO is available via HTTP specify an upload URL such as http://my.web.server/filename.iso.

## Working with Blank VMs

Users can create blank virtual machines. A blank virtual machine is a virtual machine without an OS template. Users can attach an ISO file and install the OS from the CD/DVD-ROM.

## Working with Templates

A template is a virtual disk image that can be used to instantiate a new virtual machine. Templates may be of a variety of operating systems as described later in this document. The administrator and the template creator (the end user) can set different levels of access control on templates.

In the Community Edition templates are of the QCOW image format. In the Service Provider and Enterprise Editions templates are in the VHD format.

When templates are deleted the VMs instantiated from them will continue to run. However, new VMs cannot be created based on the deleted template.

### The Default Template

The CloudStack platform includes a CentOS template. This template is downloaded by the Secondary Storage VM after the primary and secondary storage are configured. You can use this template in your production deployment or you can delete it and use custom templates.

The default template includes the standard iptables rules, which will block most access to the template excluding ssh.

# iptables --list

Chain INPUT (policy ACCEPT)

target prot opt source destination

RH-Firewall-1-INPUT all -- anywhere anywhere

Chain FORWARD (policy ACCEPT)

target prot opt source destination

RH-Firewall-1-INPUT all -- anywhere anywhere

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

Chain RH-Firewall-1-INPUT (2 references)

target prot opt source destination

ACCEPT all -- anywhere anywhere

ACCEPT icmp -- anywhere anywhere icmp any

ACCEPT esp -- anywhere anywhere

ACCEPT ah -- anywhere anywhere

ACCEPT udp -- anywhere 224.0.0.251 udp dpt:mdns

ACCEPT udp -- anywhere anywhere udp dpt:ipp

ACCEPT tcp -- anywhere anywhere tcp dpt:ipp

ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

### Creating Templates

Templates can be created from either volumes or ISO images. The procedure to create a template from a volume is relatively straightforward and is available in the web UI.

The procedure to create a template from an ISO image is as follows:

1. Log into the UI as either an end user or administrator.
2. Click on the Templates tab, and go to the ISO section.
3. Click Add New ISO. You must provide:

* **Name**. Short name for the ISO image. (E.g. Ubuntu 9.10)
* **Display** Text. Description of the ISO image. (E.g. Ubuntu 9.10 Desktop i386 32 bit)
* **URL**. The URL that hosts the ISO image. The Management Server must be able to access this location via HTTP. If needed you can place the ISO image directly on the Management Server.
* **Public**. Whether or not the ISO image should be available to all users. Select No if the template should be private.

1. Click Create.

The Management Server will download the ISO. Depending on the size of the ISO, this may take a long time. The ISO status column will display Ready once it has been successfully downloaded into the secondary storage. Clicking Refresh updates the download percentage.

**Important: Do not continue to the next step until the ISO has finished downloading.**

1. Go to the Instance tab and click on Create a New VM. Click Blank Template, located in the My Templates section, and select the ISO file. A VM will be created and booted from that ISO file.

**Note: If you do not see the Blank Template selection then the system does not have an available ISO; return to the previous step.**

1. Make any desired configuration changes on the running VM and then stop it.
2. Once stopped, click on the Volumes link for the instance and select Create Template. This will create a template from this image.

The new template will be visible in the Templates tab when the template creation process has been completed. The template is then available when creating a new VM.

### Running Sysprep for Windows Templates

Windows templates must be prepared before they can be provisioned on multiple machines. You first need to upload your Windows ISO and create a VM Instance with this ISO. After you have created your VM with Windows installed, follow these next steps to run sysprep on your VM. Sysprep allows you to create a generic Windows template and avoid any possible SID conflicts.

#### Sysprep for Windows Server 2008 R2

For Windows 2008 R2, you run Windows System Image Manager to create a custom sysprep response XML file. Windows System Image Manager is installed as part of the Windows Automated Installation Kit (AIK). Windows AIK can be downloaded from the Microsoft Download Center at the following location:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en>

Use the following steps to run sysprep for Windows 2008 R2.[[1]](#footnote-1)

1. Download and install the Windows AIK.

**Note: Windows AIK should not be installed on the Windows 2008 R2 VM you just created. Windows AIK should not be part of the template you create. It is only used to create the sysprep answer file.**

1. Copy the install.wim file in the \sources directory of the Windows 2008 R2 installation DVD to the hard disk. This is a very large file and may take a long time to copy. Windows AIK requires the WIM file to be writable.
2. Start the Windows System Image Manager, which is part of the Windows AIK.
3. In the Windows Image pane, right click “Select a Windows image or catalog file” to load the install.wim file you just copied.
4. Select the Windows 2008 R2 Edition.

You may be prompted with a warning that the catalog file cannot be opened. Click Yes to create a new catalog file.

1. In the Answer File pane, right click to create a new answer file.
2. Generate the answer file from the Windows System Image Manager using the following steps.
3. The first page you need to automate is the Language and Country or Region Selection page. To automate this, expand Components in your Windows Image pane, right-click and add the Microsoft-Windows-International-Core setting to Pass 7 oobeSystem. In your Answer File pane, configure the InputLocale, SystemLocale, UILanguage, and UserLocale with the appropriate settings for your language and country or region. Should you have a question about any of these settings, you can right-click on the specific setting and select Help. This will open the appropriate CHM help file with more information, including examples on the setting you are attempting to configure.



1. You need to automate the Software License Terms Selection page, otherwise known as the End-User License Agreement (EULA). To do this, expand the Microsoft-Windows-Shell-Setup component. High-light the OOBE setting, and add the setting to the Pass 7 oobeSystem . Under Settings, select the drop down next to HideEULAPage and select true.



1. Make sure the license key is properly set. If you use MAK key, you can just enter the MAK key on the Windows 2008 R2 VM. You need not input the MAK into the Windows System Image Manager. If you use KMS host for activation you need not enter the Product Key. Details of Windows Volume Activation can be found here: <http://technet.microsoft.com/en-us/library/bb892849.aspx>
2. You need to automate is the Change Administrator Password page. Expand the Microsoft-Windows-Shell-Setup component (if it is not still expanded), expand UserAccounts, right-click on AdministratorPassword, and add the setting to the Pass 7 oobeSystem configuration pass of your answer file. Under Settings, specify a password next to Value.



You may read the AIK documentation and set many more options that suit your deployment. The steps above are the minimum needed to make Windows unattended setup work.

1. Save the answer file as unattend.xml. You can ignore the warning messages that appear in the validation window.
2. Copy the unattend.xml file into the c:\windows\system32\sysprep directory of the Windows 2008 R2 Virtual Machine.
3. Once you place the unattend.xml file in c:\windows\system32\sysprep directory, you run the sysprep tool as follows:

cd c:\Windows\System32\sysprep

sysprep.exe /oobe /generalize /shutdown

The Windows 2008 R2 VM will automatically shut down after sysprep is complete

#### Sysprep for Windows Server 2003 R2

Earlier versions of Windows have a different sysprep tool. Follow these steps for Windows Server 2003 R2.

1. Extract the content of \support\tools\deploy.cab on the Windows installation CD into a directory called c:\sysprep on the Windows 2003 R2 VM.
2. Run c:\sysprep\setupmgr.exe to create the sysprep.inf file.
3. Select Create New to create a new Answer File.
4. Enter “Sysprep setup” for the Type of Setup.
5. Select the appropriate OS version and edition.
6. On the License Agreement screen, select “Yes fully automate the installation”.
7. Provide your name and organization.
8. Leave display settings at default.
9. Set the appropriate time zone.
10. Provide your product key.
11. Select an appropriate license mode for your deployment.
12. Select “Automatically generate computer name”.
13. Type a default administrator password. If you enable the password reset feature, the users will not actually use this password. This password will be reset by the VMOps instance manager after the guest boots up.
14. Leave Network Components at “Typical Settings”.
15. Select the “WORKGROUP” option.
16. Leave Telephony options at default.
17. Select appropriate Regional Settings.
18. Select appropriate language settings.
19. Do not install printers.
20. Do not specify “Run Once commands”.
21. You need not specify an identification string.
22. Save the Answer File as c:\sysprep\sysprep.inf.
23. Run c:\sysprep\sysprep.exe –reseal –mini –activated to sysprep the image. After this step the machine will automatically shut down.

#### Creating the Windows Template

Once your VM has shutdown, you now can create a template.

1. Click on the Volumes link under your Windows VM.
2. Click on the Create Template link next to the root disk.

### Importing AMI’s

The following procedures describe how to import an AMI into the CloudStack platform when using the XenServer hypervisor.

Assume you have an AMI file and this file is called CentOS\_5.4\_x64. Assume further that you are working on a CentOS host. If the AMI is a Fedora image, you need to be working on a Fedora host initially.

**Note: You need to have a XenServer host with a file-based storage repository (either a local ext3 SR or an NFS SR) to convert to a VHD once the image file has been customized on the Centos/Fedora host.**

1. Set up loopback on image file:

# mkdir -p /mnt/loop/centos54

# mount -o loop CentOS\_5.4\_x64 /mnt/loop/centos54

1. Install the kernel-xen package into the image. This downloads the PV kernel and ramdisk to the image.

# yum -c /mnt/loop/centos54/etc/yum.conf --installroot=/mnt/loop/centos54/ -y install kernel-xen

1. Create a grub entry in /boot/grub/grub.conf.

# mkdir -p /mnt/loop/centos54/boot/grub

# touch /mnt/loop/centos54/boot/grub/grub.conf

# echo "" > /mnt/loop/centos54/boot/grub/grub.conf

1. Determine the name of the PV kernel that has been installed into the image

# cd /mnt/loop/centos54

# ls lib/modules/

2.6.16.33-xenU 2.6.16-xenU 2.6.18-164.15.1.el5xen 2.6.18-164.6.1.el5.centos.plus 2.6.18-xenU-ec2-v1.0 2.6.21.7-2.fc8xen 2.6.31-302-ec2

# ls boot/initrd\*

boot/initrd-2.6.18-164.6.1.el5.centos.plus.img boot/initrd-2.6.18-164.15.1.el5xen.img

# ls boot/vmlinuz\*

boot/vmlinuz-2.6.18-164.15.1.el5xen boot/vmlinuz-2.6.18-164.6.1.el5.centos.plus boot/vmlinuz-2.6.18-xenU-ec2-v1.0 boot/vmlinuz-2.6.21-2952.fc8xen

Xen kernels/ramdisk always end with "xen". For the kernel version you choose, there has to be an entry for that version under lib/modules, there has to be an initrd and vmlinuz corresponding to that. Above, the only kernel that satisfies this condition is 2.6.18-164.15.1.el5xen

1. Based on your findings, create an entry in the grub.conf file. Below is an example entry.

default=0

timeout=5

hiddenmenu

title CentOS (2.6.18-164.15.1.el5xen)

        root (hd0,0)

        kernel /boot/vmlinuz-2.6.18-164.15.1.el5xen ro root=/dev/xvda

        initrd /boot/initrd-2.6.18-164.15.1.el5xen.img

1. Edit etc/fstab, changing “sda1” to “xvda” and changing “sdb” to “xvdb”.

# cat etc/fstab

/dev/xvda / ext3 defaults 1 1

/dev/xvdb /mnt ext3 defaults 0 0

none /dev/pts devpts gid=5,mode=620 0 0

none /proc proc defaults 0 0

none /sys sysfs defaults 0 0

1. Enable login via the console. The default console device in a XenServer system is xvc0. Ensure that /etc/inittab and /etc/securetty have the following lines respectively:

# grep xvc0 /etc/inittab

co:2345:respawn:/sbin/agetty xvc0 9600 vt100-nav

# grep xvc0 /etc/securetty

xvc0

1. Ensure the ramdisk supports PV disk and PV network. Customize this for the kernel version you have determined above.

# chroot /mnt/loop/centos54

# cd /boot/

# mv initrd-2.6.18-164.15.1.el5xen.img initrd-2.6.18-164.15.1.el5xen.img.bak

# mkinitrd -f /boot/initrd-2.6.18-164.15.1.el5xen.img --with=xennet --preload=xenblk --omit-scsi-modules 2.6.18-164.15.1.el5xen

1. Change the password.

 # passwd

Changing password for user root.

New UNIX password:

Retype new UNIX password:

passwd: all authentication tokens updated successfully.

1. Exit out of chroot.

# exit

1. Check etc/ssh/sshd\_config for lines allowing ssh login using a password.

# egrep "PermitRootLogin|PasswordAuthentication" /mnt/loop/centos54/etc/ssh/sshd\_config

PermitRootLogin yes

PasswordAuthentication yes

1. If you need the template to be enabled to reset passwords from the CloudStack UI or API, install the password change script into the image at this point. This can be found on http://open.cloud.com.

# wget –O – http://url/to/get\_passwd\_from\_domr > /mnt/loop/centos54/etc/init.d/

# chroot /mnt/loop/centos54

# chmod a+x /etc/init.d/get\_password\_from\_domr

# chkconfig --add get\_password\_from\_domr

# chkconfig get\_password\_from\_domr on

# exit

1. Unmount and delete loopback mount.

# umount /mnt/loop/centos54

# losetup -d /dev/loop0

1. Copy the image file to your XenServer host's file-based storage repository. In the example below, the Xenserver is "xenhost". This XenServer has an NFS repository whose uuid is a9c5b8c8-536b-a193-a6dc-51af3e5ff799.

# scp CentOS\_5.4\_x64 xenhost:/var/run/sr-mount/a9c5b8c8-536b-a193-a6dc-51af3e5ff799/

1. Log in to the Xenserver and create a VDI the same size as the image.

[root@xenhost ~]# cd /var/run/sr-mount/a9c5b8c8-536b-a193-a6dc-51af3e5ff799

[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# ls -lh CentOS\_5.4\_x64

-rw-r--r-- 1 root root 10G Mar 16 16:49 CentOS\_5.4\_x64

[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# xe vdi-create virtual-size=10GiB sr-uuid=a9c5b8c8-536b-a193-a6dc-51af3e5ff799 type=user name-label="Centos 5.4 x86\_64"

cad7317c-258b-4ef7-b207-cdf0283a7923

1. Import the image file into the VDI. This may take 10–20 minutes.

[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# xe vdi-import filename=CentOS\_5.4\_x64 uuid=cad7317c-258b-4ef7-b207-cdf0283a7923

1. Locate a the VHD file. This is the file with the VDI’s UUID as its name. Compress it and upload it to your web server.

[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# bzip2 -c cad7317c-258b-4ef7-b207-cdf0283a7923.vhd > CentOS\_5.4\_x64.vhd.bz2

[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# scp CentOS\_5.4\_x64.vhd.bz2 webserver:/var/www/html/templates/

### Adding Password Management to Your Templates

The CloudStack platform provides an optional password reset feature that allows users to set a temporary admin or root password as well as reset the existing admin or root password from the CloudStack UI.

To enable the Reset Password feature, you will need to download an additional script to patch your template. When you later upload the template into the CloudStack platform, you can specify whether reset admin/root password feature should be enabled for this template.

#### Window OS Installation

Download the installer, CloudInstanceManager.msi, from <http://open.cloud.com> and run the installer in the newly created Windows VM.

#### Linux OS Installation

Use the following steps to begin the Linux OS installation.

1. Download the installation file.
2. Run get\_password\_from\_domr from <http://open.cloud.com>.
3. Copy this password to /etc/init.d.
4. On some Linux distributions, you will need to copy the file to /etc/rc.d/init.d.
5. Run the following command to make the script executable.

chmod +x /etc/init.d/get\_password\_from\_domr

1. Depending on the Linux distribution, continue with the appropriate step.
2. **Fedora, CentOS/RHEL, and Debian**. Run “chkconfig --add get\_password\_from\_domr”.
3. **Ubuntu**. Run “sudo update-rc.d get\_password\_from\_domr defaults 98”. Then run "mkpasswd" and check that it is generating a new password. If the “mkpasswd” command does not exist, run "sudo apt-get install whois" and repeat.

### Uploading Templates

Templates are frequently large files. You can optionally gzip them to decrease upload times.

Templates are uploaded based on a URL. HTTP is the supported access protocol. The Management Server will download the file from the specified URL, such as <http://my.web.server/filename.vhd.gz>.

The operating system type should be provided when uploading a template. This helps the CloudStack platform and hypervisor perform certain operations and make assumptions that improve the performance of the guest. If the operating system present on the template is not available you should select Other.

**Note: Generally you should not choose an older version of the OS that you have. For example, choosing CentOS 5.3 to support a CentOS 5.4 image will in general not work. In those cases you should choose Other.**

“Password Enabled” refers to whether or not your template has the CloudStack platform password change script installed. This was discussed previously.

### Public Templates

Public templates are available to all users in all accounts. All users can create virtual machines from these templates.

When a user publishes a template as “public”, the template is available to all users in all domains.

### Private Templates

Private templates are only available to the user who created them. By default an uploaded template is private.

Users can create virtual machines from their collection of private templates the same way they create virtual machines from public templates.

### Published Templates

A user can publish a template to another user. In this case the template is available to the two users but not to other users.

### Deleting Templates

Templates may be deleted. In general, when a template spans multiple Zones only the copy that is selected for deletion will be deleted; the same template in other Zones will not be deleted. The provided CentOS template is an exception to this. If the provided CentOS template is deleted it will be deleted from all Zones.

## Working with Snapshots (Service Provider and Enterprise Editions)

The CloudStack platform supports snapshots of disk volumes. Snapshots are a point-in-time capture of virtual machine disks. Memory and CPU states are not captured.

**Note: Snapshots are available in the Service Provider and Enterprise Editions.**

Users can create snapshots manually, or by setting up automatic recurring snapshot policies. Users can also create disk volumes from snapshots, which may be attached to a VM as any other disk volume. Snapshots of both root disks and data disks is supported. However, the software does not currently support booting of a VM from a recovered root disk. A disk recovered from snapshot of a root disk is treated as a regular data disk; the data on recovered disk can be accessed by attaching the disk to a VM.

### Automatic Snapshot Creation and Retention

Users can set up a recurring snapshot policy to automatically create multiple snapshots of a disk at regular intervals. Snapshots can be created on an hourly, daily, weekly, or monthly intervals. Multiple policies can be set up per disk volume as long as the policies are not of the same internal type. For example, a user can set up hourly snapshots to be taken every fifteenth minute of the hour, and a daily snapshots at every 02:30 hours of the day. A user cannot set up hourly snapshots at both fifteenth and thirtieth minute of the hour.

With each snapshot schedule, users can also specify the number of snapshots to be retained. Older snapshots that exceed the retention limit are automatically deleted.

### Incremental Snapshots and Backup

Snapshots are created on primary storage where a disk resides. After a snapshot is created, it is immediately backed up to secondary storage and removed from primary storage for optimal utilization of space on primary storage.

CloudStack platform does incremental backups. Every time a snapshot is taken, only incremental changes since the last snapshot are backed up to secondary store.

### Volume Status

When a snapshot operation is triggered by means of a recurring snapshot policy, a snapshot is skipped if a volume has remained inactive since its last snapshot was taken. A volume is considered to be inactive if it is either detached or attached to a VM that is not running. The CloudStack platform ensures that at least one snapshot is taken since the volume last became inactive.

When a snapshot is taken manually, a snapshot is always created regardless of whether a volume has been active or not.

### Snapshot Restore

There are two paths to restoring snapshots. Users can create volumes from the snapshot. The volume can then be mounted to a VM and files recovered as needed. A template may be created from the snapshot of a root disk. The user can then boot a VM from this template to effect recovery of the enter root disk.

### Performance Considerations

Snapshots not only consume space in secondary storage, but can take up significant CPU cycles and network bandwidth as the snapshots are moved between primary and secondary storage. This is something to be factored in for capacity planning and end-user pricing of snapshot operations.

# Network Features

The CloudStack platform provides network virtualization. Network virtualization allows the guests to communicate with each other using shared infrastructure with the security and user perception that the guests have a private LAN.

The virtual router is the linchpin of the networking features. The Management Server programs the Virtual Router over the management network. The Virtual Router is then able to implement the following features for the guest network.

## Guest Virtual Networks

The IP ranges of the guest virtual networks can be specified on the Zone configuration in the Guest CIDR field. By default each virtual network is a 10.1.1.0/24.

Administrators should set different default Guest CIDRs for each Zone. This will enable easier VPN connectivity in the future.

## IP Forwarding and Firewalling

By default all incoming traffic to the public IP address is rejected. All outgoing traffic from the guests is translated via NAT to the public IP address and is allowed. Users may enable port forwarding for specific public IP addresses, public port to guest IP addresses and guest port.

## IP Load Balancing

The user may choose to associate the same public IP for multiple guests. The system implements a TCP-level load balancer with the following policies.

* Round-robin
* Least connection
* Source IP

This is similar to port forwarding but the destination may be multiple IP addresses.

## Port Forwards

A port forward service is a set of port forwarding rules that define a policy. A port forward service is then applied to one or more guest VMs. The guest VM then has its inbound network access managed according to the policy defined by the port forwarding service.

A guest VM can be in any number of port forward services.

Port forward services can be defined but have no members.

## DNS and DHCP

The Virtual Router provides DNS and DHCP services to the guests. It proxies DNS requests to the DNS server configured on the Availability Zone.

# Working with System Virtual Machines

The CloudStack platform uses several types of system virtual machines to perform tasks in the cloud. In general the CloudStack platform manages these system VMs and creates, starts, and stops them as needed based on scale and immediate needs. However, the administrator should be aware of them and their roles to assist in debugging issues.

## Console Proxy (Premium Edition only)

The Console Proxy has a role in presenting a console view via the web UI. It connects the user’s browser to the VNC port made available via the hypervisor for the console of the guest. Both the administrator and end user web UIs offer a console connection.

Clicking on a console icon brings up a new window. The AJAX code downloaded into that window refers to the public IP address of a console proxy VM. There is exactly one public IP address allocated per console proxy VM. The AJAX application connects to this IP. The console proxy then proxies the connection to the VNC port for the requested VM on the Computing Node hosting the guest.

**Note: The hypervisors will have many ports assigned to VNC usage so that multiple VNC sessions can occur simultaneously.**

There is never any traffic to the guest virtual IP, and there is no need to enable VNC within the guest.

The console proxy VM (available in Premium Edition only) will periodically report its active session count to the Management Server. The default reporting interval is five seconds. This can be changed through standard Management Server configuration with the parameter consoleproxy.loadscan.interval. Assignment of guest VM to console proxy is determined by first determining if the guest VM has a previous session associated with a console proxy. If it does, the Management Server will assign the guest VM to the target Console Proxy VM regardless of the load on the proxy VM. Failing that, the first available running Console Proxy VM that has the capacity to handle new sessions is used.

Console proxies can be restarted by administrators but this will interrupt existing console sessions for users.

The console viewing functionality uses realhostip.com addresses to assist in providing SSL security to console sessions. The console proxy is assigned a public IP address. In order to avoid browser warnings for mismatched SSL certificates the URL for the new console window is set to the form of https://a-b-c-d.realhostip.com. Customers will see this URL during console session creation. The CloudStack includes the realhostip.com SSL certificate in the console proxy VM. Of course the CloudStack cannot know about DNS A records for our customers' public IPs prior to shipping the software. As a result Cloud.com runs a dynamic DNS server that is authoritative for the realhostip.com domain. It maps the a-b-c-d part of the DNS name to the IP address of a.b.c.d on lookups. This allows the browser to correctly connect to the console proxy's public IP, where it then expects and receives a SSL certificate for realhostip.com, and SSL is set up without browser warnings.

## Virtual Router

The function of the virtual router was explained in section 1.4. The end user has no direct access to the virtual router. They can ping it and take actions that impact it (E.g. setting up port forwarding) but they do not have SSH access into the virtual router.

There is no mechanism for the administrator to log in to the virtual router. Virtual routers can be restarted by administrators, but this will interrupt public network access and other services for end users.

A basic test in debugging networking issues is to attempt to ping the virtual router from a guest VM.

## Secondary Storage VM (Premium Edition Only)

The secondary storage VM provides a background task that copies templates from one Availability Zone to another.

The administrator can log in to the secondary storage VM if needed. The procedure for this is documented in the Troubleshooting section of the Installation Guide.

# System Reliability and HA

## Management Server

The CloudStack Management Server should be deployed on a server farm such that it is not susceptible to individual server failures. The Management Server itself (as distinct from the MySQL database) is stateless and may be placed behind a load balancer.

Normal operation of Computing Nodes is not impacted by an outage of all Management Serves. All guest VMs will continue to work.

When the Management Server is down, no new VMs can be created, and the end user and admin UI, API, dynamic load distribution, and HA will cease to work.

## Computing Node

When Computing Nodes are down, the CloudStack platform will restart impacted HA-enabled VMs automatically, assuming that other Computing Nodes have sufficient resources available. When the Computing Node comes back online it will be marked as available and newly started VMs may be allocated to it. VMs previously migrated from it will not be migrated back. VMs that were running on it but did not have HA enabled will not be started automatically.

The user will not lose the virtual machine disk image during a Computing Node outage. However, the guest OS may perceive its disk image as corrupt (and needing fsck or equivalent) on restart.

## Primary Storage Outage and Data Loss

When a primary storage outage occurs the hypervisor immediately stops all VMs stored on that storage device. Guests that are marked for HA will be restarted as soon as practical when the primary storage comes back on line. With NFS, the hypervisor may allow the virtual machines to continue running depending on the nature of the issue. For example, an NFS hang will cause the guest VMs to be suspended until storage connectivity is restored.

In the event of data loss impacting a primary storage resource the administrator should restore the primary storage file system to the most recent point in time that is available. Once the primary storage has been restored the virtual machines stored on that storage may be restarted. Any changes between the point in time of the restore and the time of the data loss event will be lost.

The administrator can restore individual virtual machines from the backup if the end user deletes a virtual machine by mistake.

## Secondary Storage Outage and Data Loss

A secondary storage outage will have feature level impact to the system but will not impact running guest VMs. It may become impossible to create a VM with the selected template for a user. A user may also not be able to save snapshots or examine/restore saved snapshots. These features will automatically be available when the secondary storage comes back online.

Secondary storage data loss will impact recently added user data including templates, snapshots, and ISO images.

## HA-Enabled VM (Service Provider and Enterprise Edition)

The user can specify a virtual machine as HA-enabled.

The system detects HA-enabled VM crashes and restarts the VM automatically within the same Availability Zone. HA is never performed across different Availability Zones.

The CloudStack platform has a conservative policy towards restarting VMs and ensures that there will never be two instances of the same VM running at the same time. The Management Server attempts to start the VM on another Computing Node in the same Pod.

Users will be alerted when the system performs an HA failover.

All virtual router VMs are automatically configured as HA-enabled.

HA features work with iSCSI or NFS primary storage. HA with local storage is not supported.

# Management Features

## Users, Administrators, and Domains

There are two types of users in the system: administrators and users. Both administrators and users are created in a particular domain. A domain is a set of users and administrators with some logical relationship. For example, they may be in the same department or they may be customers of the same reseller.

Domains can have other domains as their members. This creates a hierarchy of domains. This hierarchy can be arbitrarily deep.

Administrators can perform operations across users in their domain and its subdomains. There is a ROOT domain that has no parent. Administrators in the ROOT domain are root administrators.

There may be multiple administrators in the system. Administrators can create or delete other administrators.

### Root Administrators

Root administrators have complete access to the system, including managing templates, service offerings, customer care administrators, and domains.

### Domain Administrators

Domain administrators can perform administrative operations for users who belong to that domain. Domain administrators do not have visibility into physical servers or other domains.

## Provisioning

### Register

Users must be provisioned and modified through the provisioning API. The following user attributes are specified through the provisioning API:

* Email address and user name (may be the same)
* First and last names
* A callback authentication function or encrypted password
* Reseller ID

## VM Lifecycle Management

The CloudStack platform provides administrators with complete control over the lifecycle of all guest VMs executing in the cloud.

### VM Creation

Virtual machines are usually created from a template. They may be created from a blank VM booted off an ISO.

### VM Deletion

Users can delete their own virtual machines. A running virtual machine will be abruptly stopped before it is deleted.

Administrators can delete any virtual machines.

### VM Lifecycle

Virtual machines can be in the following states:

Start

Stop

Rebootot

Destroy

Start

Fail

Once a virtual machine is destroyed, it cannot be recovered. All the resources used by the virtual machine will be reclaimed by the system. This includes the virtual machine’s IP address.

A stop will attempt to gracefully shut down the operating system, which typically involves terminating all the running applications. If the operation system cannot be stopped, it will be forcefully terminated. This has the same effect as pulling the power cord to a physical machine.

A reboot is a stop followed by a start.

Unlike Amazon EC2, the system preserves the state of the virtual machine hard disk until the machine is destroyed.

A running virtual machine may fail because of hardware or network issues. A failed virtual machine is in the down state.

The system places the virtual machine into the down state if it does not receive the heartbeat from the hypervisor for three minutes.

The hard disk image is preserved when a virtual machine enters the down state.

The user can manually restart the virtual machine from the down state.

The system will start the virtual machine from the down state automatically if the virtual machine is marked as HA-enabled.

### Remote Access

The user is able to access virtual machine console through the web management UI.

Administrators can access the virtual machine consoles that belong to any users for the purpose of support and troubleshooting. The administrators will be subject to providing the root (or other) password for the guest.

## PV Drivers

Windows and Ubuntu 10 require PV drivers to be added in either the template or after install for the CloudStack platform management functions to work properly. The PV drivers allow functions such as mounting additional volumes and ISO images, live migration, and graceful shutdown.

## Administrator Alerts

Emails will be sent to administrators under the following circumstances:

1. The Management Server cluster runs low on CPU, memory, or storage resources
2. The Management Server loses heartbeat from a Computing Node for more than 3 minutes
3. The Computing Node cluster runs low on CPU, memory, or storage resources

## Event Logs

The system records in the database a detailed event log of all the activities performed by users and administrators. The event log contains the user name, date/time stamp, and the relevant details of the activity.

Database logs can be queried from the user interface. The list of events captured by the system includes:

* Virtual machine creation, deletion, and on-going management operations
* Virtual router creation, deletion, and on-going management operations
* Template creation and deletion
* Network/load balancer rules creation and deletion
* Storage volume creation and deletion
* User login and logout

The full list of event types are:

VM.CREATE

VM.DESTROY

VM.START

VM.STOP

VM.REBOOT

VM.DISABLEHA

VM.ENABLEHA

VM.UPGRADE

VM.RESETPASSWORD

ROUTER.CREATE

ROUTER.DESTROY

ROUTER.START

ROUTER.STOP

ROUTER.REBOOT

ROUTER.HA

PROXY.CREATE

PROXY.DESTROY

PROXY.START

PROXY.STOP

PROXY.REBOOT

PROXY.HA

VNC.CONNECT

VNC.DISCONNECT

NET.IPASSIGN

NET.IPRELEASE

NET.RULEADD

NET.RULEDELETE

NET.RULEMODIFY

PF.SERVICE.APPLY

PF.SERVICE.REMOVE

SECGROUP.APPLY

SECGROUP.REMOVE

LB.CREATE

LB.DELETE

USER.LOGIN

USER.LOGOUT

USER.CREATE

USER.DELETE

USER.UPDATE

TEMPLATE.CREATE

TEMPLATE.DELETE

TEMPLATE.UPDATE

TEMPLATE.COPY

TEMPLATE.DOWNLOAD.START

TEMPLATE.DOWNLOAD.SUCCESS

TEMPLATE.DOWNLOAD.FAILED

VOLUME.CREATE

VOLUME.DELETE

VOLUME.ATTACH

VOLUME.DETACH

SERVICEOFFERING.CREATE

SERVICEOFFERING.UPDATE

SERVICEOFFERING.DELETE

DOMAIN.CREATE

DOMAIN.DELETE

DOMAIN.UPDATE

SNAPSHOT.CREATE

SNAPSHOT.DELETE

SNAPSHOTPOLICY.CREATE

SNAPSHOTPOLICY.UPDATE

SNAPSHOTPOLICY.DELETE

ISO.CREATE

ISO.DELETE

ISO.COPY

ISO.ATTACH

ISO.DETACH

SSVM.CREATE

SSVM.DESTROY

SSVM.START

SSVM.STOP

SSVM.REBOOT

SSVM.HA

## Working with Server Logs

The CloudStack Management Server logs all web site, middle tier, and database activities for diagnostics purposes in /var/log/cloud/management/.

The CloudStack Agent Server (present in the Community Edition) logs its activities in /var/log/cloud/agent/.

## Limits

The CloudStack platform provides several administrator control points for capping resource usage by users. Some of these limits are global configuration parameters. Others are applied at the ROOT domain and may be overridden on a per-account basis.

### Configuration Limits

On a Zone the guest virtual network has a 24 bit CIDR by default. This limits the guest virtual network to 254 running instances. It can be adjusted as needed, but this must be done before any instances are created in the Zone. For example, 10.1.1.0/22 would provide for ~1000 addresses.

The following table lists limits set on in the Global Configuration.

|  |  |
| --- | --- |
| **Parameter Name** | **Definition** |
| max.template.iso.size | Maximum size for a downloaded template or ISO in GB |
| max.volume.size.gb | Maximum size for a volume in GB |
| multicast.throttling.rate | Default multicast rate in megabits per second allowed |
| network.throttling.rate | Default data transfer rate in megabits per second allowed per user |
| snapshot.max.hourly | Maximum hourly snapshots for a volume |
| snapshot.max.daily | Maximum daily snapshots for a volume |
| snapshot.max.weekly | Maximum weekly snapshots for a volume |
| snapshot.max.monthly | Maximum monthly snapshots for a volume |

### ROOT Domain Limits

The following limits are set at the ROOT domain and may be overridden on a per-account basis.

* Number of instances a user can create.
* Number of public IP addresses a user can own.
* Number of disk volumes a user can create.
* Number of snapshots a user can create.
* Number of templates that a user can register/create.

# Working with Computing Nodes

## Adding Computing Nodes with Community Edition

Additional Computing Nodes may be added at any time. The Computing Node will register itself with the Management Server (thereby adding itself) after the Agent is installed on it. The Node is then listed in the Hosts tab in the web UI.

## Adding Computing Nodes with Service Provider and Enterprise Edition

Additional Computing Nodes may be added at any time up to the limit of nodes in a Pod. This limit is sixteen.

The administrator can use the Add Host function in the Hosts tab in the web UI to add a new XenServer host. An API call may be made as well.

## Scheduled Maintenance and Maintenance Mode

The administrator can manually place a Computing Node into scheduled maintenance mode. When this is requested the Computing Node first moves into the Prepare for Maintenance state. In this state it cannot be the target of new guest VM starts. Then all VMs will be migrated off the server. With the Service Provider Edition and Enterprise Edition, live migration will be used. This allows the guests to be migrated to other Computing Nodes with no disruption to the guests. After this migration is completed the Computing Node enters the Ready for Maintenance mode. During this time the administrator can perform whatever actions are necessary. After maintenance is done the server will rejoin the cloud after it boots up. It cannot be the target of new VM allocations until the administrator cancels maintenance for it. When the Computing Node comes back online, no VMs that were migrated off of it are migrated back to it.

## Removing Computing Nodes

Computing Nodes can be removed from the cloud as needed. A node cannot be removed from a Pod until all of the VMs on it have been migrated off and it is in maintenance mode.

## Computing Node Allocation

The system automatically picks the most appropriate Computing Node to host virtual machines. End users may specify the Availability Zone in which the virtual machine will be created. End users do not have control over which Computing Node will host the virtual machine instance.

### OS Preferences

The CloudStack platform allows administrators to specify that certain Computing Nodes should have a preference for particular types of guest instances. For example, an administrator could state that a Computing Node should have a preference to run Windows guests. If this is set the default Computing Node allocator will attempt to place guests of that OS type on such nodes first. If no such node is available the allocator will place the node wherever there is sufficient physical capacity.

### Over-Provisioning

The CloudStack platform does not perform memory over provisioning.

The CloudStack platform performs CPU over-provisioning based on an over-provisioning ratio configured by the administrator.

# Working with Usage

The Usage Server provides aggregated usage records. It provides billing integration for the CloudStack platform. The Usage Server works by taking data from the events log, and then creating summary usage records for access via the listUsageRecords API call.

The Usage Server runs at least once per day. It can be configured to run multiple times per day. Its behavior is controlled by the following Configuration table settings.

|  |  |
| --- | --- |
| **Parameter Name** | **Parameter Definition** |
| usage.stats.job.exec.time | This is the time that the Usage Server processing will start. It is specified in 24-hour format in the time zone of the server, which should be GMT. For example, to start the Usage job at 10:30 GMT, enter “10:30”.  **Note: The Usage server processing may run multiple times per day depending on the value of usage.stats.job.aggregation.range.** |
| usage.aggregation.timezone | The usage records are calculated on intervals based on this time zone. The CloudStack Management Server is expected to be in GMT. This parameter more accurately tells the Usage Server when a day ends for the user population. Valid values for the time zone are specified in Appendix A—Time Zones. |
| usage.stats.job.aggregation.range | This is the time period in minutes between Usage server processing jobs. For example, if you set it to 1440 the Usage server will run once per day. If you set it to 600 it will run every ten hours. In general, when a Usage server job runs it processes all events generated since usage was last run.  There is special handling for the case of 1440 (once per day). In this case the Usage Server does not necessarily process all records since Usage was last run. The CloudStack platform assumes that you require processing once per day for the previous, complete day’s records. For example, if the current day is October 7 then you would like to process records for October 6, from midnight to midnight. The CloudStack platform assumes this “midnight to midnight” is relative to the usage.aggregation.timezone. |

For example, suppose that your server is in GMT, your user population is predominantly in the East Coast of the United States, and you would like to process usage records every night at 2 AM local (EST) time. Choose these settings:

* **usage.stats.job.exec.time** = 07:00. This will run the Usage job at 2:00 AM EST. Note that this will shift by an hour as the East Coast of the U.S. enters and exits Daylight Savings Time.
* **usage.aggregation.timezone** = America/New\_York
* **usage.stats.job.aggregation.range** = 1440

With this configuration, the Usage job will run every night at 2 AM EST and will process records for the previous day’s midnight-midnight as defined by the EST (America/New\_York) time zone.

**Note: Because the special value 1440 has been used for usage.stats.job.aggregation.range the Usage Server will ignore the data between midnight and 2 AM.**

# User Interface and API

## User Interface

The system supports both an administrator interface and an end user interface.

### Admin User Interface

The Admin UI supports the following functionalities:

* Service offering management
* User management
* Template management
* Virtual machine management
* Server management
* Storage management
* Network management
* Events
* Initial set up
* Dashboard

### End User Interface

The end user UI is an AJAX-based UI available in popular browsers including IE7, IE8, Firefox 3, and Safari 4. It offers a number of features for end users:

* Service Offering Description
* Template Management
* Virtual Machine Management
* Network Management
* Event Logs
* Snapshot Management
* Dashboard

## API

The CloudStack API is a low level API that has been used to implement the web UI’s. It is also a good basis for implementing other popular API’s such as EC2/S3 and emerging DMTF standards.

The 2.0 API has had structural changes to make many of the calls that were previously synchronous are now asynchronous. These calls will return a Job ID immediately when called. This Job ID can be used to query the status of the job later. Also, status calls on impacted resources will provide some indication of their state.

The API has a REST-like query basis and returns results in XML or JSON.

The complete API is available at http://open.cloud.com.

### Provisioning and Authentication API

The CloudStack platform expects that a customer will have their own user provisioning infrastructure. It provides APIs to integrate with these existing systems where the systems call out to the CloudStack platform to add/remove users.

The CloudStack platform support pluggable authenticators. By default the CloudStack platform assumes it is provisioned with the user’s password, and as a result authentication is done locally. However, external authentication (E.g. via LDAP) is possible as well.

### Allocators

The CloudStack platform enables administrators to write custom allocators that will choose the Computing Node to place a new guest and the storage host from which to allocate guest virtual disk images.

### User Data and Meta Data

The CloudStack platform provides API access to attach user data to a deployed VM. Deployed VMs also have access to instance metadata via the virtual router.

User data can be accessed once the IP address of the virtual router is known. Once the IP address is known, use the following steps to access the user data:

1. Run the following command to find the virtual router.

# cat /var/lib/dhclient/dhclient-eth0.leases | grep dhcp-server-identifier | tail -1

1. Access user data by running the following command using the result of the above command.

# curl <http://10.1.1.1/latest/user-data>

Meta Data can be accessed similarly, using a URL of the form http://10.1.1.1/latest/{metadata type}. The following are the possible metadata types.

* **service-offering**. A description of the VMs service offering.
* **availability-zone**. The Zone name.
* **local-ipv4**. The guest IP of the VM.
* **local-hostname**. The hostname of the VM.
* **public-ipv4**. The first public IP for the router. (E.g. the first IP of eth2)
* **public-hostname**. This is the same as public-ipv4.
* **instance-id**. The instance name of the VM.

# Appendix A—Time Zones

The following time zone identifiers are accepted by the CloudStack API. There are several places that have a time zone as a required or optional parameter. These include scheduling recurring snapshots, creating a user, and specifying the usage time zone in the Configuration table.

Etc/GMT+12

Etc/GMT+11

Pacific/Samoa

Pacific/Honolulu

US/Alaska

America/Los\_Angeles

Mexico/BajaNorte

US/Arizona

US/Mountain

America/Chihuahua

America/Chicago

America/Costa\_Rica

America/Mexico\_City

Canada/Saskatchewan

America/Bogota

America/New\_York

America/Caracas

America/Asuncion

America/Cuiaba

America/HalifaxAmerica/La\_Paz

America/Santiago

America/St\_Johns

America/Araguaina

America/Argentina/Buenos\_Aires

America/Cayenne

America/Godthab

America/Montevideo

Etc/GMT+2

Atlantic/Azores

Atlantic/Cape\_Verde

Africa/Casablanca

Etc/UTC

Atlantic/Reykjavik

Europe/London

CET

Europe/Bucharest

Africa/Johannesburg

Asia/Beirut

Africa/CairoAsia/Jerusalem

Europe/Minsk

Europe/Moscow

Africa/Nairobi

Asia/Karachi

Asia/Kolkata

Asia/Bangkok

Asia/Shanghai

Asia/Kuala\_Lumpur

Australia/Perth

Asia/Taipei

Asia/Tokyo

Asia/Seoul

Australia/Adelaide

Australia/Darwin

Australia/Brisbane

Australia/Canberra

Pacific/Guam

Pacific/Auckland

1. The steps outlined here are derived from the excellent guide by Charity Shelbourne, originally published at the following URL. <http://blogs.technet.com/askcore/archive/2008/10/31/automating-the-oobe-process-during-windows-server-2008-sysprep-mini-setup.aspx> [↑](#footnote-ref-1)