Apache CloudStack 4.1.0

CloudStack 管理元指南

Apache CloudStack

Apache CloudStack 4.1.0 CloudStack 管理元指南

作者 Apache CloudStack

CloudStack 管理指南

概念

1.1. 甚麼是CloudStack?

CloudStack 是一個開放原始碼的軟體，將運算資源抽象化成一整個資源庫提供了公有、私有以及混和式的雲端平台服務(IAAS)。CloudStack具備了管理網路、儲存裝置和計算資源的能力，使用者可以運用 CloudStack 部屬、管理、設定雲端環境

一般使用者為服務提供者及企業，有了CloudStack，您可以:

- 依照需求建立一個具備彈性的雲端服務，網路服務提供業者可以販售虛擬機、儲存服務、網路設定服務。
- 建立一個只提供內部員工所使用的私有雲服務，與傳統管理實體主機的方式有所不同，企業員工不需透過IT部門即可自助式的使用虛擬機

1.2. What Can CloudStack Do?

Multiple Hypervisor Support

CloudStack works with a variety of hypervisors, and a single cloud deployment can contain multiple hypervisor implementations. The current release of CloudStack supports pre-packaged enterprise solutions like Citrix XenServer and VMware vSphere, as well as KVM or Xen running on Ubuntu or CentOS.

Massively Scalable Infrastructure Management

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

Automatic Configuration Management

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

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

Graphical User Interface

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

API and Extensibility

CloudStack provides an API that gives programmatic access to all the management features available in the UI. The API is maintained and documented. This API enables the creation of command line tools and new user interfaces to suit particular needs. See the Developer's Guide and API Reference, both available at Apache CloudStack Guides[1] and Apache CloudStack API Reference[2] respectively.

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

High Availability

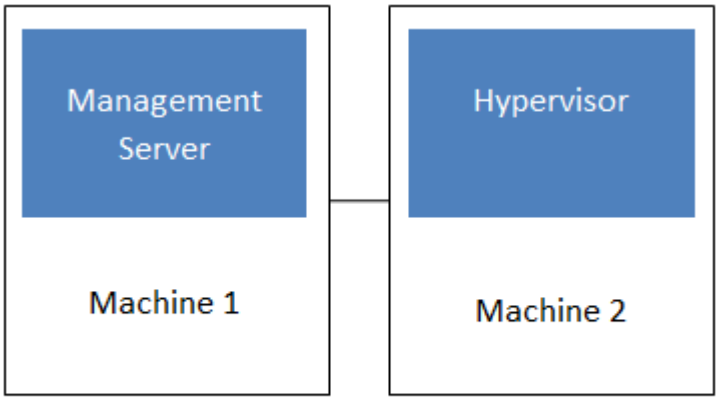
CloudStack has a number of features to increase the availability of the system. The Management Server itself may be deployed in a multi-node installation where the servers are load balanced. MySQL may be configured to use replication to provide for a manual failover in the event of database loss. For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

1.3. 架設架構總攬

CloudStack的安裝包含兩個部分：管理伺服器及雲端基礎架構，當您架設及管理一個CloudStack雲端時，您需要提供如主機、儲存裝置及IP位址等資源給管理伺服器，而管理伺服器幫您管理這些資源

產品的最少安裝包含一個執行CloudStack管理伺服器的機器及雲端基礎架構的機器(這個例子是只包含一個執行超級監督者程式的主機)，在最小的架構中，一個機器可以同時執行管理伺服器及超級監督者主機(使用 KVM hypervisor)

[1] http://cloudstack.apache.org/docs/en-US/index.html
[2] http://cloudstack.apache.org/docs/api/index.html



Simplified view of a basic deployment

完全安裝包含多點管理伺服器及上千上萬使用多種進階網路設定的主機，更多資訊詳見 SPRODUCT;安裝指南的"Choosing a Deployment Architecture"部分

1.3.1. Management Server Overview

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

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

The machine must meet the system requirements described in System Requirements.

The Management Server:

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

1.3.2. 雲端基礎架構簡介

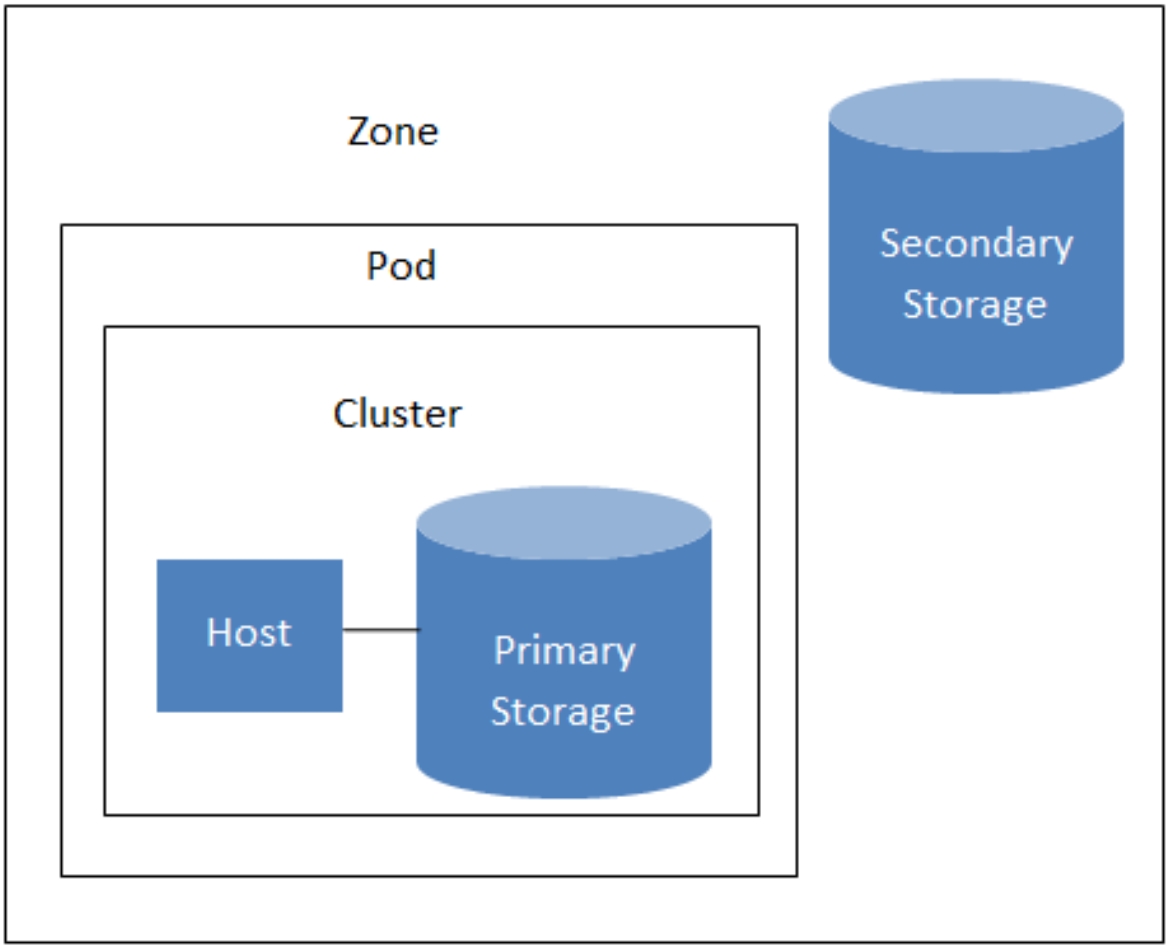
管理伺服器管理多個區域(通常為資料中心)，包含訪客虛擬機器的主機，雲端基礎架構可以組織為下:

- Zone: 通常，區域等於一個資料中心。區域包含一至多個pods極次要儲存裝置
- Pod: 通常是一層硬體架構，包含 layer-2交換器及一至多個叢集
- Cluster: 通常包含一至多個主機及主要儲存裝置

・Host：叢集中的運算節點，以訪客虛擬機器的形式在實際的雲端運行

・主要儲存裝置連結到叢集，存放所有VM的硬碟容量

・次要儲存裝置連結到區域，儲存模組、ISO映像及硬碟容量快取物件



Nested organization of a zone

More Information

更多資訊，請參閱cloud infrastructure concepts的文件

1.3.3. 網路簡介

CloudStack提供兩種網路範本：

・基本。為類似AWS模式的網路架構，提供layer-3的Security group安全機制(IP位置過濾機制)

・進階。 提供使用者更多的網路拓撲結構，選擇此選項將可更彈性的設定網路

更多細節，見Network Setup

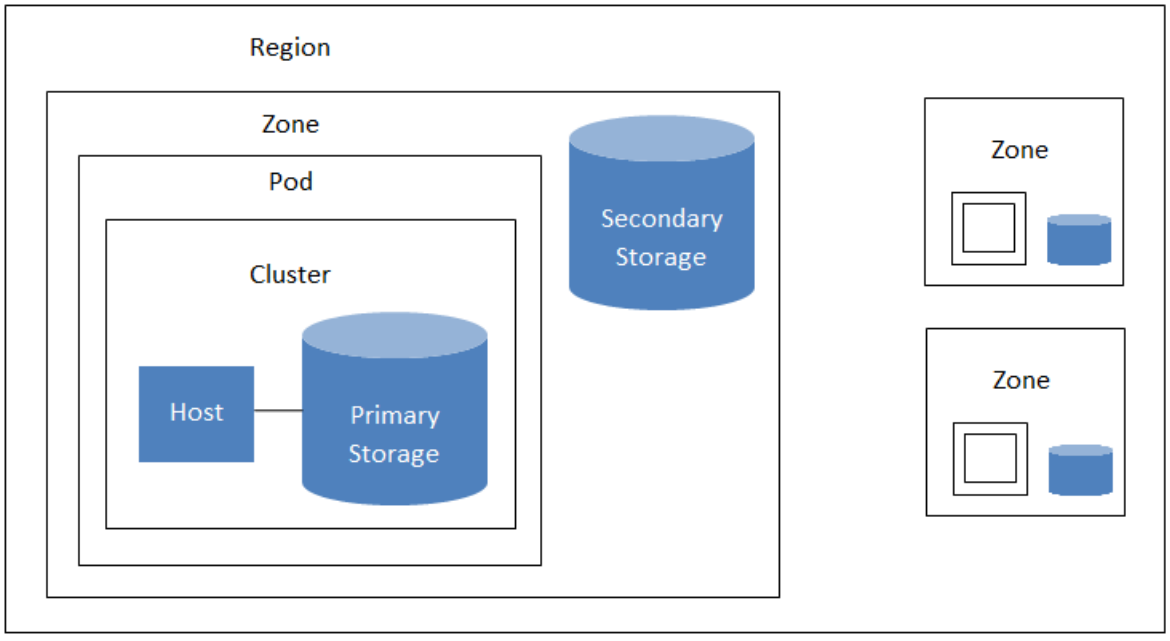
雲端基礎架構概念

2.1. About Regions

To increase reliability of the cloud, you can optionally group resources into multiple geographic regions. A region is the largest available organizational unit within a CloudStack deployment. A region is made up of several availability zones, where each zone is roughly equivalent to a datacenter. Each region is controlled by its own cluster of Management Servers, running in one of the zones. The zones in a region are typically located in close geographical proximity. Regions are a useful technique for providing fault tolerance and disaster recovery.

By grouping zones into regions, the cloud can achieve higher availability and scalability. User accounts can span regions, so that users can deploy VMs in multiple, widely-dispersed regions. Even if one of the regions becomes unavailable, the services are still available to the end-user through VMs deployed in another region. And by grouping communities of zones under their own nearby Management Servers, the latency of communications within the cloud is reduced compared to managing widely-dispersed zones from a single central Management Server.

Usage records can also be consolidated and tracked at the region level, creating reports or invoices for each geographic region.



A region with multiple zones

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

2.2. 關於區域

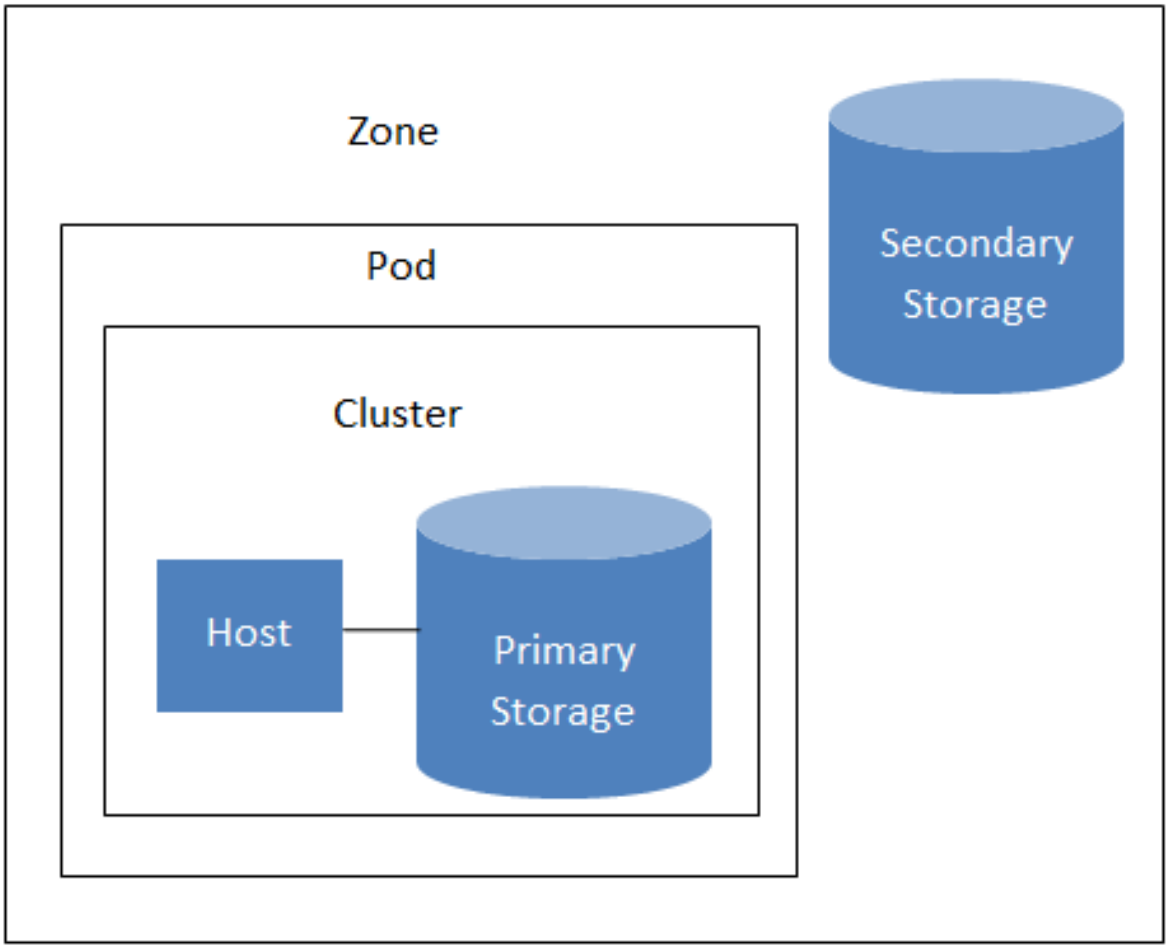
A zone is the second largest organizational unit within a CloudStack deployment. A zone typically corresponds to a single datacenter, although it is permissible to have multiple

zones in a datacenter. The benefit of organizing infrastructure into zones is to provide physical isolation and redundancy. For example, each zone can have its own power supply and network uplink, and the zones can be widely separated geographically (though this is not required).

一個區域包含:

・一至多個pod。每個pod包含一至多個叢集主機及主要儲存伺服器

・次要儲存裝置，所有pod共享



Nested organization of a zone

終端使用者可以看到區域，當使用者啓動訪客VM時，必須選擇一個區域。或是會需要複製自己的私人模組到其他區域來建立訪客VM

區域可為公開或私人。公開區域為所有使用者都可見，任意使用者都可以建立訪客帳戶；私人區域僅為特定網域，僅網域或其子網域中的使用者能建立訪客帳戶

相同區域的主機可以不經過防火牆而互相通信。不同區域的主機則需要透過固定設定的VPN通道

美個區域的管理者必須決定以下:

・多少pod

・多少叢集

・多少主機

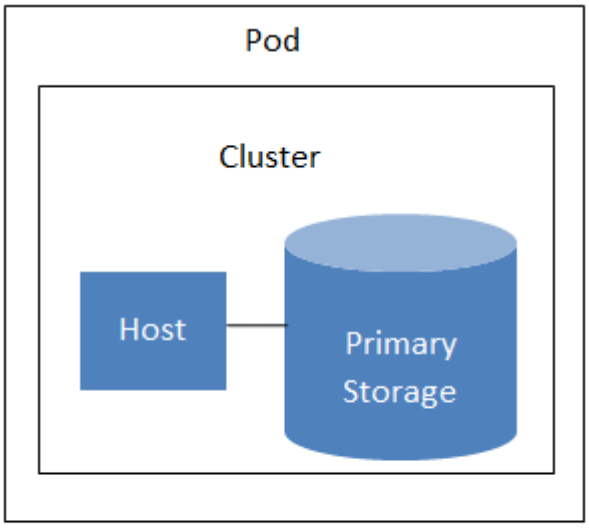
・多少主要儲存裝置及總容量

・多少次要儲存裝置

當您新增一個區域時，您會被提示設定該區域的實體網路及增加第一個pod、叢集、主要儲存裝置及次要儲存裝置

2.3. 關於Pods

Pod通常代表一個單一的架子，同一個pod的主機會有相同的子網路。pod是CloudStack架構中第二大的組織單位，而pod包含在zone之下，每個zone都包含一至多個pod；每一個pod都包含一至多個cluster主機及主要儲存裝置，並且終端使用者是看不見的



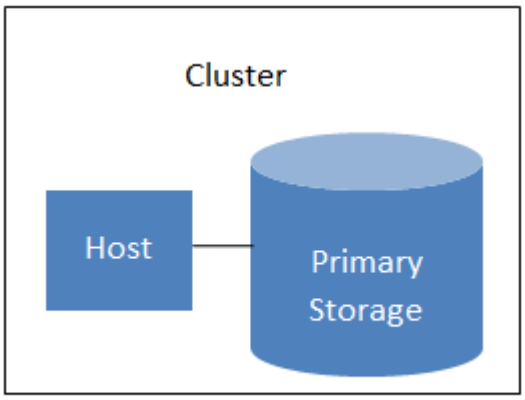
A simple pod

2.4. 關於Clusters

CloudStack所定義的群組是一群實體主機的集合，更精確的說，一個群組可以是一群XenServer主機的集合、一群KVM主機的集合，甚至是一個於VCenter中預先配置好的VMWare集合。群組中的主機擁有相同的硬體、使用相同的Hypervisor、運行於相同的子網路、並且存取相同的主存儲。在同一個群組下的虛擬機器(VMs)可以在不中斷的情況下從一台主機，搬移到另一台主機上。

群組在CloudStack中是第三大的集合單位;

一個cluster的組成至少含有一個(或以上)實體主機，並還有至少一個擁有一個(或以上)的主要儲存裝置



A simple cluster

CloudStack允許環境中擁有多個cluster

即使採用了本機端的儲存設定，Cluster仍然是需要的，在這個情況下，一個Cluster只能擁有一台主機

當使用VMware時，每一個VMware的cluster是有vCenter所管理，管理者需將vCenter於CloudStack中註冊。每個Zone可以擁有多個vCenter伺服器、而每一個vCenter伺服器可以控制多個VMware cluster

2.5. About Hosts

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

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

Hosts in a CloudStack deployment:

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

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

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

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

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

- Install hypervisor software on the host
- Assign an IP address to the host

- Ensure the host is connected to the CloudStack Management Server

2.6. About Primary Storage

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

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

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

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

2.7. About Secondary Storage

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

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

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

To make items in secondary storage available to all hosts throughout the cloud, you can add OpenStack Object Storage (Swift, swift.openstack.org[1]) in addition to the zone-based NFS secondary storage. When using Swift, you configure Swift storage for the entire CloudStack, then set up NFS secondary storage for each zone as usual. The NFS storage in each zone acts as a staging area through which all templates and other secondary storage data pass before being forwarded to Swift. The Swift storage acts as a cloud-wide resource, making templates and other data available to any zone in the cloud. There is no hierarchy in the Swift storage, just one Swift container per storage object. Any secondary storage in the whole cloud can pull a container from Swift at need. It is not necessary to copy templates and snapshots from one zone to another, as would be required when using zone NFS alone. Everything is available everywhere.

2.8. About Physical Networks

Part of adding a zone is setting up the physical network. One or (in an advanced zone) more physical networks can be associated with each zone. The network corresponds to a

[1] http://swift.openstack.org

NIC on the hypervisor host. Each physical network can carry one or more types of network traffic. The choices of traffic type for each network vary depending on whether you are creating a zone with basic networking or advanced networking.

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

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

2.8.1. Basic Zone Network Traffic Types

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

- Guest. When end users run VMs, they generate guest traffic. The guest VMs communicate with each other over a network that can be referred to as the guest network. Each pod in a basic zone is a broadcast domain, and therefore each pod has a different IP range for the guest network. The administrator must configure the IP range for each pod.
- Management. When CloudStack's internal resources communicate with each other, they generate management traffic. This includes communication between hosts, system VMs (VMs used by CloudStack to perform various tasks in the cloud), and any other component that communicates directly with the CloudStack Management Server. You must configure the IP range for the system VMs to use.

注意

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

- Public. Public traffic is generated when VMs in the cloud access the Internet. Publicly accessible IPs must be allocated for this purpose. End users can use the CloudStack UI to acquire these IPs to implement NAT between their guest network and the public network, as described in Acquiring a New IP Address.
- Storage. While labeled "storage" this is specifically about secondary storage, and doesn't affect traffic for primary storage. This includes traffic such as VM templates and snapshots, which is sent between the secondary storage VM and secondary storage servers. CloudStack uses a separate Network Interface Controller (NIC) named storage NIC for storage network traffic. Use of a storage NIC that always operates on a high

bandwidth network allows fast template and snapshot copying. You must configure the IP range to use for the storage network.

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

2.8.2. Basic Zone Guest IP Addresses

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

2.8.3. Advanced Zone Network Traffic Types

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

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

- Management. When CloudStack's internal resources communicate with each other, they generate management traffic. This includes communication between hosts, system VMs (VMs used by CloudStack to perform various tasks in the cloud), and any other component that communicates directly with the CloudStack Management Server. You must configure the IP range for the system VMs to use.

- Public. Public traffic is generated when VMs in the cloud access the Internet. Publicly accessible IPs must be allocated for this purpose. End users can use the CloudStack UI to acquire these IPs to implement NAT between their guest network and the public network, as described in "Acquiring a New IP Address" in the Administration Guide.

- Storage. While labeled "storage" this is specifically about secondary storage, and doesn't affect traffic for primary storage. This includes traffic such as VM templates and snapshots, which is sent between the secondary storage VM and secondary storage servers. CloudStack uses a separate Network Interface Controller (NIC) named storage NIC for storage network traffic. Use of a storage NIC that always operates on a high bandwidth network allows fast template and snapshot copying. You must configure the IP range to use for the storage network.

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

2.8.4. Advanced Zone Guest IP Addresses

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

2.8.5. Advanced Zone Public IP Addresses

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

2.8.6. 系統保留IP位址

在每個區域，您需要設定一組保留IP範圍給管理網路，此網路保持CloudStack管理伺服器及多種系統虛擬機器，如次要儲存虛擬機器、控制台代理虛擬機器及DHCP，間的通信

保留IP必須在雲端中是唯一的，您不行有個主機在一個區域和另一個區域內的主機有相同的私人IP位址

pod中的主機會指定私人IP位址，通常為RFC1918 位址。控制台代理及次要儲存裝置系統虛擬機器也會在pod中的CIDR分配私人IP位址

請確定計算伺服器及管理伺服器使用不是保留IP範圍內的IP位址。例如，假設保留IP範圍為 192.168.154.2到 192.168.154.7，則 CloudStack的系統虛擬機器可以使用.2到.7的IP，而pod CIDR就分.8 到 .254給管理伺服器及超級監督者主機

In all zones:

提供私人IP給每個pod中的系統，並提供給CloudStack

對於KVM及XenServer，建議每個pod的私人IP數量為每個主機1個，如果您希望pod持續增長，請加入足夠的私人IP

In a zone that uses advanced networking:

對於使用進階網路的區域，建議提拱足夠的私人IP給您所有的客戶，以及CloudStack 系統虛擬機器需要的數量。通常系統虛擬機器需要10個額外的IP。更多資訊，詳見管理者指南的Working with System Virtual Machines

當進階網路被使用時，每個pod中的可用私人IP數量會依超級監督者的類型不同而不同。 Citrix XenServer 及 KVM使用連接本地的位址，理論上提供超過65,000個私人IP位址。隨著pod增長，這些應該是足夠的。 VMWare ESXi，相較之下，使用任一管理者限定的子網域計畫，以及典型的管理者，提供每個pod僅255個IP。因為這些IP與實體機器、訪客虛擬路由器及其他可操作的單位。私人IP可能會不夠用

使用一個或全部以下的技術來確保足夠的擴展高度給使用進階網路的ESXi pod中的私人IP空間

- 指定一個大的CIDR給子網路，使用 /20 字尾的子遮罩可以提供超過4,000個IP位址
- 建立多個pod，並有自己的子網域。例如，如果您建立10個pod，每個pod有255個IP，這樣就有總共2,550個IP位址

Accounts

3.1. Accounts, Users, and Domains

Accounts

An account typically represents a customer of the service provider or a department in a large organization. Multiple users can exist in an account.

Domains

Accounts are grouped by domains. Domains usually contain multiple 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.

For each account created, the Cloud installation creates three different types of user accounts: root administrator, domain administrator, and user.

Users

Users are like aliases in the account. Users in the same account are not isolated from each other, but they are isolated from users in other accounts. Most installations need not surface the notion of users; they just have one user per account. The same user cannot belong to multiple accounts.

Username is unique in a domain across accounts in that domain. The same username can exist in other domains, including sub-domains. Domain name can repeat only if the full pathname from root is unique. For example, you can create root/d1, as well as root/foo/d1, and root/sales/d1.

Administrators are accounts with special privileges in the system. There may be multiple administrators in the system. Administrators can create or delete other administrators, and change the password for any user in the system.

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.

Root Administrator

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

The resources belong to the account, not individual users in that account. For example, billing, resource limits, and so on are maintained by the account, not the users. A user can operate on any resource in the account provided the user has privileges for that operation. The privileges are determined by the role.

3.2. 使用LDAP Server來使用者認證

您可以使用外部LDAP server，像是 Microsoft Active Directory 或ApacheDS，來認證CloudStack終端使用者，只要使用詢問過濾器對照CloudStack帳戶到相對應的LDAP帳戶即可，此詢問過濾器使用特定LDAP server 的query syntax編寫，並且可以包含由CloudStack提供的特殊wildcard characters，用來比對一般的數值，像是使用者Email及名稱。CloudStack會搜尋外部 LDAP directory tree，由指定的 base directory開始，之後回復對應的使用者distinguished name (DN) 及密碼。此資訊及密碼用來認證使用者

呼叫 CloudStack API command ldapConfig來建立LDAP authenticatio，提供以下：

- 主機名稱或IP位址，以及LDAP server等候的通訊埠
- Base directory 及 query filter
- 搜尋使用者的DN credentials，使CloudStack能在LDAP server上搜尋
- 如果有使用SSL，請提供SSL keystore及 密碼

3.2.1. Example LDAP Configuration Commands

To understand the examples in this section, you need to know the basic concepts behind calling the CloudStack API, which are explained in the Developer's Guide.

The following shows an example invocation of ldapConfig with an ApacheDS LDAP server

```
http://127.0.0.1:8080/client/api?command=ldapConfig&hostname=127.0.0.1&searchbase=ou
%3Dtesting%2Co%3Dproject&queryfilter=%28%26%28uid%3D%25u%29%29&binddn=cn%3DJohn+Singh%2Cou
%3Dtesting%2Co%project&bindpass=secret&port=10389&ssl=true&truststore=C%3A%2Fcompany%2Finfo
%2Ftrusted.ks&truststorepass=secret&response=json&apiKey=YourAPIKey&signature=YourSignatureHash
```

The command must be URL-encoded. Here is the same example without the URL encoding:

```
http://127.0.0.1:8080/client/api?command=ldapConfig
&hostname=127.0.0.1
&searchbase=ou=testing,o=project
&queryfilter=(&(%uid=%u))
&binddn=cn=John+Singh,ou=testing,o=project
&bindpass=secret
&port=10389
&ssl=true
&truststore=C:/company/info/trusted.ks
&truststorepass=secret
&response=json
&apiKey=YourAPIKey&signature=YourSignatureHash
```

The following shows a similar command for Active Directory. Here, the search base is the testing group within a company, and the users are matched up based on email address.

```
http://10.147.29.101:8080/client/api?command=ldapConfig&hostname=10.147.28.250&searchbase=OU%3Dtesting
%2CDC%3Dcompany&queryfilter=%28%26%28mail%3D%25e%29%29 &binddn=CN%3DAdministrator%2COU%3Dtesting%2CDC
%3Dcompany&bindpass=llll_aaaa&port=389&response=json&apiKey=YourAPIKey&signature=YourSignatureHash
```

The next few sections explain some of the concepts you will need to know when filling out the ldapConfig parameters.

3.2.2. Search Base

An LDAP query is relative to a given node of the LDAP directory tree, called the search base. The search base is the distinguished name (DN) of a level of the directory tree below which all users can be found. The users can be in the immediate base directory or in some subdirectory. The search base may be equivalent to the organization, group, or domain name. The syntax for writing a DN varies depending on which LDAP server you are using. A full discussion of distinguished names is outside the scope of our documentation. The following table shows some examples of search bases to find users in the testing department..

LDAP Server	Example Search Base DN
ApacheDS	ou=testing,o=project
Active Directory	OU=testing, DC=company

3.2.3. Query Filter

The query filter is used to find a mapped user in the external LDAP server. The query filter should uniquely map the CloudStack user to LDAP user for a meaningful authentication. For more information about query filter syntax, consult the documentation for your LDAP server.

The CloudStack query filter wildcards are:

Query Filter Wildcard	敘述
%u	User name
%e	Email address
%n	First and last name

The following examples assume you are using Active Directory, and refer to user attributes from the Active Directory schema.

If the CloudStack user name is the same as the LDAP user ID:

```
(uid=%u)
```

If the CloudStack user name is the LDAP display name:

```
(displayName=%u)
```

To find a user by email address:

```
(mail=%e)
```

3.2.4. Search User Bind DN

The bind DN is the user on the external LDAP server permitted to search the LDAP directory within the defined search base. When the DN is returned, the DN and passed password are used to authenticate the CloudStack user with an LDAP bind. A full discussion of bind DNs is outside the scope of our documentation. The following table shows some examples of bind DNs.

LDAP Server	Example Bind DN
ApacheDS	cn=Administrator,dc=testing,ou=project,ou=org
Active Directory	CN=Administrator, OU=testing, DC=company, DC=com

3.2.5. SSL Keystore Path and Password

If the LDAP server requires SSL, you need to enable it in the ldapConfig command by setting the parameters ssl, truststore, and truststorepass. Before enabling SSL for ldapConfig, you need to get the certificate which the LDAP server is using and add it to a trusted keystore. You will need to know the path to the keystore and the password.

User Services Overview

In addition to the physical and logical infrastructure of your cloud, and the CloudStack software and servers, you also need a layer of user services so that people can actually make use of the cloud. This means not just a user UI, but a set of options and resources that users can choose from, such as templates for creating virtual machines, disk storage, and more. If you are running a commercial service, you will be keeping track of what services and resources users are consuming and charging them for that usage. Even if you do not charge anything for people to use your cloud — say, if the users are strictly internal to your organization, or just friends who are sharing your cloud — you can still keep track of what services they use and how much of them.

4.1. Service Offerings, Disk Offerings, Network Offerings, and Templates

A user creating a new instance can make a variety of choices about its characteristics and capabilities. CloudStack provides several ways to present users with choices when creating a new instance:

- Service Offerings, defined by the CloudStack administrator, provide a choice of CPU speed, number of CPUs, RAM size, tags on the root disk, and other choices. See Creating a New Compute Offering.
- Disk Offerings, defined by the CloudStack administrator, provide a choice of disk size for primary data storage. See Creating a New Disk Offering.
- Network Offerings, defined by the CloudStack administrator, describe the feature set that is available to end users from the virtual router or external networking devices on a given guest network. See Network Offerings.
- Templates, defined by the CloudStack administrator or by any CloudStack user, are the base OS images that the user can choose from when creating a new instance. For example, CloudStack includes CentOS as a template. See Working with Templates.

In addition to these choices that are provided for users, there is another type of service offering which is available only to the CloudStack root administrator, and is used for configuring virtual infrastructure resources. For more information, see Upgrading a Virtual Router with System Service Offerings.

使用者介面

5.1. 登入使用者介面

CloudStack 提供了管理者以及使用者的web-based的介面,在您登入系統後,系統會自動為您載入適當的操控介面。使用者介面支援了目前市面常見的瀏覽器類型，例如：IE7、IE8、IE9、Firefox 3.5+、Firefox 4、Safari 4和Safari 5。而URL為:

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

如果您的管理伺服器是新安裝的,將會有安裝精靈引導您進行後續的安裝步驟，若非新安裝，登入後即是您的主控台

使用者帳號

使用者帳號預設是admin

密碼

預設使用者(root)帳號的密碼為password

Domain

如果您是root，此欄位請勿填寫

如果您是sub-domains的使用者,請輸入domain的完整路徑,如果為root domain的使用者,則不需要輸入

舉例來說，root domain底下具有許多階層，例如：Comp1/hr，而在Comp1底下的使用者就必須在Domain欄位輸入Comp1；在Comp1/hr底下的使用者，就必須輸入Comp1/hr

更多關於使用者登入的資訊可以參閱：Loggin In as the Root Administrator

5.1.1. End User's UI Overview

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

5.1.2. Root Administrator's UI Overview

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

5.1.3. 以Root Administrator的身分登入

當管理伺服器以安裝完畢開始運行後，您就可以使用CloudStack的使用者介面。透過此介面，您可以提供、檢視和管理您的雲端系統。

1. 打開您慣用的瀏覽器瀏覽以下網址:

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

登錄進新的Management Server安裝後，會出現引導視窗。之後登錄時，你會直接進入 Dashboard

2. 如果您看到第一次登入的畫面，請選擇以下步驟進行:

- 如果您想簡單試用CloudStack 請選擇Continue with basic setup. ，並且如果您想一個配置一個簡單的環境，CloudStack 的安裝精靈將會引導您繼續進行設定，我們將會幫助您建置一個運行 CloudStack 的單一實體主機; NFS儲存裝置; 一個採用XenServer或是KVM Hypervisor之主機，並擁有一個公開的分享網路。

  安裝精靈將會提供您足夠的資訊，如果您想更深入的了解細節，您可以寄去閱讀Trial Installation Guid。

- 如果您已經經過設計並規劃架設更複雜的環境，或是希望擴充之前的環境，您可以選擇此選項 : I have used CloudStack before.，在管理員介面中，您可以開始使用更複雜但更強大的功能設定，例如: 進階的VLAN網路功能、高可用性功能、額外的網路資源，如load balancers和firewall，以及更多種類的Hypervisor，如: Citrix XenServer、KVM和VMware vSphere。

  root administrator的控制台將呈現在您眼前。

3. 在開始所有的步驟前，您應該為root administrator設置新的密碼。如果您選擇了透過安裝設定精靈的基礎設定，它會提示您輸入新的密碼; 如果您是具經驗的使用者，請透過節 5.1.4，“改變root密碼”中的步驟設定。

警告

如果您是以root administrator登入，此帳號可以對CloudStack做管理、佈署，當然包含了配置實體架構。root administrator可以修改基礎設定、建立或刪除使用者帳號、以及進行需要授權的操作，因此在第一次登入後，記得修改您root administrator的密碼。

5.1.4. 改變root密碼

在安裝及執行雲端管理者時，您需要以root administrator登入，此帳號可以對CloudStack做管理、佈署，當然包含了配置實體架構。root administrator可以修改基礎設定、建立或刪除使用者帳號、以及進行需要授權的操作，因此在第一次安裝CloudStack後，記得修改您root administrator的密碼。

1. 打開您慣用的瀏覽器瀏覽以下網址:

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

2. 使用現在的root使用者ID及密碼登入使用者介面，預設為admin、password
3. 按Accounts
4. 選擇管理帳戶名稱
5. 按 View Users
6. 點選管理使用者名稱

7. 點選Change Password 

8. 輸入新的密碼，然後按OK

5.2. 使用SSH Key授權

除了使用者名稱及密碼授權， CloudStack支援使用SSH key登入雲端，您可以使用createSSHKeyPair API來產生

因為每個雲端使用者有自己的SSH key，兩個使用者將不能登入互相的帳戶除非他們共用，使用一個SSH key pair，您可以管理多個帳戶

5.2.1. 建立支援SSH Key的Instance Template

建立支援SSH Key的Instance Template

1. 使用cloudstack提供的 template新增Instance

   更多關於新增instance的資訊，詳見

2. 下載cloudstack script從The SSH Key Gen Script[1]到您建立的instance

```
wget http://downloads.sourceforge.net/project/cloudstack/SSH%20Key%20Gen%20Script/cloud-set-guest-sshkey.in?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fcloudstack%2Ffiles%2FSSH%2520Key%2520Gen%2520Script%2F&ts=1331225219&use_mirror=iweb
```

3. 將檔案複製到/etc/init.d。

```
cp cloud-set-guest-sshkey.in /etc/init.d/
```

4. 給必要的允許:

```
chmod +x /etc/init.d/cloud-set-guest-sshkey.in
```

5. 執行作業系統時執行script:

```
chkconfig --add cloud-set-guest-sshkey.in
```

6. 停止Instance

5.2.2. 新增SSH Keypair

您必須呼叫 createSSHKeyPair api ，您可以使用CloudStack Python API 或 curl指令來呼叫 cloudstack api

例如， 從 cloudstack 伺服器呼叫 "keypair-doc" 來建立

[1] http://sourceforge.net/projects/cloudstack/files/SSH%20Key%20Gen%20Script/

注意

確保您已修正您需要的數值，如果您從不同伺服器呼叫API，您的URL/PORT會不同，並需要使用API Keys

1. 執行以下curl指令：

```
curl --globoff "http://localhost:8096/?command=createSSHKeyPair&name=keypair-
doc&account=admin&domainid=5163440e-c44b-42b5-9109-ad75cae8e8a2"
```

結果會顯示如下：

```
<?xml version="1.0" encoding="ISO-8859-1"?><createsshkeypairresponse
 cloud-stack-version="3.0.0.20120228045507"><keypair><name>keypair-doc</
name><fingerprint>f6:77:39:d5:5e:77:02:22:6a:d8:7f:ce:ab:cd:b3:56</fingerprint><privatekey>-----BEGIN RSA
 PRIVATE KEY-----
MIICXQIBAAKBgQCSydmnQ67jP61NoXdX3noZjQdrMAWNQZ7y5SrEu4wDxp1vhYci
dXYBeZVwakDVsU2MLG1/K+wefwefwefwefwefJyKJaogMKn7BperPD6n1wIDAQAB
AoGAdXaJ7uyZKeRDoy6wA0UmF0kSPbMZCR+UTIHNkS/E0/4U+61hMokmFSHtu
mfDZ1kGGDYhMsdytjDBzt1jawfawfeawefawfawfawQQDCjEsoRdgkduTy
QpbSGDIa11Jsc+XNDx2fgRinDsxXI/zJYXTKRhS1/LIPHBw/brW8vzxh01SOrwm7
VvemkkgpAkEAwSeEw394LYZiEVv395ar9MLRVTVLwpo54jC4ts0xQCB11oocK
1Yaocpk0yBqq0USBawfIiDCuLXSdvBo1Xz5ICTM19vgvEp/+kMuECQBzm
nVo8b2Gvyagqt/KEQo8wzH2THghZ1qQ1QRhIeJG2aissEacF6bGB2oZ7Igim5L14
4KR70eEToyCLC2k+02UCQQCrniSnWKtDVoVqeK/zbB32JhW3Wu11v5p5zUEcd
KfEEuzcCUIxtJYTahJ1pv1FkQ8anpuxjSEDp8x/18bq3
-----END RSA PRIVATE KEY-----
</privatekey></keypair></createsshkeypairresponse>
```

2. 將資料複製到檔案中，檔案會像：

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCSydmnQ67jP61NoXdX3noZjQdrMAWNQZ7y5SrEu4wDxp1vhYci
dXYBeZVwakDVsU2MLG1/K+wefwefwefwefwefJyKJaogMKn7BperPD6n1wIDAQAB
AoGAdXaJ7uyZKeRDoy6wA0UmF0kSPbMZCR+UTIHNkS/E0/4U+61hMokmFSHtu
mfDZ1kGGDYhMsdytjDBzt1jawfawfeawefawfawfawQQDCjEsoRdgkduTy
QpbSGDIa11Jsc+XNDx2fgRinDsxXI/zJYXTKRhS1/LIPHBw/brW8vzxh01SOrwm7
VvemkkgpAkEAwSeEw394LYZiEVv395ar9MLRVTVLwpo54jC4ts0xQCB11oocK
1Yaocpk0yBqq0USBawfIiDCuLXSdvBo1Xz5ICTM19vgvEp/+kMuECQBzm
nVo8b2Gvyagqt/KEQo8wzH2THghZ1qQ1QRhIeJG2aissEacF6bGB2oZ7Igim5L14
4KR70eEToyCLC2k+02UCQQCrniSnWKtDVoVqeK/zbB32JhW3Wu11v5p5zUEcd
KfEEuzcCUIxtJYTahJ1pv1FkQ8anpuxjSEDp8x/18bq3
-----END RSA PRIVATE KEY-----
```

3. 儲存

5.2.3. 新增Instance

當您儲存好SSH keypair檔案，您必須使用您在節 5.2.1, “建立支援SSH Key的Instance Template”建立的 template建立一個帳戶，確保您使用和相同的 SSH key 名稱

注意

您不行使用GUI來新增及連結Instance新建的SSH keypair

新增Instance 的curl指令的範本如下:

```
curl --globoff http://localhost:<port number>/?command=deployVirtualMachine
\&zoneId=1\&serviceOfferingId=18727021-7556-4110-9322-d625b52e0813\&templateId=e899c18a-
ce13-4bbf-98a9-625c5026e0b5\&securitygroupids=ff03f02f-9e3b-48f8-834d-91b822da40c5\&account=admin
\&domainid=1\&keypair=keypair-doc
```

替換您雲端的template, service offering 和 security group IDs(如果您有使用security group)

5.2.4. 用 SSH Keypair登入

用您是否能登入雲端設定來測試SSH key有沒有建立成功

例如, 在Linux OS執行:

```
ssh -i ~/.ssh/keypair-doc <ip address>
```

-i 變數告訴SSH客戶使用~/.ssh/keypair-doc內的ssh key

5.2.5. 重設

由於有resetSSHKeyForVirtualMachine這個API指令, 使用者可以設定或重設 SSH keypair, 忘掉或有危害的SSH keypair可以被換掉, 使用者可以使用新的keypair存取VM。建立或註冊新的keypair, 然後呼叫 resetSSHKeyForVirtualMachine

使用Projects來管理使用者及資源

6.1. 計畫簡介

計畫用來組織成員及資源，在一網域中的CloudStack 使用者可以組織在一起，並合作及分享資源如VM、快取物件、模組、資料硬碟及IP位址。CloudStack會追蹤每個計劃及使用者的資源使用率，因此可以用來收費。例如，軟體公司的私人雲端可能有QA部門所有成員的計畫，如此公司可以追蹤資源使用來區分計畫成員的努力程度

您可以設定 CloudStack 允許任何使用者建立新的計畫，或是限制為僅CloudStack 管理者能使用。一旦您建立計畫，您就是計劃管理者，您可以加入其他人到計畫中。CloudStack可以建立其中一種，如此您可以直接加入成員或是寄出邀請，計畫成員可以看及管理所有虛擬資源(例如，分享VM)，使用者可以加入任意數量的計畫，而且可以設定僅在CloudStack使用者介面顯示計畫相關的訊息，像是計畫VM、計畫同伴、計畫相關警訊及更多

計劃管理者可以影響其他計畫成員，計畫管理者可以新增成員、移除成員、設定新資源限制(只要低於CloudStack管理者的廣域預設)及刪除計畫，當管理者移除成員，該成員建立的資源，像是VM，仍會存在，這將我們帶到資源擁有的主題及何種資源可以給計劃使用

在計畫內建立的資源由計畫擁有，並且僅能使用在計畫內。擁有多個計劃的使用者可以在計畫外建立資源，而這些資源屬於使用者，並不列入計畫使用計算或受資源限制影響。您可以寄練計畫等級網路來區分流量，以及提供網路服務，像是通訊埠轉送、負載平衡、VPN及static NAT。如果特定類型的資源有分享，計畫也可以從外部使用這些資源。例如，分享網路或公開模組可以給網域內任何計畫使用，如果私人模組有被擁有者允許，計畫就可以存取。計畫可以使用任何服務或硬碟供應，但是不能建立私人服務及硬碟提供

6.2. Configuring Projects

Before CloudStack users start using projects, the CloudStack administrator must set up various systems to support them, including membership invitations, limits on project resources, and controls on who can create projects.

6.2.1. 建立邀請

CloudStack允許計畫管理者直接加入新成員，也可以藉由Email或使用者CloudStack 帳戶寄送來邀請，如果管理者使用邀請來加入成員，請開啓並設定CloudStack的邀請功能

1. 以管理者登入CloudStack 使用者介面
2. 在左邊的導覽視窗，選擇Global Settings
3. 在搜尋列中，輸入計畫然後搜尋 
4. 在搜尋結果，您會看到一些欄位，您需要設定邀請如何作用，下方表格顯示廣域設定，按下編輯鈕來設定參數

設定參數	敘述
project.invite.required	設為true
project.email.sender	Email會顯示在 From欄位
project.invite.timeout	允許新成員回應的時間
project.smtp.host	當作處理邀請的主機名稱

設定參數	敘述
project.smtp.password	(選擇性)SMTP要求的密碼，您必須設定project.smtp.username及project.smtp.useAuth為true
project.smtp.port	SMTP伺服器的等候不
project.smtp.useAuth	如果SMTP伺服器需要使用者名稱及密碼，設為true
project.smtp.username	(選擇性)認證SMTP伺服器要求的使用者名稱，您必須設定project.smtp.password及project.smtp.useAuth為true

5. 重新啓動 Management Server ：

```
service cloudstack-management restart
```

6.2.2. Setting Resource Limits for Projects

The CloudStack administrator can set global default limits to control the amount of resources that can be owned by each project in the cloud. This serves to prevent uncontrolled usage of resources such as snapshots, IP addresses, and virtual machine instances. Domain administrators can override these resource limits for individual projects with their domains, as long as the new limits are below the global defaults set by the CloudStack root administrator. The root administrator can also set lower resource limits for any project in the cloud

6.2.2.1. 設定每個計劃的資源限制

CloudStack root管理者或網域管理者可以為獨立的計畫設定新的資源限制，計畫擁有者只有在自己也是以上兩種管理者時才可以設定資源限制

新的限制需低於CloudStack管理者設定的廣域預設限制(在節 6.2.2, “Setting Resource Limits for Projects”中描述)，如果計畫已經有比新限制多的資源，這些資源不會受影響，但是此計畫就不能再新增資源了，除非降到新限制之下

1. 以管理者登入CloudStack 使用者介面
2. 在左邊的導覽視窗，選擇Projects
3. 於Select View中選擇Projects
4. 選擇你想要套用的計畫
5. 點選Resources標籤，此標籤會列出現在計畫允許使用的資源的最大值
6. 輸入新的數值
7. 按Apply

6.2.2.2. 設定廣域計畫資源的限制

1. 以管理者登入CloudStack 使用者介面
2. 在左邊的導覽視窗，選擇Global Settings
3. 在搜尋欄位裡鍵入max.projects並點選搜尋按鈕。

4. 您會在搜尋結果中看到您可以用來設定每個計劃的最大資源數量的欄位，每個計畫的資源只能低，不能高。點選edit來設定每個參數 

max.project.public.ips	最大數量可以給任何計畫使用的公開IP位址，詳見About Public IP Addresses
max.project.snapshots	最大數量可以給任何計畫使用的快取物件，詳見Working with Snapshots
max.project.templates	最大數量可以給任何計畫使用的模組，詳見Working with Templates
max.project.uservms	最大數量可以給任何計畫使用的訪客虛擬機器，詳見Working With Virtual Machines
max.project.volumes	最大數量可以給任何計畫使用的資料容量，詳見Working with Volumes

5. 重新啓動 Management Server

```
# service cloudstack-management restart
```

6.2.3. 設定允許 Project Creator

您可以設定CloudStack為允許所有使用者可以建立新的計畫，或是僅限CloudStack 管理者

1. 以管理者登入CloudStack 使用者介面
2. 在左邊的導覽視窗，選擇Global Settings
3. 在搜尋欄位裡鍵入allow.user.create.projects並點選搜尋按鈕。
4. 按下edit並設定參數 

allow.user.create.projects	設為"true"使終端使用者可以建立計畫；設為"false"則只有CloudStack root及網域管理者可以建立

5. 重新啓動 Management Server

```
# service cloudstack-management restart
```

6.3. 新增新的計畫

CloudStack管理者及網域管理者可以建立計畫，如果廣域設定欄位allow.user.create.projects設定為true，則終端使用這也可以建立計畫

1. 以管理者登入CloudStack 使用者介面
2. 在左邊的導覽視窗，選擇Projects
3. 於Select View中選擇Projects
4. 點選New Project
5. 給計劃名稱及描述，然後按Create Project

6. 會出現視窗讓您能夠立即新增成員，此為選擇性，按 Next繼續

7. 按Save

6.4. Adding Members to a Project

New members can be added to a project by the project's administrator, the domain administrator of the domain where the project resides or any parent domain, or the CloudStack root administrator. There are two ways to add members in CloudStack, but only one way is enabled at a time:

- If invitations have been enabled, you can send invitations to new members.
- If invitations are not enabled, you can add members directly through the UI.

6.4.1. 送出計畫成員邀請

在邀請功能，在節 6.2.1, “建立邀請”描述，可用的前提下此步驟教如何新增成員到計畫中您，如果邀請功能不能用的話，請按照Adding Project Members From the UI來進行

1. 登入 CloudStack UI
2. 在左邊的導覽視窗，選擇Projects
3. 於Select View中選擇Projects
4. 選擇你想要套用的計畫
5. 選擇Invitations標籤
6. 在 Add，璇則其中一項:
   a. Account：邀請會出現在使用者Project View的邀請標籤，參照Using the Project View
   b. Email：邀請會寄到使用者的信箱，每個信箱包含特殊的編碼，當接受邀請後，點選連結會回到 CloudStack。此方法僅在 SMTP伺服器的廣域欄位有設定才能用，詳見 節 6.2.1, “建立邀請”
7. 輸入使用者名稱或Email，然後點選Invite。如果您選擇 Account，請輸入 CloudStack 使用者名稱。如果您選擇Email，請輸入地址。您只能邀請在同一網域的雲端使用者，但您可以寄Email給任意人
8. 您可以會到這個標籤來看和管理您寄出的邀請，當邀請接受了，新成員就會出現在計畫的 Accounts 標籤

6.4.2. 使用使用者介面增加計畫成員

此步驟教您，如果邀請功能不能用的話，如何新增成員到計畫中，如果邀請功能，在節 6.2.1, “建立邀請”中描述的，可以用的話，請依照節 6.4.1, “送出計畫成員邀請”的步驟執行

1. 登入 CloudStack 使用者介面
2. 在左邊的導覽視窗，選擇Projects
3. 於Select View中選擇Projects
4. 選擇你想要套用的計畫

5. 點選Accounts標籤，會列出現在計畫的成員

6. 輸入新成員的帳戶名，然後按Add Account，您可以只加入在同一網域的雲端使用者

6.5. 接受邀請

如果您收到加入CloudStack計畫的邀請，您想加入的話，請按照以下步驟:

1. 登入 CloudStack UI

2. 在左邊的導覽視窗，選擇Projects

3. 於Select View中選擇Invitations

4. 如果您看到邀請出現在畫面上方，請點選Accept

   邀請會使用您的 CloudStack帳戶送給您

5. 如果您收到Email邀請，點選Enter Token，並提供計劃ID及獨特的ID編碼（token）

6.6. 中止或刪除計畫

當計畫終止時，資源會保留，但無法再使用。終止的計畫無法再加入新的資源或成員

當計畫刪除時，資源會被摧毀，成員會被刪除，計畫的狀態會變成Disabled

計畫可以被計畫管理者、網域管理者、上層網域管理者或CloudStack root管理者中止或刪除

1. 登入 CloudStack UI

2. 在左邊的導覽視窗，選擇Projects

3. 於Select View中選擇Projects

4. 選擇你想要套用的計畫

5. 按下其中一個按鍵:

   刪除，使用 

   中止，使用 

6.7. 使用Project View

如果您是專案的一員，你可以使用 CloudStack 的project view，透過project view 您可以檢視專案成員、以消耗的專案資源以及其他專案相關資訊。Project view僅呈現單一專案，您可以先行過濾一些其他資訊，然而就可以專住在單一專案的狀態以及資源。

1. 登入 CloudStack UI

2. 點選Project View

3. 專案的主控台將呈現再您面前，其中包含了虛擬機、磁碟、專案成員、專案相關事件、網路設定以及其他專案相關資訊。於主控台您可以:

- 點選Accounts分頁檢視並管理專案成員，如果你是專案管理者，你可以新增專案成員、移除專案成員、或是更改專案角色，專案同時間只能有一個專案管理者，如果您設定了其他使用者為管理者，您本身的角色將更換成為一般使用者。

- （如果有開啓邀請功能）點選Invitations分頁您可以檢視並管理新邀請但仍未接受的專案成員，等待中的邀請會一直出現在列表中，直到該位使用者接受邀請、邀請時間過期或是您取消邀請。

Steps to Provisioning Your Cloud Infrastructure

This section tells how to add regions, zones, pods, clusters, hosts, storage, and networks to your cloud. If you are unfamiliar with these entities, please begin by looking through 章 2, 雲端基礎架構概念.

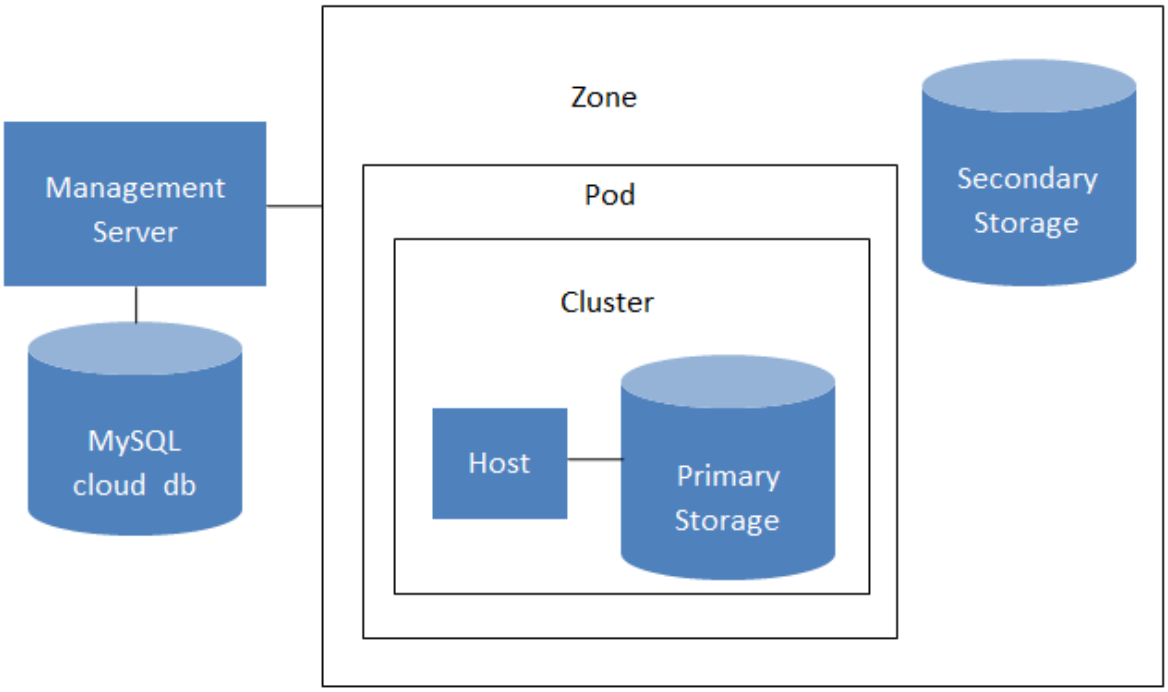
7.1. Overview of Provisioning Steps

After the Management Server is installed and running, you can add the compute resources for it to manage. For an overview of how a CloudStack cloud infrastructure is organized, see 節 1.3.2, “雲端基礎架構簡介”.

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

1. Define regions (optional). See 節 7.2, “Adding Regions (optional)”.
2. Add a zone to the region. See 節 7.3, “新增Zone”.
3. Add more pods to the zone (optional). See 節 7.4, “新增Pod”.
4. Add more clusters to the pod (optional). See 節 7.5, “新增一個Cluster”.
5. Add more hosts to the cluster (optional). See 節 7.6, “增加主機”.
6. Add primary storage to the cluster. See 節 7.7, “新增Primary Storage”.
7. Add secondary storage to the zone. See 節 7.8, “新增次要儲存裝置”.
8. Initialize and test the new cloud. See 節 7.9, “初始化及測試”.

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



Conceptual view of a basic deployment

7.2. Adding Regions (optional)

Grouping your cloud resources into geographic regions is an optional step when provisioning the cloud. For an overview of regions, see 節 2.1, “About Regions” .

7.2.1. The First Region: The Default Region

If you do not take action to define regions, then all the zones in your cloud will be automatically grouped into a single default region. This region is assigned the region ID of 1.

You can change the name or URL of the default region by using the API command updateRegion. For example:

```
http://<IP_of_Management_Server>:8080/client/api?command=updateRegion&id=1&name=Northern&endpoint=http://
<region_1_IP_address_here>:8080/client&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZOnUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP001hU%3D
```

7.2.2. Adding a Region

Use these steps to add a second region in addition to the default region.

1. Each region has its own CloudStack instance. Therefore, the first step of creating a new region is to install the Management Server software, on one or more nodes, in the geographic area where you want to set up the new region. Use the steps in the Installation guide. When you come to the step where you set up the database, use the additional command-line flag -r <region_id> to set a region ID for the new region. The default region is automatically assigned a region ID of 1, so your first additional region might be region 2.

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

2. By the end of the installation procedure, the Management Server should have been started. Be sure that the Management Server installation was successful and complete.

3. Add region 2 to region 1. Use the API command addRegion. (For information about how to make an API call, see the Developer's Guide.)

```
http://<IP_of_region_1_Management_Server>:8080/client/api?
command=addRegion&id=2&name=Western&endpoint=http://<region_2_IP_address_here>:8080/
client&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
JB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZOnUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP001hU%3D
```

4. Now perform the same command in reverse, adding region 1 to region 2.

```
http://<IP_of_region_2_Management_Server>:8080/client/api?
command=addRegion&id=1&name=Northern&endpoint=http://<region_1_IP_address_here>:8080/
client&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
JB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZOnUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP001hU%3D
```

5. Copy the account, user, and domain tables from the region 1 database to the region 2 database.

   In the following commands, it is assumed that you have set the root password on the database, which is a CloudStack recommended best practice. Substitute your own MySQL root password.

   a. First, run this command to copy the contents of the database:

   ```
   # mysqldump -u root -p<mysql_password> -h <region1_db_host> cloud account user domain > region1.sql
   ```

   b. Then run this command to put the data onto the region 2 database:

   ```
   # mysql -u root -p<mysql_password> -h <region2_db_host> cloud < region1.sql
   ```

6. Remove project accounts. Run these commands on the region 2 database:

```
mysql> delete from account where type = 5;
```

7. Set the default zone as null:

```
mysql> update account set default_zone_id = null;
```

8. Restart the Management Servers in region 2.

7.2.3. Adding Third and Subsequent Regions

To add the third region, and subsequent additional regions, the steps are similar to those for adding the second region. However, you must repeat certain steps additional times for each additional region:

1. Install CloudStack in each additional region. Set the region ID for each region during the database setup step.

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

2. Once the Management Server is running, add your new region to all existing regions by repeatedly calling the API command addRegion. For example, if you were adding region 3:

```
http://<IP_of_region_1_Management_Server>:8080/client/api?
command=addRegion&id=3&name=Eastern&endpoint=http://<region_3_IP_address_here>:8080/
client&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZOnUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP001hU%3D

http://<IP_of_region_2_Management_Server>:8080/client/api?
command=addRegion&id=3&name=Eastern&endpoint=http://<region_3_IP_address_here>:8080/
client&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZOnUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP001hU%3D
```

3. Repeat the procedure in reverse to add all existing regions to the new region. For example, for the third region, add the other two existing regions:

```
http://<IP_of_region_3_Management_Server>:8080/client/api?
command=addRegion&id=1&name=Northern&endpoint=http://<region_1_IP_address_here>:8080/
client&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZOnUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP001hU%3D

http://<IP_of_region_3_Management_Server>:8080/client/api?
command=addRegion&id=2&name=Western&endpoint=http://<region_2_IP_address_here>:8080/
client&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZOnUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP001hU%3D
```

4. Copy the account, user, and domain tables from any existing region's database to the new region's database.

   In the following commands, it is assumed that you have set the root password on the database, which is a CloudStack recommended best practice. Substitute your own MySQL root password.

   a. First, run this command to copy the contents of the database:

   ```
   # mysqldump -u root -p<mysql_password> -h <region1_db_host> cloud account user domain > region1.sql
   ```

   b. Then run this command to put the data onto the new region's database. For example, for region 3:

   ```
   # mysql -u root -p<mysql_password> -h <region3_db_host> cloud < region1.sql
   ```

5. Remove project accounts. Run these commands on the region 2 database:

```
mysql> delete from account where type = 5;
```

6. Set the default zone as null:

```
mysql> update account set default_zone_id = null;
```

7. Restart the Management Servers in the new region.

7.2.4. Deleting a Region

To delete a region, use the API command removeRegion. Repeat the call to remove the region from all other regions. For example, to remove the 3rd region in a three-region cloud:

```
http://<IP_of_region_1_Management_Server>:8080/client/api?
command=removeRegion&id=3&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZOnUkkJbPmY3y2bciKwFQ&signature=LxxlDM40AjcXU%2FcaiK8RAP001hU%3D

http://<IP_of_region_2_Management_Server>:8080/client/api?
command=removeRegion&id=3&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZOnUkkJbPmY3y2bciKwFQ&signature=LxxlDM40AjcXU%2FcaiK8RAP001hU%3D
```

7.3. 新增Zone

以下步驟假設您已經登入了 CloudStack UI。請參閱: 節 5.1, “登入使用者介面” 。

1. (非必要)如果您欲使用Swift作為您的secondary storage, 在新增zone之前, 您需要事先將Swift準備好。

   a. 以administrator身分登入CloudStack UI

   b. 如果這是您第一次造訪使用者介面, 系統將提供一個安裝精靈給您。請選擇"Experienced user", 接著您會看到主控台。

   c. 於左側的navigation按鈕中, 點選Global Settings。

   d. 在搜尋欄位裡鍵入swift.enable並點選搜尋按鈕。

   e. 點選編輯按鈕並將swift.enable設定為true 

   f. 重新啓動 Management Server

      ```
      # service cloudstack-management restart
      ```

   g. 重新整理 CloudStack UI 的瀏覽器分頁並重新登入。

2. 於左側的navigation按鈕中, 點選Infrastructure。

3. 於Zones的方框中點選View More

4. (非必要)如果您使用的是 Swift儲存裝置, 請將開啓Swift並輸入以下資訊:

   • URL. Swift的URL

   • Account. Swift帳號。

   • Username. Swift帳號的密碼。

   • Key. Swift的key

5. 點選新增Zone，將會出現Zone安裝精靈

6. 選擇您要建立的網路類型：

   - Basic．為類似AWS模式的網路架構，提供每一台虛擬機器實體網路IP位置，並可提供layer-3的Security group安全機制(IP位置過濾機制)。

   - Advanced．提供使用者更多的網路拓撲結構，選擇此選項將可更彈性的設定網路，且提供了更多的網路服務，例如：firewall、VPN、Load balancer。

   更多有關網路類型的資訊請參閱：節 2.8，“About Physical Networks”。

7. 以下步驟將視您選擇Basic網路或是Advance網路而定，請選擇您的設定並繼續以下步驟：

   - 節 7.3.1，“基礎區域設定”

   - 節 7.3.2，“進階Zone設定”

7.3.1. 基礎區域設定

1. 您在Add Zone精靈選擇Basic後，按Next，您會被詢問以下細節，然後按Next

   - Name.：zone名稱

   - DNS 1 and 2.：訪客VM使用的DNS伺服器，可由公開網路存取，您之後會新增。公開IP位址必須有路徑到此DNS伺服器

   - Internal DNS 1 and Internal DNS 2.：系統VM使用的DNS伺服器(CloudStack使用的VM，像是虛擬路由器、工作臺代理及次要儲存裝置VM)，這些DNS可經由管理流量網路介面存取，私人IP位址必須有路線到此內部DNS伺服器

   - Hypervisor.(3.0.1版後有)選擇第一個叢集超級監督者，您之後可以增加不同監督者的叢集

   - Network Offering.：您的選擇會決定哪種網路服務可以在訪客VM使用

Network Offerings	敘述
DefaultSharedNetworkOfferingWithSGService	如果您想啓用安全群組到訪客流量隔離，請選擇這個(詳見Using Security Groups to Control Traffic to VMs)
DefaultSharedNetworkOffering	如果您不需要安全群組，請選擇這個
DefaultSharedNetscalerEIPandELBNetworkOffering	如果您已安裝Citrix NetScaler，並且您會使用彈性IP和彈性負載平衡功能，請選擇這個。使用EIP 及ELB功能，啓用安全群組的基礎區域就可以提供1:1static NAT及負載平衡

   - Network Domain.：(選擇性)如果您想要特殊的網域名稱，請指定DNS suffix

   - Public.：所有使用者都能用的公開區，非公開區會指定為特定網域，只有此網域內的使用這才能建立訪客VM

2. 選擇流量刑事

   形式為管理、公開、訪客及儲存流量，更多資訊，滾動圖示來展示技巧，或是參閱Basic Zone Network Traffic Types，此畫面會有一些流量類型已經指定，如果您要加入更多，拉出流量類型到greyed-out的網路就會變成啓動。您也可以變更網路名稱

3. 3. (3.0.1版本後)指定網路流量標籤給每個實體網路上的每種流量形式，這些標籤必須符合您在超級監督者主機定義的標籤。在流量圖示點選Edit，會彈出對話框，您可以輸入標籤，然後按OK

   這些標籤只會在第一個叢集的超級監督者定義，對於其他所有超級監督者，標籤可以在區域建立後設定

4. 按Next

5. (僅NetScaler)，如果您為NetScaler選擇網路服務，您會有額外的視窗要填寫，提供需要的細節並建立NetScaler，然後按Next

   - IP address.: NetScaler裝置的NSIP (NetScaler IP) 位址
   - Username/Password.: 存取裝置的授權證明，CloudStack使用這些證明來存取裝置
   - Type. : NetScaler裝置類型，可能為NetScaler VPX，NetScaler MPX，或 NetScaler SDX，關於類型的比較，詳見About Using a NetScaler Load Balancer
   - Public interface.: NetScaler的介面，在公開網路設定
   - Private interface.: NetScaler的介面，在私人網路設定
   - Number of retries.: 嘗試指令的次數，不包含失敗，預設為2
   - Capacity.: 分享此裝置的訪客網路/帳戶的數量
   - Dedicated. : 標示為專用時，此裝置即為一個帳戶專用，而 Capacity欄位數值即為1

6. (僅NetScaler)為公開流量設定IP範圍，此範圍的IP會被使用為 static NAT容量，此容量為您使用 EIP 及 ELB選擇網路服務時啓用。輸入以下細節，然後按Add。您可以重複此步驟來增加IP範圍，結束後，請按Next

   - Gateway. : IP位址使用的閘道
   - Netmask: 和VPC閘道關聯的IP位址
   - VLAN.: 將被用在公用流量的VLAN
   - Start IP/End IP.: 一組預定可被網際網路存取的IP，並會被分配來存取訪客VM

7. 在新的區域中，CloudStack會先新增新的pod給您，您可以之後隨時增加。關於pod簡介，詳見節 2.3，“關於Pods”

   輸入以下來設定第一個pod，然後按Next

   - Pod Name.: pod名稱
   - Reserved system gateway. : pod中的主機閘道
   - Reserved system netmask.: 定義pod子網路的網路prefix ，使用CIDR表示方法
   - Start/End Reserved System IP. Management網路的IP範圍；被用來分配給system VMs: 如secondary storage vm、console proxy vm或是DHCP之用，關於IP範圍更多的資訊，請參閱系統保留IP章節

8. 為訪客流量設定網路，提供以下，然後按Next :

   - Guest gateway. : 客戶要用的閘道

- Guest Netmask: 客戶要使用的子網路遮罩
- Guest start IP/End IP.: 輸入開始及結束的IP位址，此定義CloudStack可以分配的給訪客的範圍
  - 强烈建議使用多網路卡，如果使用多網路卡，它們可能會在不同的子網域
  - 如果使用一張網路卡，這些 IP 應該為與 pod 的 CIDR 相同範圍

9. 在新的pod，CloudStack會先新增一個叢集給您，您可以之後自行增加，對於叢集的簡介，詳見About Clusters

   輸入以下來設定第一個叢集，然後按Next:

   - Hypervisor.(僅3.0.0版本; 3.0.1版本為唯讀)選擇一種超級監督者軟體給所有主機使用，如果您選擇VMware，會出現額外的欄位，您可以輸入vSphere 叢集的資訊，對於vSphere伺服器，建議您先在vCenter建立叢集主機，然後再將整的叢集加到CloudStack，詳見Add Cluster: vSphere
   - Cluster name.: 輸入叢集的名稱。這可以由您來選擇一個未被 CloudStack 使用的文字。

10. 在新的叢集中，CloudStack會先新增新的主機給您，您可以之後隨時增加。關於主機簡介，詳見About Hosts

    注意

    當您增加超級監督者主機給CloudStack時，所有主機的VM都不能是執行狀態

    在您設定主機前，您必須安裝超級監督者軟體，您需要知道何種版本支援CloudStack ，及需要那些額外設定，對於這些安裝細節，詳見:

    - Citrix XenServer安裝及設定
    - VMware vSphere安裝與設定
    - KVM vSphere安裝及設定

    輸入以下來設定第一個主機，然後按Next

    - Host Name.: 主機的DNS名稱或IP位址
    - Username.: 通常為root
    - Password.: 給以上使用者的密碼(從您的 XenServer 或 KVM安裝)
    - Host Tags(選擇性): 任何您用來分類主機的標籤，例如，如果您想要主機僅使用有"high availability"功能的VM，您可以設定雲端HA標籤(ha.tag廣域設定欄位設定)，更多資訊，詳見HA-Enabled Virtual Machines及HA for Hosts

11. 在新的叢集中，CloudStack會先新增一個主要儲存裝置給您，您可以之後自行增加，對於主要儲存裝置的簡介，詳見About Primary Storage

    輸入以下來設定第一個主要儲存裝置，然後按Next:

    - Name.儲存裝置的名稱

- Protocol. Protocol. 以XenServer來說，您可以選擇NFS、iSCSI、或是 PreSetup. 以KVM來說，您可以選擇NFS、SharedMountPoint，CLVM，及RBD。vSphere您可以選擇VMFS（iSCSI或FiberChannel)或NFS。其他剩下的欄位取決於您的選擇

7.3.2. 進階Zone設定

1. 您在Add Zone精靈選擇Advanced後，按Next，您會被詢問以下細節，然後按Next

   - Name.: zone名稱
   - DNS 1 and 2.: 訪客VM使用的DNS伺服器，可由公開網路存取，您之後會新增。公開IP位址必須有路徑到此DNS伺服器
   - Internal DNS 1 and Internal DNS 2.: 系統VM使用的DNS伺服器(CloudStack使用的VM，像是虛擬路由器、工作臺代理及次要儲存裝置VM)，這些DNS可經由管理流量網路介面存取，私人IP位址必須有路線到此內部DNS伺服器
   - Network Domain. : (選擇性)如果您想要特殊的網域名稱，請指定DNS suffix
   - Guest CIDR.: 在訪客虛擬網路描述IP位址的CIDR，例如10.1.1.0/24，您需要在不同的zone設定不同的CIDR，會使您設定VPN時比較容易
   - Hypervisor.(3.0.1版後有)選擇第一個叢集超級監督者，您之後可以增加不同監督者的叢集
   - Public.: 所有使用者都能用的公開區，非公開區會指定為特定網域，只有此網域內的使用這才能建立訪客VM

2. 選擇流量刑事

   形式為管理、公開、訪客及儲存流量，更多資訊，滾動圖示來展示技巧，或是參閱節 2.8.3, “Advanced Zone Network Traffic Types”，此畫面會有一個網路已經設定，如果您有多實體網路，您需要加入更多，拉出流量類型到greyed-out的網路就會變成啓動。您可以移動流量圖示到另一個網路，例如，預設流量出現在網路1，但不符您的需要，您可以將它們移出網路，您也可以變更網路名稱

3. (3.0.1版本後)指定網路流量標籤給每個實體網路上的每種流量形式，這些標籤必須符合您在超級監督者主機定義的標籤。在流量圖示點選Edit，會彈出對話框，您可以輸入標籤，然後按OK

   這些標籤只會在第一個叢集的超級監督者定義，對於其他所有超級監督者，標籤可以在區域建立後設定

4. 按Next

5. 為公開網路設定IP範圍，輸入以下細節，然後按Add。您可以重複此步驟來增加多個範圍，結束後，請按Next

   - Gateway. : IP位址使用的閘道
   - Netmask: 和VPC閘道關聯的IP位址
   - VLAN.: 將被用在公用流量的VLAN
   - Start IP/End IP.: 一組預定可被網際網路存取的IP，並會被分配來存取來賓網路

6. 在新的區域中，CloudStack會先新增新的pod給您，您可以之後隨時增加。關於pod簡介，詳見節 2.3, “關於Pods”

輸入以下來設定第一個pod，然後按Next

- Pod Name.: pod名稱
- Reserved system gateway. : pod中的主機閘道
- Reserved system netmask.: 定義pod子網路的網路prefix ， 使用CIDR表示方法
- Start/End Reserved System IP. : Management網路的IP範圍；被用來分配給system VMs：如secondary storage vm、console proxy vm或是DHCP之用，關於IP範圍更多的資訊，請參閱 節 2.8.6，“系統保留IP位址”.

7. 在每個實體網路指定一個VLAN ID範圍來搭載訪客流量(詳見VLAN Allocation Example)，然後按Next

8. 在新的pod，CloudStack會先新增一個叢集給您，您可以之後自行增加，對於叢集的簡介，詳見 節 2.4，“關於Clusters”

   輸入以下來設定第一個叢集，然後按Next:

   - Hypervisor.(僅3.0.0版本；3.0.1版本為唯讀)選擇一種超級監督者軟體給所有主機使用，如果您選擇VMware，會出現額外的欄位，您可以輸入vSphere 叢集的資訊，對於vSphere伺服器，建議您先在vCenter建立叢集主機，然後再將整的叢集加到CloudStack，詳見Add Cluster: vSphere
   - Cluster name.: 輸入叢集的名稱。這可以由您來選擇一個未被 CloudStack 使用的文字。

9. 在新的叢集中，CloudStack會先新增新的主機給您，您可以之後隨時增加。關於主機簡介，詳見 節 2.5，“About Hosts”

   注意

   當您配置CloudStack時，所有超級管理者主機的VM都不能是執行狀態

   在您設定主機前，您必須安裝超級監督者軟體，您需要知道何種版本支援CloudStack ，及需要那些額外設定，對於這些安裝細節，詳見:

   - CloudStack的Citrix XenServer安裝
   - VMware vSphere安裝與設定
   - KVM安裝與設定

   輸入以下來設定第一個主機，然後按Next

   - Host Name.: 主機的DNS名稱或IP位址
   - Username.: 通常為root
   - Password.: 給以上使用者的密碼(從您的 XenServer 或 KVM安裝)
   - Host Tags(選擇性): 任何您用來分類主機的標籤，例如，如果您想要主機僅使用有"high availability"功能的VM，您可以設定雲端HA標籤(ha.tag廣域設定欄位設定)，更多資訊，詳見HA-Enabled Virtual Machines及HA for Hosts，都在Administration Guide中

10. 在新的叢集中，CloudStack會先新增一個主要儲存裝置給您，您可以之後自行增加，對於主要儲存裝置的簡介，詳見節 2.6, “About Primary Storage”

    輸入以下來設定第一個主要儲存裝置，然後按Next:

    - Name.儲存裝置的名稱
    - Protocol. Protocol. 以XenServer來說，您可以選擇NFS、iSCSI、或是 PreSetup. 以KVM來說，您可以選擇NFS、SharedMountPoint，CLVM，及RBD。vSphere您可以選擇VMFS（iSCSI或FiberChannel)或NFS。其他剩下的欄位取決於您的選擇

NFS	• Server.: 儲存裝置的IP位址或DNS名稱 • Path.: 從伺服器匯出的路徑 • Tags (optional). 儲存裝置的標籤逗號分隔表，這在您的硬碟服務，必須是同等或更高的設定 橫跨Zone中的cluster，設在主要儲存裝置的標籤，必須一模一樣。例如，如果cluster A提供主要儲存裝置，他有標籤T1和T2，其他Zone內的cluster也必須提供相同標籤T1和T2的主要儲存裝置
iSCSI	• Server.: 儲存裝置的IP位址或DNS名稱 • Target IQN. : 目標的IQN。例如，iqn.1986-03.com.sun:02:01ec9bb549-1271378984 • Lun. : LUN數字，例如 , 3 • Tags (optional). 儲存裝置的標籤逗號分隔表，這在您的硬碟服務，必須是同等或更高的設定 橫跨Zone中的cluster，設在主要儲存裝置的標籤，必須一模一樣。例如，如果cluster A提供主要儲存裝置，他有標籤T1和T2，其他Zone內的cluster也必須提供相同標籤T1和T2的主要儲存裝置
preSetup	• Server.: 儲存裝置的IP位址或DNS名稱 • SR Name-Label. : 輸入已經在 CloudStack外設定好的SR名稱標籤 • Tags (optional). 儲存裝置的標籤逗號分隔表，這在您的硬碟服務，必須是同等或更高的設定 橫跨Zone中的cluster，設在主要儲存裝置的標籤，必須一模一樣。例如，如果cluster A提供主要儲存裝置，他有標籤T1和T2，其他Zone內的cluster也必須提供相同標籤T1和T2的主要儲存裝置
SharedMountPoint	• Path.: 每台主機掛載主要儲存裝置的路徑，例如"/mnt/primary"

	• Tags (optional). 儲存裝置的標籤逗號分隔表，這在您的硬碟服務，必須是同等或更高的設定 橫跨Zone中的cluster，設在主要儲存裝置的標籤，必須一模一樣。例如，如果cluster A提供主要儲存裝置，他有標籤T1和T2，其他Zone內的cluster也必須提供相同標籤T1和T2的主要儲存裝置
VMFS	• Server. : vCenter server的IP位址或DNS名稱 • Path.: 資料庫的名稱和名稱的組合。格式為"/" datacenter name "/" datastore name。例如，"/cloud.dc.VM/clusterldatastore" • Tags (optional). 儲存裝置的標籤逗號分隔表，這在您的硬碟服務，必須是同等或更高的設定 橫跨Zone中的cluster，設在主要儲存裝置的標籤，必須一模一樣。例如，如果cluster A提供主要儲存裝置，他有標籤T1和T2，其他Zone內的cluster也必須提供相同標籤T1和T2的主要儲存裝置

11. 在新的區域中，CloudStack會先新增新的次要儲存裝置給您，您可以之後隨時增加。關於次要儲存裝置簡介，詳見 節 2.7, “About Secondary Storage”

    在您填入此視窗前，您需要建立NFS shares機安裝最新的CloudStack System VM 模組來準備次要儲存裝置，詳見 Adding Secondary Storage :

    • NFS Server. The IP address of the server or fully qualified domain name of the server.

    • Path.: 從伺服器匯出的路徑

12. 點選Launch.

7.4. 新增Pod

當您建立了一個新的zone，CloudStack同時也為您新增了一個pod，您也可於之後自行新增。

1. 登入 CloudStack UI. 請參閱: 節 5.1, “登入使用者介面” .
2. 於左側的navigation按鈕中，選擇Infrastructure。於右側Zones的方框下點選View More，接著請選擇您欲新增pod的zone。
3. 點選Compute and Storage分頁，在pod節點的圖中點選View All
4. 點選Add pod
5. 於對話視窗中輸入以下資訊。

    • Name. 此pod之名稱。

- Gateway. Host於此pod的網路閘道。
- Netmask. 用於設定pod的子網路, 使用CIDR表示方法。
- Start/End Reserved System IP. Management網路的IP範圍; 被用來分配給system VMs: 如secondary storage vm、console proxy vm或是DHCP之用, 關於IP範圍更多的資訊, 請參閱系統保留IP章節

6. 點選OK

7.5. 新增一個Cluster

你需要告知CloudStack主機, 由於主機在cluster內, 所以在新增主機之前, 你必須要至少有一個cluster

7.5.1. 新增Cluster: KVM 或 XenServer

此步驟是假設您已經安裝超級監督者及已登入CloudStack使用者介面

1. 於左邊的navigation列表中點選Infrastructure, 接者點選zone並選擇View More, 最後點選新增cluster。
2. 點選Compute分頁
3. 在圖中的Clusters node, 點選 View All
4. 點選新增Cluster
5. 選擇超級監督者類型
6. 選擇要新增cluster的pod
7. 輸入叢集的名稱。這可以由您來選擇一個未被 CloudStack 使用的文字。
8. 按OK

7.5.2. 加入叢集: vSphere

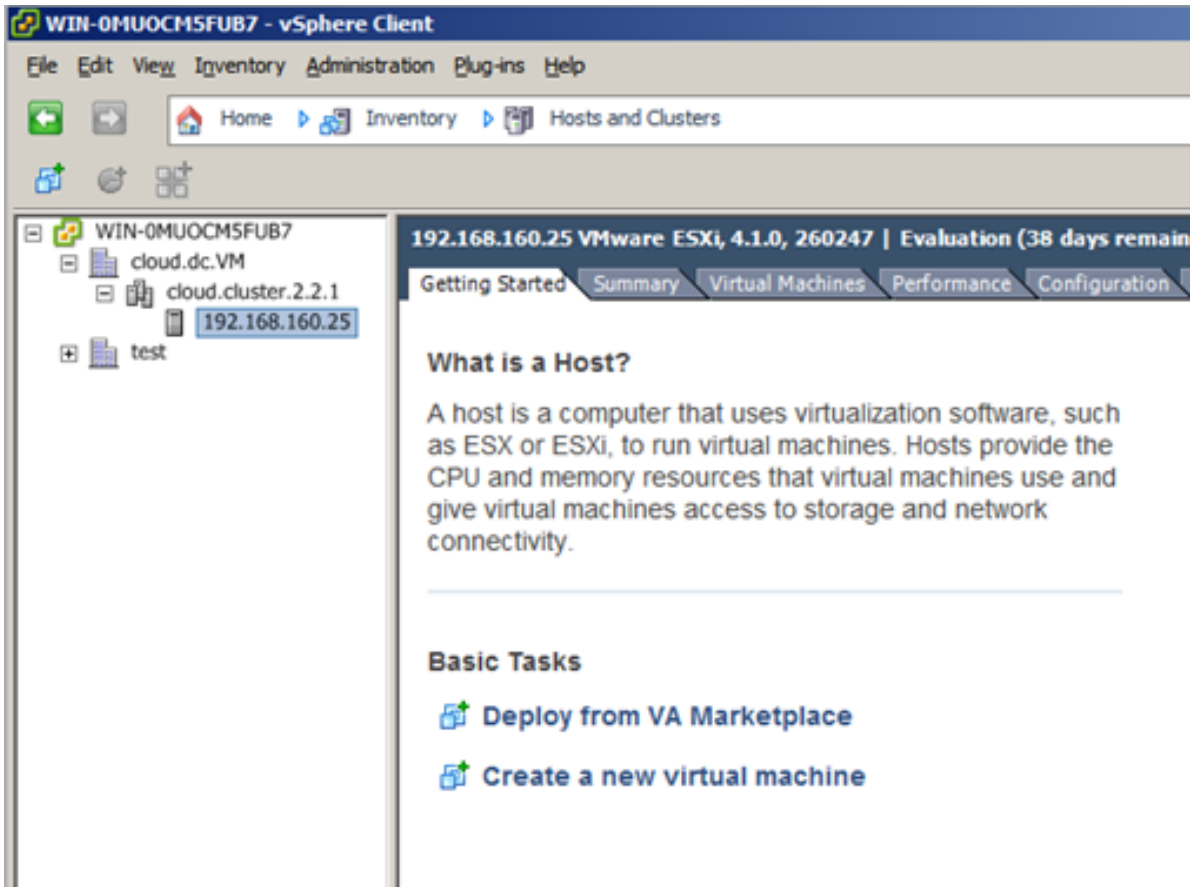
藉由結合vCenter及CloudStack管理介面, 可以完成vSphere主機管理, CloudStack需要所有主機都必須在 CloudStack叢集中, 但是叢集有可能只包含一個主機。身為管理者, 您必須決定叢集是使用一個還多個主機, 多主機叢集可以操作live migration等功能, 叢集要求像 NFS or iSCSI的分享儲存

對於 vSphere伺服器, 建議建立主機在vCenter的叢集, 並建立整個叢集到CloudStack, 依照以下要求:

- vSphere叢集不要超過8台主機
- 確定CloudStack加入前, 超級監督者主機還沒有任何VM執行

加入vSphere叢集到CloudStack:

1. 根據指南來建立主機在vCenter的叢集



2. 登入使用者介面

3. 於左邊的navigation列表中點選Infrastructure，接者點選zone並選擇View More，最後點選新增cluster。

4. 點選 Compute標籤，在 Pods選擇View All，選擇您要加入叢集的pod

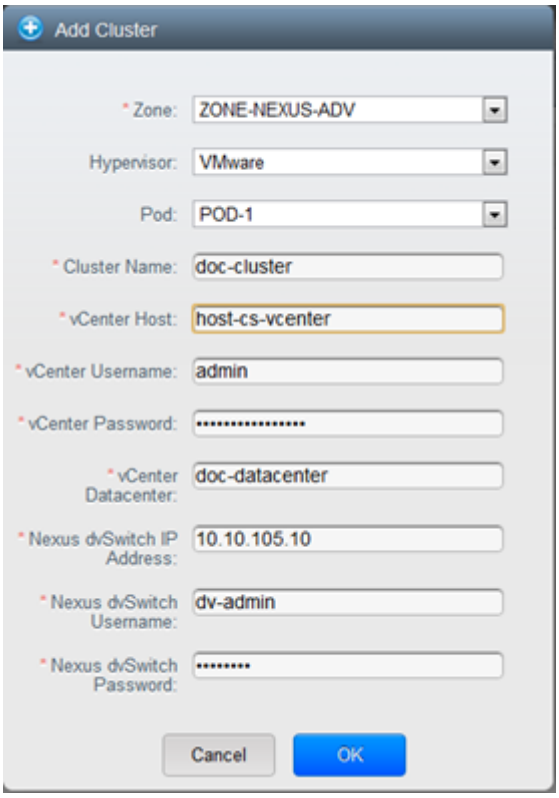
5. 按 View Clusters

6. 點選新增Cluster

7. 在Hypervisor，選擇VMware

8. 在對話框提供以下資訊，以下欄位會從 vCenter對應數值

   - Cluster Name：輸入叢集名稱，例如"cloud.cluster.2.2.1"
   - vCenter Host： vCenter伺服器的主機名稱或IP位址
   - vCenter Username：CloudStack連結vCenter的使用者名稱，此使用者必須為管理優先
   - vCenter Password：輸入使用者密碼
   - vCenter Datacenter：輸入叢集位於的 vCenter資料庫，例如"cloud.dc.VM"

- 

  等待一段時間，它就會自動顯示在使用這介面了

7.6. 增加主機

1. 在將主機加入 CloudStack組態前，您必須先安裝超級監督者，如此CloudStack才能管理運行虛擬機器的主機

   CloudStack安裝指南提供指示，請參閱Installation Guide的一些章節來取得一些資訊，如支援的版本，額外的步驟

   警告

   請確定您執行額外的 CloudStack限定設定步驟，描述在超級監督者安裝章節

2. 現在，請加入超級監督者主機到CloudStack，使用的技術取決於您的超級監督者

   - 節 7.6.1, “(XenServer 或 KVM)增加主機”
   - 節 7.6.2, “Adding a Host (vSphere)”

7.6.1. (XenServer 或 KVM)增加主機

XenServer 及 KVM主機可以隨時加到叢集

7.6.1.1. XenServer 及 KVM主機需求

警告

確定CloudStack加入前，超級監督者主機還沒有任何VM執行

設定需求:

- 每個叢集必須有相同的超級監督者主機
- 對於 XenServer，請勿放置超過8台主機
- 對於KVM，請不要超過16台主機

硬體需求，詳見CloudStack Installation Guide的安裝部分

7.6.1.1.1. XenServer主機額外需求

如果網路鍵結正在使用，管理者必須將新主機接成跟其他主機一樣的接線

對於所有額外的主機，執行以下指令。此步驟會將主機加入XenServer群的主要主機

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

注意

當複製及貼上指令時，請確定指令是貼成單一條線，因為有些文件瀏覽器會多出不必要的中斷

當所有主機都加入XenServer後，執行 cloud-setup-bond程式，此程式會完成設定並建立所有主機的鍵結

1. 從管理伺服器/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver/cloud-setup-bonding.sh複製程式到主要主機，並確定是可執行
2. 執行程式碼:

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

7.6.1.1.2. KVM主機額外需求

- 如果 shared mountpoint儲存正在使用，管理者必須確定新主機有與其他主機相同的mountpoints (搭載儲存裝置)
- 確定新主機跟其他主機有相同的網路設定(訪客、私人及公開網路)
- 如果您在使用 OpenVswitch橋接器編輯agent.properties檔案，並在加入主機到CloudStack前設定欄位network.bridge.type為openvswitch

7.6.1.2. 增加XenServer 或 KVM主機

- 請先安裝超級監督者軟體到主機上，如果您想知道哪個版本支援CloudStack，及額外設定，請參閱CloudStack Installation Guide的部分章節
- 以administrator身分登入CloudStack UI
- 於左邊的navigation列表中點選Infrastructure，接者點選zone並選擇View More，最後點選想要新增主機的zone。
- 點選Compute標籤，在Clusters節點點選View All
- 點選要新增主機的叢集
- 按 View Hosts
- 按 Add Host
- 提供以下資訊:
  - Host Name: DNS名稱或IP位址
  - Username: 通常為root
  - Password: 這是使用者在上面命名的密碼，來自您的 XenServer 安裝)。
  - Host Tags(選擇性): 任何您用來分類主機的標籤，例如，如果您想要主機僅使用有"high availability"功能的VM，您可以設定雲端HA標籤(ha.tag廣域設定欄位設定)，更多資訊，詳見HA-Enabled Virtual Machines及HA for Hosts

  等待一段時間，它就會自動顯示在使用這介面了
- 如有其他主機，重複以上步驟

7.6.2. Adding a Host (vSphere)

For vSphere servers, we recommend creating the cluster of hosts in vCenter and then adding the entire cluster to CloudStack. See Add Cluster: vSphere.

7.7. 新增Primary Storage

7.7.1. 系統需求

硬體需求:

- 任一被underlying hypervisor支援的同一標準iSCI 或NFS server
- 儲存伺服器必須是有大量硬碟的機器，硬碟須由硬碟RAID控制器來管理
- 最小容量取決於您的需求

當設定主要儲存裝置時，請依照以下限制:

- 在主機被加到cluster之前，請不要新增主要儲存裝置
- 如果您還未提供分享主要儲存裝置，您必需先設定廣義設定參數system.vm.local.storage.required為true，否則您就不能啓動VM

7.7.2. 新增主要儲存裝置

當您新增了一個zone，過程中您間加入第一個primary storage，您可以隨時新增primary storage伺服器進入您的CloudStack，例如：當您新增了一個cluster或是當新增了許多的伺服器進入一個已存在的cluster。

警告

請確保伺服器端是沒有任何資料的，新增一個伺服器至 CloudStack 將會刪除所有存在的資料。

1. 登入 CloudStack UI.（請參閱: 節 5.1, “登入使用者介面”.）
2. 於左邊的navigation列表中點選Infrastructure，接者點選zone並選擇View More，最後點選新增primary storage。
3. 點選Compute分頁
4. 於圖示中的Primary storage節點中點選View All
5. 點選Add Primary Storage
6. 於對話視窗中，輸入以下資訊，所有的資訊都跟您的protocol有關。
   - Pod. 儲存裝置的曹
   - Cluster. 儲存裝置的cluster
   - Name.儲存裝置的名稱
   - Protocol. Protocol. 以XenServer來說，您可以選擇NFS、iSCSI、或是 PreSetup. 以KVM來說，您可以選擇NFS or SharedMountPoint。vSphere您可以選擇VMFS（iSCSI或 FiberChannel)或NFS
   - Server (for NFS, iSCSI, or PreSetup).儲存裝置的IP位址或DNS名稱
   - Server (for VMFS). vCenter server的IP位址或DNS名稱
   - Path (for NFS). 在NFS中的伺服器輸出管道
   - Path (for VMFS). 在vSphere中，是資料庫的名稱和名稱的組合。格式為"/" datacenter name "/" datastore name。例如，"/cloud.dc.VM/clusterldatastore"
   - Path (for SharedMountPoint). 路徑指向每一個host所掛載的primary storage 路徑，例如："/mnt/primary
   - SR Name-Label (for PreSetup). 輸入SR已經在 CloudStack外設定好的
   - Target IQN (for iSCSI). 在iSCSI，這是目標的IQN。例如，iqn.1986-03.com.sun:02:01ec9bb549-1271378984
   - Lun # (for iSCSI). 在iSCSI，這是LUN數字，例如，3
   - Tags (optional). 儲存裝置的標籤逗號分隔表，這在您的硬碟服務，必須是同等或更高的設定

   橫跨Zone中的cluster，設在主要儲存裝置的標籤，必須一模一樣。例如，如果cluster A提供主要儲存裝置，他有標籤T1和T2，其他Zone內的cluster也必須提供相同標籤T1和T2的主要儲存裝置

7. 按OK

7.8. 新增次要儲存裝置

7.8.1. 次要儲存裝置系統需求

・NFS儲存裝置工具或Linux NFS server

・(選擇性)OpenStack Object Storage (Swift)(詳見http://swift.openstack.org)

・100GB最小容量

・次要儲存裝置必須和訪客VM在同一個區域內

・每個次要儲存伺服器必須對所有區域內的主機都可用

7.8.2. 新增次要儲存裝置

當您新增了一個區域，過程中會加入第一個主要儲存裝置，您可以隨時新增次要儲存伺服器到已有的區域

警告

請確保伺服器端是沒有任何資料的，新增一個伺服器至 CloudStack 將會刪除所有存在的資料。

1. 如果您欲使用Swift作為您的次要儲存裝置，您必須在加入本地區域次要儲存伺服器前，先將Swift儲存裝置加入 CloudStack ，詳見節 7.3，“新增Zone”
2. 您需要在安裝管理伺服器時，建立及掛載NFS share來準備建立區域次要儲存伺服器，See Preparing NFS Shares in the Installation Guide.
3. 確定您已在管理伺服器安裝時，準備了系統VM模組See Prepare the System VM Template in the Installation Guide.
4. 每個區域儲存裝置的次要儲存伺服器已經準備好了，將他加入CloudStack，次要儲存裝置現在是新增區域的一個部份了，詳見節 7.3，“新增Zone”

7.9. 初始化及測試

當所有東西都設定好了，CloudStack會開始初始化，可能會花30分鐘以上的時間執行，這取決於您的網路速度。當初始化成功完成， CloudStack UI中會出現administrator's Dashboard

1. 確認系統已經準備好。在左邊的導覽視窗，選擇 Templates，選擇CentOS 5.5 (64bit) no Gui (KVM) template。確認狀態為"Download Complete."，注意，狀態還沒顯示前，不要執行下一步
2. 到 Instances標籤，使用My Instances過濾
3. 選擇Add Instance並跟著精靈的步驟
   a. 選擇您想要加入的zone
   b. 在template selection選擇要在VM中使用的 template，如果是基本安裝，應該只會有CentOS template

c. 選擇一個service offering，請確定您允許的硬體開始執行選擇的service offering

d. 在資料硬碟服務中，增加另一個資料硬碟。這個第二個容量可以被訪客使用，但不是掛載的。例如， XenServer的Linux，重新開機後，您會在訪客看到 /dev/xvdb。如果您有PV-enabled OS kernel，那麼您就不需要重新開機

e. 預設上，訪客是使用主要儲存裝置；在試用版，您只會有一個選項

f. 您可以選擇性的給您的VM名字及群組。

g. 點選Launch VM，您的VM將會新增並啓動，會花點時間下載模組。您可以看 Instances畫面來監控進度

4. 點選 View Console來使用VM。 

更多使用VM的資訊，包含允許輸入流量、啓動、停止、刪除及移動VM，詳見Administrator's Guide中的Working With Virtual Machines

恭喜！您完成CloudStack安裝

如果您想要增加部署量，您可以新增更多主機、主要儲存裝置、zone、pod及cluster

服務提供

這個章節，我們會來討論計算、硬碟及系統服務。網路服務提供會在幫使用者設定網路的章節提到

8.1. Compute and Disk Service Offerings

A service offering is a set of virtual hardware features such as CPU core count and speed, memory, and disk size. The CloudStack administrator can set up various offerings, and then end users choose from the available offerings when they create a new VM. 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

For example, one service offering might allow users to create a virtual machine instance that is equivalent to a 1 GHz Intel® Core™ 2 CPU, with 1 GB memory at $0.20/hour, with network traffic metered at $0.10/GB. Based on the user's selected offering, CloudStack emits usage records that can be integrated with billing systems. CloudStack separates service offerings into compute offerings and disk 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 (optional). An offering without a disk size will allow users to pick their own
- Tags on the data disk

8.1.1. 建立新的計算服務

想要新增計算服務:

1. 以管理者優先登入CloudStack使用者介面
2. 在左邊的導覽視窗，選擇Service Offerings
3. 在Select Offering中，選擇 Compute Offering
4. 按下Add Compute Offering
5. 在對話框中，選擇以下:
    - Name: 服務的名稱
    - Description: 使用者可見的簡述

- Storage type: 硬碟分配的形式。本地分配會直接連結到系統VM正在執行的主機; 分享分配則經由NFS存取
- # of CPU cores: 應分配的核心數
- CPU (in MHz): CPU的核心時脈, 例如 "2000" 為2GHz
- Memory (in MB): 記憶體的數量, 例如"2048"為2GB的記憶體分配
- Network Rate: 允許的資料傳輸速率, 單位為MB每秒
- Offer HA: 如果為是, 則管理者可以選擇監視系統VM
- Storage Tags: 連結到主要儲存裝置的tags
- Host Tags: (選擇性)您組織主機的tag
- CPU cap: 是否限制CPU使用率
- Public: 決定服務使否為所有網域使用, 選擇Yes使所有網域都可使用; 選擇No, CloudStack會出現提示要您輸入子網域的名稱。

6. 按Add

8.1.2. 新增硬碟服務

想要新增系統服務:

1. 以管理者優先登入CloudStack使用者介面
2. 在左邊的導覽視窗, 選擇Service Offerings
3. 在Select Offering中, 選擇Disk Offering
4. 按下Add Disk Offering
5. 在對話框中, 選擇以下:
   - Name: 系統服務的名稱
   - Description: 使用者可見的簡述
   - Custom Disk Size: 如果啓用, 使用者可以自訂硬碟大小; 不啓用, 則只有root管理者能定義
   - Disk Size: 只有Custom Disk Size不啓用時才會顯示, 定義容量大小, 單位為GB
   - (選擇性)Storage Tags: tag應該會連結到硬碟的主要儲存區, 而tag是comma separated list屬性的儲存, 例如 "ssd,blue"。tag也會被主要儲存裝置加入, CloudStack會比對硬碟及儲存裝置的tag。如果硬碟有tag(tags), 則主要儲存裝置就會有相同的tag, 如果沒有, 容量分配就會失敗
   - Public: 決定服務使否為所有網域使用, 選擇Yes使所有網域都可使用; 選擇No, CloudStack會出現提示要您輸入子網域的名稱。
6. 按Add

8.1.3. Modifying or Deleting a Service Offering

Service offerings cannot be changed once created. This applies to both compute offerings and disk offerings.

A service offering can be deleted. If it is no longer in use, it is deleted immediately and permanently. If the service offering is still in use, 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.

8.2. 系統服務

系統服務提供CPU速度、CPU數量、標籤及記憶體大小等選擇，如其他服務。但是除了給虛擬機器及使用者使用，此服務可以改變虛擬路由器、控制台代理及其他系統VM的預設性質。系統服務僅能被 CloudStack root 管理者使用，而CloudStack會提供預設的系統服務。CloudStack root管理者可以建立自訂的系統服務

當 CloudStack 建立虛擬路由器時，會使用預設設定。您可以藉由使用新的網路服務來更新虛擬路由器的能力，新的網路服務包含不同的系統服務。所有虛擬路由器會開始使用新的服務設定

8.2.1. 建立新的系統服務

想要新增系統服務:

1. 以管理者優先登入CloudStack使用者介面
2. 在左邊的導覽視窗，選擇Service Offerings
3. 在Select Offering中，選擇 System Offering
4. 按下Add System Service Offering
5. 在對話框中，選擇以下:
    - Name: 系統服務的名稱
    - Description: 使用者可見的簡述
    - System VM Type: 選擇此服務支援的系統虛擬機器的形式
    - Storage type: 硬碟分配的形式。本地分配會直接連結到系統VM正在執行的主機；分享分配則經由NFS存取
    - # of CPU cores: 應分配的核心數
    - CPU (in MHz): CPU的核心時脈，例如 "2000" 為2GHz
    - Memory (in MB): 記憶體的數量，例如"2048"為2GB的記憶體分配
    - Network Rate: 允許的資料傳輸速率，單位為MB每秒
    - Offer HA: 如果為是，則管理者可以選擇監視系統VM
    - Storage Tags: 連結到主要儲存裝置的tags
    - Host Tags: (選擇性)您組織主機的tag
    - CPU cap: 是否限制CPU使用率

- Public：決定服務使否為所有網域使用，選擇Yes使所有網域都可使用；選擇No，CloudStack會出現提示要您輸入子網域的名稱。

6. 按Add

8.3. Network Throttling

Network throttling is the process of controlling the network access and bandwidth usage based on certain rules. CloudStack controls this behaviour of the guest networks in the cloud by using the network rate parameter. This parameter is defined as the default data transfer rate in Mbps (Megabits Per Second) allowed in a guest network. It defines the upper limits for network utilization. If the current utilization is below the allowed upper limits, access is granted, else revoked.

You can throttle the network bandwidth either to control the usage above a certain limit for some accounts, or to control network congestion in a large cloud environment. The network rate for your cloud can be configured on the following:

- Network Offerings
- Service Offering
- Global parameter

If network rate is set to NULL in service offering, the value provided in the vm.network.throttling.rate global parameter is applied. If the value is set to NULL for network offering, the value provided in the network.throttling.rate global parameter is considered.

For the default public, storage, and management networks, network rate is set to 0. This implies that the public, storage, and management networks will have unlimited bandwidth by default. For default guest networks, network rate is set to NULL. In this case, network rate is defaulted to the global parameter value.

The following table gives you an overview of how network rate is applied on different types of networks in CloudStack.

Networks	Network Rate Is Taken from
Guest network of Virtual Router	Guest Network Offering
Public network of Virtual Router	Guest Network Offering
Storage network of Secondary Storage VM	System Network Offering
Management network of Secondary Storage VM	System Network Offering
Storage network of Console Proxy VM	System Network Offering
Management network of Console Proxy VM	System Network Offering
Storage network of Virtual Router	System Network Offering
Management network of Virtual Router	System Network Offering
Public network of Secondary Storage VM	System Network Offering
Public network of Console Proxy VM	System Network Offering
Default network of a guest VM	Compute Offering
Additional networks of a guest VM	Corresponding Network Offerings

A guest VM must have a default network, and can also have many additional networks. Depending on various parameters, such as the host and virtual switch used, you can observe a difference in the network rate in your cloud. For example, on a VMware host the actual network rate varies based on where they are configured (compute offering, network offering, or both); the network type (shared or isolated); and traffic direction (ingress or egress).

The network rate set for a network offering used by a particular network in CloudStack is used for the traffic shaping policy of a port group, for example: port group A, for that network: a particular subnet or VLAN on the actual network. The virtual routers for that network connects to the port group A, and by default instances in that network connects to this port group. However, if an instance is deployed with a compute offering with the network rate set, and if this rate is used for the traffic shaping policy of another port group for the network, for example port group B, then instances using this compute offering are connected to the port group B, instead of connecting to port group A.

The traffic shaping policy on standard port groups in VMware only applies to the egress traffic, and the net effect depends on the type of network used in CloudStack. In shared networks, ingress traffic is unlimited for CloudStack, and egress traffic is limited to the rate that applies to the port group used by the instance if any. If the compute offering has a network rate configured, this rate applies to the egress traffic, otherwise the network rate set for the network offering applies. For isolated networks, the network rate set for the network offering, if any, effectively applies to the ingress traffic. This is mainly because the network rate set for the network offering applies to the egress traffic from the virtual router to the instance. The egress traffic is limited by the rate that applies to the port group used by the instance if any, similar to shared networks.

例如:

Network rate of network offering = 10 Mbps

Network rate of compute offering = 200 Mbps

In shared networks, ingress traffic will not be limited for CloudStack, while egress traffic will be limited to 200 Mbps. In an isolated network, ingress traffic will be limited to 10 Mbps and egress to 200 Mbps.

8.4. 改變系統VM的預設系統服務

您可以手動改變系統服務，除此之外，身為CloudStack 管理者，您可以改變預設的系統服務

1. 建立新的系統服務:

   更多資訊，詳見 Creating a New System Service Offering

2. 備份資料庫

   ```
   mysqldump -u root -p cloud | bzip2 > cloud_backup.sql.bz2
   ```

3. 開啓MySQL提示:

   ```
   mysql -u cloud -p cloud
   ```

4. 在雲端資料庫執行以下疑問

   a. 在 disk_offering表，確認原始預設的服務，及您想要做為新的預設的服務

記下新服務的ID

```
從disk_offering選擇 id,name,unique_name,type;
```

b. 從原始預設服務，設定unique_name為NULL

```
# update disk_offering set unique_name = NULL where id = 10;
```

確定您使用正確的ID

c. 現在新服務已經變成預設值，設定unique_name 數值如下

對於預設Console Proxy VM (CPVM)offering，將unique_name設為 'Cloud.com-ConsoleProxy'。對於預設Secondary Storage VM (SSVM) offering，將unique_name設為 'Cloud.com-SecondaryStorage'，例如:

```
update disk_offering set unique_name = 'Cloud.com-ConsoleProxy' where id = 16;
```

5. 重新啓動CloudStack管理伺服器，為使變更仔入記憶體

```
service cloudstack-management restart
```

6. 催毀現存的CPVM 或 SSVM offerings，然後等它們再生，新的CPVM 或 SSVM即有心的設定

為使用者建立網路

9.1. 為使用者設定網路簡介

使用者在使用雲端時，會有不同的需求及偏好。身為一個CloudStack管理者，您可以做以下事情來達成使用者的需求:

- 在zone中設定實體網路
- 在一個實體網路上建立多個不同的提供者(例如，有 Cisco和Juniper兩個防火牆)
- 將不同形式的網路服務合為一個網路服務，如此使用者可以在任何虛擬機器選擇不同的網路服務
- 隨時間新增網路服務，如此終端使用者可以更新到更好的服務
- 提供多種存取網路的方式，例如透過專案

9.2. 關於虛擬網路

虛擬網路是種邏輯架構，允許多個租戶在同一條實體網路。在CloudStack，虛擬網路可以分享或獨立

9.2.1. 獨立網路

獨立網路僅能被單一帳戶的虛擬機器存取，此網路有以下特性:

- 資源像是VLAN會被動態地分配及回收
- 有一個網路服務給整個網路
- 網路服務可以被更新或還原

9.2.2. Shared Networks

A shared network can be accessed by virtual machines that belong to many different accounts. Network Isolation on shared networks is accomplished using techniques such as security groups (supported only in basic zones).

- Shared Networks are created by the administrator
- Shared Networks can be designated to a certain domain
- Shared Network resources such as VLAN and physical network that it maps to are designated by the administrator
- Shared Networks are isolated by security groups
- Public Network is a shared network that is not shown to the end users

9.2.3. 虛擬網路資源的執行時間分配

當您定義一個新的虛擬網路，所有網路中的設定會被存在CloudStack，實際網路資源只會在第一個虛擬機器啓動時才會啓動。當所有虛擬機器離開虛擬網路時，網路資源會被垃圾回收好讓它們能再被分配。

9.3. 網路服務提供者

注意

對於大多最新支援的網路服務提供者，詳見CloudStack UI或呼叫listNetworkServiceProviders

服務提供者(也稱為網路元素)是使網路服務可用的硬體或虛擬應用，例如，防火牆可以提供防火牆服務。在單一網路，多個提供者可以提供同一種網路服務，例如，同一個網路防火牆可以由Cisco 或 Juniper裝置提供

您可以在同一個服務提供者中(例如不只一個Juniper SRX裝置)有多個instances

如果不同的提供者提供同一種服務，管理者可以建立網路服務讓使用者可以選用哪一個提供者(除了網路服務提供的選擇)，否則CloudStack會任意挑選服務

支援的網路服務提供者

CloudStack搭載一個內建的支援名單，您可以從名單中挑選建立網路服務的提供者

	虛擬路由器	Citrix NetScaler	Juniper SRX	F5 BigIP	Host based (KVM/Xen)
遠端存取VPN	Yes	No	No	No	No
DNS/DHCP/User Data	Yes	No	No	No	No
Firewall	Yes	No	Yes	No	No
Load Balancing	Yes	Yes	No	Yes	No
Elastic IP	No	Yes	No	No	No
Elastic LB	No	Yes	No	No	No
Source NAT	Yes	No	Yes	No	No
Static NAT	Yes	Yes	Yes	No	No
Port Forwarding	Yes	No	Yes	No	No

9.4. Network Offerings

注意

對於大多最新支援的網路服務名單，詳見CloudStack UI或呼叫listNetworkServices

Network offering是指一群網路服務的集合

- DHCP
- DNS

- Source NAT
- Static NAT
- Port Forwarding
- Load Balancing
- Firewall
- VPN
- 選擇性)選擇一個可用的提供者來使用這個服務，如將防火牆使用在 Juniper
- (選擇性)將網路tag到要使用的實體網路

當建立一個新的VM時，使用者需要選擇一個可用的網路來供VM使用

除了CloudStack建立的預設網路服務，CloudStack管理者可以建立任意個網路服務。您可以設定您的雲端在多租戶網路提供不同等級的服務，例如，如果兩租戶的基本實體網路配線是相同的，假使租戶A只需要簡單的防火牆，而租戶B想要運行網頁伺服器並需要替終端安裝可擴充的防火牆、 load balancing及替代網路。

注意

如果你在使用像NetScaler，這種會改變其他正在用CloudStack虛擬路由器使用者的網路服務的外部負載平衡裝置，你必須在虛擬路由器上，為每一個存在的規則建立防火牆，好讓它們能正確執行

建立新的虛擬網路時， CloudStack管理者會選擇一個網路服務給網路。每個虛擬網路會接到一個網路服務。而虛擬網路可以藉由更新或還原來改變連結，如果您做了此步驟，請重新改編實體網路

CloudStack在CloudStack系統VMs也有內部網路服務，這些網路服務對使用者是不可見的，但管理者可以修改

9.4.1. 新增新的網路服務

想新增網路服務:

1. 以管理者優先登入CloudStack使用者介面
2. 在左邊的導覽視窗，選擇Service Offerings
3. 在Select Offering中，選擇Network Offering
4. 按下Add Network Offering
5. 在對話框中，選擇以下:
   - Name: 網路服務的名稱
   - Description: 使用者可見的簡述
   - Network Rate: 允許的資料傳輸速率，單位為MB每秒
   - Guest Type: 選擇訪客網路為獨立或分享

這項的詳細敘述，參見節 9.2, “關於虛擬網路”

- Persistent：訪客網路是否持續，即您是否需要部屬VM在這個網路，更多資訊，詳見節 15.20, “持續網路”
- Specify VLAN：(僅獨立訪客網路)使用服務時，VLAN使否需要指定
- VPC：訪客網路是否Virtual Private Cloud-enabled，Virtual Private Cloud (VPC)是私人、獨立的CloudStack部件。VPC擁有自己的虛擬網路拓樸，像傳統實體網路。更多資訊，參見節 15.19.1, “關於虛擬私人雲端”
- Supported Services：選擇一至多個可用的服務。有些服務您必須選擇提供者，例如，如果您選擇Load Balancer，則您可以選擇CloudStack 虛擬路由器或是其他已設定的負載平衡器，取決於您選擇的服務，其他欄位可能會出現在其他對話框

基於訪客網路類型選擇，您可以看到以下支援的服務

支援的服務	Description	Isolated	Shared
DHCP	更多資訊，詳見 節 15.16, “DNS 及 DHCP”	Supported	Supported
DNS	更多資訊，詳見 節 15.16, “DNS 及 DHCP”	Supported	Supported
Load Balancer	如果您選擇Load Balancer，您可以選擇CloudStack虛擬路由器或是其他已設定的負載平衡器	Supported	Supported
Firewall	更多資訊，詳見 Administration Guide	Supported	Supported
Source NAT	如果您選擇Source NAT，您可以選擇 CloudStack虛擬路由器或是其他已設定的Source NAT提供者	Supported	Supported
Static NAT	如果您選擇Static NAT，您可以選擇 CloudStack虛擬路由器或是其他已設定的Static NAT提供者	Supported	Supported
Port Forwarding	如果您選擇Port Forwarding，您可以選擇 CloudStack虛擬路由器或是其他已設定的Port Forwarding提供者	Supported	不支援
VPN	更多資訊，詳見 節 15.17, “VPN”	Supported	不支援

支援的服務	Description	Isolated	Shared
User Data	更多資訊，詳見 節 20.3，“User Data and Meta Data”	不支援	Supported
Network ACL	更多資訊，詳見 節 15.19.4，“設定Access Control List”	Supported	不支援
Security Groups	更多資訊，詳見 節 15.7.2，“新增”	不支援	Supported

- System Offering：如果服務提供者在 Supported Services中選擇虛擬路由器，則會出現 System Offering欄位。選擇您想要的虛擬路由器系統服務，例如，您選擇了 Load Balancer，並選擇虛擬路由器提供負載平衡，則 System Offering欄位就會出現在CloudStack預設系統服務及其他由CloudStack root管理者定義的自訂系統服務之間

  更多資訊，詳見 節 8.2，“系統服務”

- Redundant router capability：只有當虛擬路由器被選為Source NAT provider時才能使用。如果您想要用兩個虛擬路由器作為不間斷連結，請選此選項：一個做為主路由器，另一個作為備份，主路由器接收要求，備份路由器僅在主路由器故障時啓動，此時備份路由器就變成主路由器。CloudStack會在多個主機部署路由器以增加網路可靠性

- Conserve mode. Indicate whether to use conserve mode. In this mode, network resources are allocated only when the first virtual machine starts in the network. When conservative mode is off, the public IP can only be used for a single service. For example, a public IP used for a port forwarding rule cannot be used for defining other services, such as StaticNAT or load balancing. When the conserve mode is on, you can define more than one service on the same public IP.

  注意

  如果啓用StaticNAT，不論使否有啓用保存模式，IP都不能建立通訊埠轉送及負載平衡規則，但您可以使用createFirewallRule指令來建立防火牆規則

- Tags：將網路tag到要使用的實體網路

6. 按Add

使用Virtual Machines

10.1. About Working with Virtual Machines

CloudStack provides administrators with complete control over the lifecycle of all guest VMs executing in the cloud. CloudStack provides several guest management operations for end users and administrators. VMs may be stopped, started, rebooted, and destroyed.

Guest VMs have a name and group. VM names and groups are opaque to CloudStack and are available for end users to organize their VMs. Each VM can have three names for use in different contexts. Only two of these names can be controlled by the user:

- Instance name — a unique, immutable ID that is generated by CloudStack, and can not be modified by the user. This name conforms to the requirements in IETF RFC 1123.
- Display name — the name displayed in the CloudStack web UI. Can be set by the user. Defaults to instance name.
- Name — host name that the DHCP server assigns to the VM. Can be set by the user. Defaults to instance name

Guest VMs can be configured to be Highly Available (HA). An HA-enabled VM is monitored by the system. If the system detects that the VM is down, it will attempt to restart the VM, possibly on a different host. For more information, see HA-Enabled Virtual Machines on

Each new VM is allocated one public IP address. When the VM is started, CloudStack automatically creates a static NAT between this public IP address and the private IP address of the VM.

If elastic IP is in use (with the NetScaler load balancer), the IP address initially allocated to the new VM is not marked as elastic. The user must replace the automatically configured IP with a specifically acquired elastic IP, and set up the static NAT mapping between this new IP and the guest VM's private IP. The VM's original IP address is then released and returned to the pool of available public IPs.

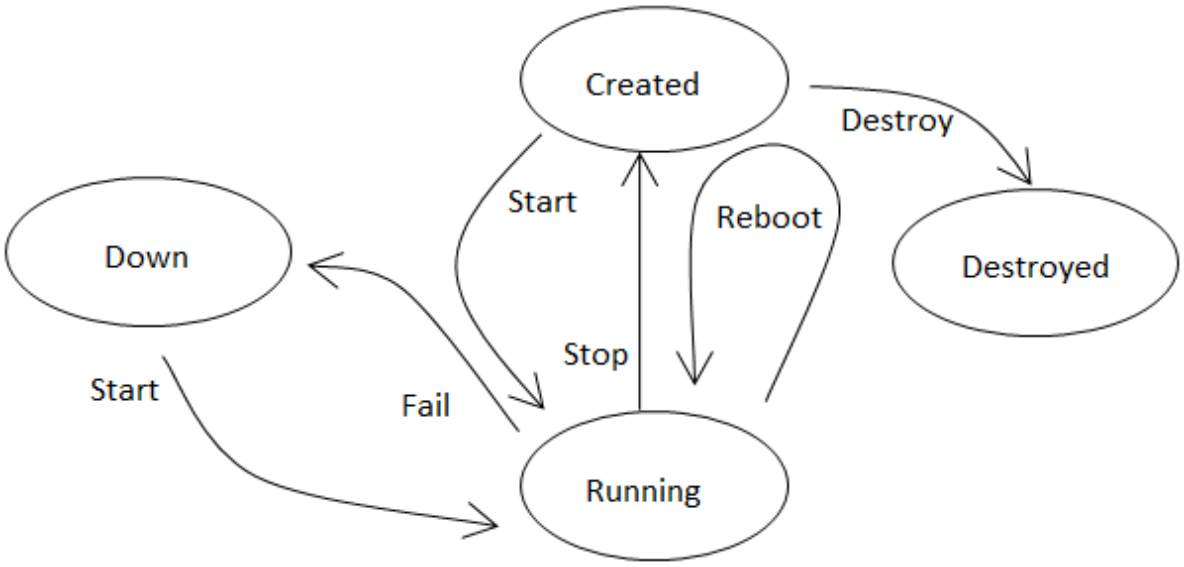
CloudStack cannot distinguish a guest VM that was shut down by the user (such as with the "shutdown" command in Linux) from a VM that shut down unexpectedly. If an HA-enabled VM is shut down from inside the VM, CloudStack will restart it. To shut down an HA-enabled VM, you must go through the CloudStack UI or API.

10.2. 虛擬機器的最佳練習

CloudStack 管理者需要監視每台叢集上有多少虛擬機器，如果接近超級監督者能負荷的最大量，管理者需要停止分配到此叢集。請確定遠離安全界線，以增加主機故障的容忍程度，主機故障會增加其他主機的虛擬機器負擔。參照您選擇的超級監督者文件，取得允許的最大量，然後使用 CloudStack廣域組態設定將其設為預設值。隨時監視虛擬機器的活動，並保持虛擬機器總數在安全界線之下，以允許偶而的主機故障。例如，如果有N台主機，然後您想要隨時關閉一台主機，而能夠允許的虛擬機器總量最多為(N-1) *(每台主機限制)，一旦叢集達到限制數量，請使用 CloudStack使用者介面來停止更多虛擬機器分配到此叢集

10.3. 虛擬機器生命週期

虛擬機器可能為以下幾種狀態:



虛擬機器被移除後，將無法復原。所有資源將會還給系統，包含IP位址

停止虛擬機器會關閉作業系統，所有執行中的應用程式都會終止。如果作業系統無法正常停止，則會被强制終止。與拔除機器電源線有相同的效果

重新啓動是啓動之後的下一個狀態

CloudStack 會保留虛擬機器硬碟狀態直到機器被移除為止

執行中的虛擬機器有可能因硬體或網路問題而錯誤，故障的虛擬機器會在 down狀態

如果超級監督者沒有收到虛擬機器的心跳三分鐘，系統會將虛擬機器放到down狀態

使用者可以手動重新啓動虛擬機器如果機器在down狀態

如果虛擬機器被標示為HA-enabled，系統會自動啓動虛擬機器

10.4. 建立VM

虛擬機器通常由模組建立，使用者也可以建立空的虛擬機器，空的虛擬機器是沒有作業系統的虛擬機器。使用者可以附上ISO然後從光碟機安裝

注意

您可以建立VM但不要啓動，您可以決定是否隨部署完成啓動虛擬機器，在deployVm API提供欄位startVM給您，更多資訊，詳見Developer's Guide

想要從模組建立VM:

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇 Instances
3. 點選Add Instance
4. 選擇一個區域

5. 選擇一個模組，然後依照安裝精靈執行，更多資訊，詳見章 12，使用模組

6. 請確定您允許的硬體開始執行選擇的service offering

7. 點選Submi，您的VM就會建立及啓動

注意

為安全考量，VM的內部名稱僅為root管理者所見

想要從ISO建立VM:

注意

(XenServer)Windows VMs在XenServer上執行需要PV驅動程式，有可能會在模組中就有，或是在VM建立後新增。PV驅動程式對基礎管理功能如掛在額外的volumes和ISO images、live migration和graceful shutdown是必要的。

1. 以管理者或終端使用者登入CloudStack UI

2. 在左邊的導覽視窗，選擇 Instances

3. 點選Add Instance

4. 選擇一個區域

5. 選擇 ISO Boot並跟著精靈的步驟安裝

6. 點選Submi，您的VM就會建立及啓動

10.5. 存取VM

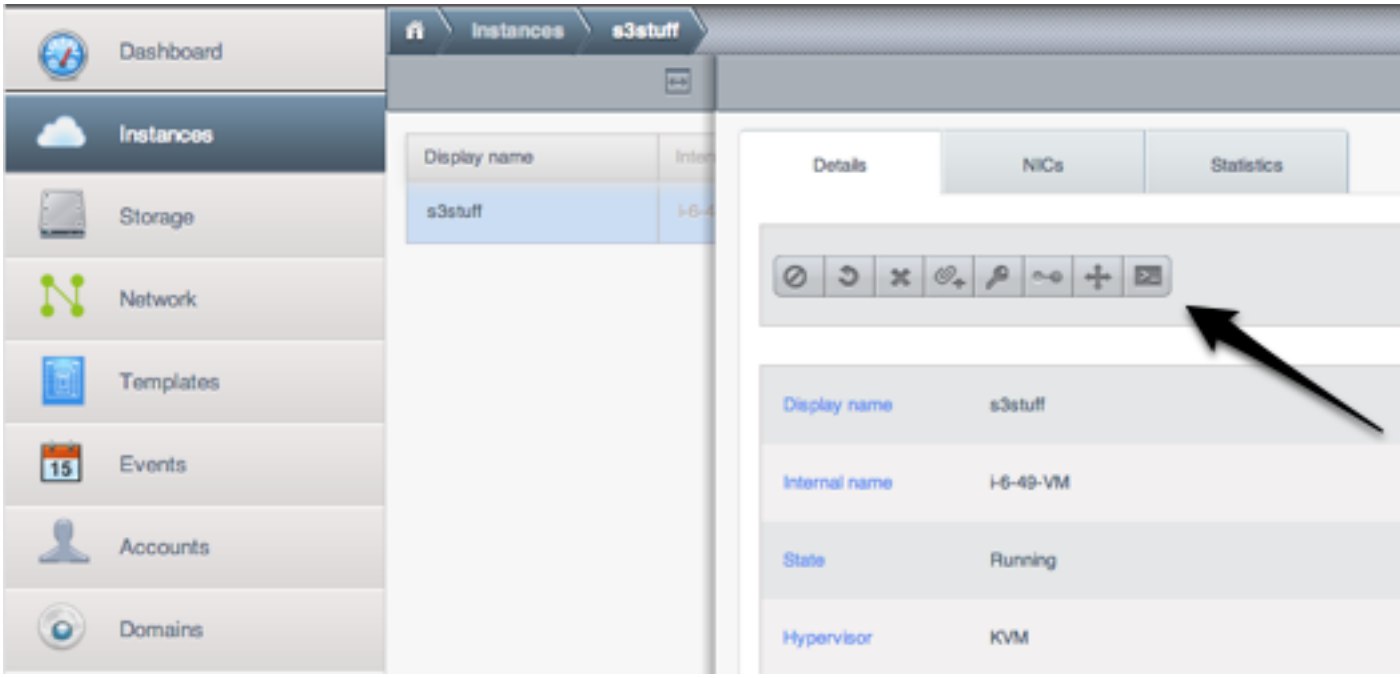
任何使用者都可以存取他們的虛擬機器，管理者可以存取所有運作的VM

從CloudStack使用者介面登入VM:

1. 以使用者或管理者身分登入CloudStack UI

2. 選擇Instances，然後點選運行的VM名稱

3. 點選View Console



透過網路直接存取VM:

1. VM必須有輸入流量的通訊埠，例如，在basic zone，新的VM可能會指定給一個允許輸入流量的安全群組，取決於建立VM時您挑的安全群組。另一個例子，您可以建立通訊埠轉送規則來開啓通訊埠，詳見 節 15.14，“IP轉送及防火牆”

2. 如果通訊埠是開啓的，但您不能用ssh存取VM，有可能是ssh還沒啓用，這取決於模組的ssh是否開啓。透過 CloudStack使用者介面存取VM，然後使用以下指令啓用ssh:

3. 如果網路有外部防火牆裝置，您需要建立防火牆規則來允許存取，詳見節 15.14，“IP轉送及防火牆”

10.6. Stopping and Starting VMs

Once a VM instance is created, you can stop, restart, or delete it as needed. In the CloudStack UI, click Instances, select the VM, and use the Stop, Start, Reboot, and Destroy links.

10.7. 改變VM名稱、作業系統或群組

VM建立後，您可以修改名稱、作業系統及所屬群組

從CloudStack使用者介面登入VM:

1. 以使用者或管理者身分登入CloudStack UI

2. 在左邊的導覽視窗，選擇 Instances

3. 選擇要修改的VM

4. 點選Stop按鈕暫停您的虛擬機器 

5. 按下Edit 

6. 依照您的需求修改:

7. Display name: 輸入新的名稱

8. OS Type: 選擇想要的作業系統

9. Group: 輸入群組名稱

10. 按Apply

10.8. 更改虛擬機的Service Offering

您可以透過修改虛擬機器的Compute Offering調整運算資源。

1. 以使用者或管理者身分登入CloudStack UI

2. 在左邊的導覽視窗, 選擇 Instances

3. 選擇一台虛擬機器

4. 點選Stop按鈕暫停您的虛擬機器 

5. 點選Change Service按鈕。 

   將出現修改Service Offering的對話視窗

6. 選擇一個您想要提供虛擬機器的Service Offering。

7. 按OK

10.9. 在主機間移動VM(手動移動)

CloudStack管理者可以再不打斷服務及進入維護模式的情況下, 移動執行中的VM。此動作稱為手動移動, 可以在以下情況操作:

・登入root管理者, 網域管理者及使用者無法執行此動作

・VM正在運行。停止的VM無法執行動作

・目的地主機必須和原來的主機是同一cluster

・VM必須使用本地硬碟儲存裝置

・目的地主機必須有足夠的空間, 否則VM會持續 "migrating"狀態直到記憶體足夠為止

要手動移動虛擬機器

1. 以使用者或管理者身分登入CloudStack 使用者介面

2. 在左邊的導覽視窗, 選擇 Instances

3. 選擇想要移動的VM

4. 點選Migrate Instance 

5. 從主機列表中選擇要移動VM的目的地主機

6. 按OK

10.10. 刪除VM

使用者可以刪除自己的VM，被刪除的VM如果正在執行，會直接被中斷。管理者能刪除任何VM

刪除VM:

1. 以使用者或管理者身分登入CloudStack UI
2. 在左邊的導覽視窗，選擇 Instances
3. 選擇想要刪除的VM
4. 按下Destroy Instance 

10.11. 使用ISO

CloudStack 支援ISO及其附件。ISO為唯讀檔案，是ISO/CD-ROM形式的檔案系統。使用者可以上傳自己的ISO，並將其安裝在自己的訪客虛擬機器

ISOs使用URL上傳，HTTP為支援的協定。一旦ISO可經由HTTP存取，請指定一組上傳URL，像是http://my.web.server/filename.iso

ISOs可能為公開或私人，跟模組很像。ISO並沒有超級監督者限定，也就是在vSphere地訪客可以安裝與KVM訪客相同的映象

ISO映像可能會存放在系統中，並可在私人層級存取，如同模組。ISO映像可分類為可開機或不可開機。可開機ISO映像包含作業系統，CloudStack 允許使用者使用ISO映像啓動訪客虛擬機器，使用者也可以連接ISO映像到訪客虛擬機器。例如，此功能讓PV驅動程式可以安裝到 Windows。ISO映像不是超級監督者限定

10.11.1. 新增ISO

為了使額外的作業系統或其他軟體可以被訪客VM使用，您可以新增一個ISO。ISO典型上是作業系統的映像，但是您需要為其他型態的軟體新增ISO，例如您想要將"桌面"設為安裝模組

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Templates
3. 於Select View中選擇ISO
4. 點選Add ISO
5. 在Add ISO畫面，提供以下:
   - Name: ISO映像的短名，例如 CentOS 6.2 64-bit
   - Description: 顯示ISO映像的描述，例如CentOS 6.2 64-bit
   - URL: 接管ISO映像的URL，管理伺服器必須能夠透過HTTP存取這個位址。您可以直接將映像放在管理伺服器
   - Zone: 選擇您想要用ISO的zone，選擇 All Zones使整個CloudStack都能使用
   - Bootable: 訪客是否能啓動映像，例如，CentOS ISO 可以啓動，Microsoft Office ISO不能啓動

- OS Type: 這項幫助CloudStack及超級監督者可以執行特定指令，並承擔改善訪客效能的責任，從以下選擇一個
  - 如果您要的作業系統映像有在裡面，請選它
  - 如果沒有或是不可啓動，則選Other
  - (僅XenServer)如果您想用PV模式啓動這個ISO，選擇PV (32-bit) 或 Other PV (64-bit)
  - (僅KVM)如果您選擇啓用PV的作業系統，從ISO建立的VM將會有 SCSI (virtio) root 硬碟；如果不是，VM會產生IDE root硬碟。PV啓用的形式為:

Fedora 13	Fedora 12	Fedora 11
Fedora 10	Fedora 9	Other PV
Debian GNU/Linux	CentOS 5.3	CentOS 5.4
CentOS 5.5	Red Hat Enterprise Linux 5.3	Red Hat Enterprise Linux 5.4
Red Hat Enterprise Linux 5.5	Red Hat Enterprise Linux 6	

注意

我們不建議您選擇較舊的版本，例如，選擇CentOS 5.4來支援CentOS 6.2映像通常是不行的，這個情況請選Other

- Extractable: 如果想要ISO可以解壓縮，請選Yes
- Public: 如果想要ISO可以給其他使用者使用，請選Yes
- Featured: 如果您想要ISO比較顯眼，請選Yes。ISO會在Featured ISOs表中出現，這項功能僅管理者能使用

6. 按OK

   管理伺服器會開始下載ISO，時間由ISO大小決定。下載完成會顯示Ready，按Refresh可以更新下載進度

7. Important: 請等ISO下載完成，如果您在還沒下載完成就直接使用，會出現錯誤。因此請等到CloudStack能夠使用

10.11.2. 附加ISO到VM

1. 在左邊的導覽視窗，選擇 Instances
2. 選擇想要套用的VM
3. 按下Attach ISO
4. 在Attach ISO對話框，選擇想要的ISO

5. 按OK

使用主機

11.1. 新增主機

您可以隨時增加主機來提供更多訪客虛擬機器的容量，關於需求及指南，詳見 節 7.6, “增加主機”

11.2. Scheduled Maintenance and Maintenance Mode for Hosts

You can place a host into maintenance mode. When maintenance mode is activated, the host becomes unavailable to receive new guest VMs, and the guest VMs already running on the host are seamlessly migrated to another host not in maintenance mode. This migration uses live migration technology and does not interrupt the execution of the guest.

11.2.1. vCenter and Maintenance Mode

To enter maintenance mode on a vCenter host, both vCenter and CloudStack must be used in concert. CloudStack and vCenter have separate maintenance modes that work closely together.

1. Place the host into CloudStack's "scheduled maintenance" mode. This does not invoke the vCenter maintenance mode, but only causes VMs to be migrated off the host

   When the CloudStack maintenance mode is requested, the host 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. Live migration will be used to move VMs off the host. This allows the guests to be migrated to other hosts with no disruption to the guests. After this migration is completed, the host will enter the Ready for Maintenance mode.

2. Wait for the "Ready for Maintenance" indicator to appear in the UI.

3. Now use vCenter to perform whatever actions are necessary to maintain the host. During this time, the host cannot be the target of new VM allocations.

4. When the maintenance tasks are complete, take the host out of maintenance mode as follows:

   a. First use vCenter to exit the vCenter maintenance mode.

      This makes the host ready for CloudStack to reactivate it.

   b. Then use CloudStack's administrator UI to cancel the CloudStack maintenance mode

      When the host comes back online, the VMs that were migrated off of it may be migrated back to it manually and new VMs can be added.

11.2.2. XenServer及維護模式

對於 XenServer，您可以暫時將伺服器離線，進入維護模式。當您進入維護模式，所有執行的VM將自動移到群組中其他主機，如果伺服器為群組的主伺服器，則會選擇另一個新的主伺服器，在維護模式，您不能建立或啓動VM

To place a server in Maintenance Mode:

1. 在Resources面板，選擇該伺服器，然後以下其中一個:

   ・按右鍵，然後再潔淨選單點選Enter Maintenance Mode

   ・在Server 選單，點選Enter Maintenance Mode

2. 點選 Enter Maintenance Mode

所有執行中的VM完成移動後，Resources面板上的伺服器狀態會出現

To take a server out of Maintenance Mode:

1. 在Resources面板，選擇該伺服器，然後以下其中一個:

   ・案右鍵，然後在捷徑選單點選Exit Maintenance Mode

   ・在 Server 選單，點選Exit Maintenance Mode

2. 點選Exit Maintenance Mode

11.3. 停用及啓用區域、pod及叢集

您可以啓用或停用區域、pod或叢集，不用永久移除，對於維護或有問題時很有用，停用的區域、pod或叢集不能被分配直到回到啓用狀態，當區域、pod或叢集剛加到雲端時，預設為 Disabled

停用及啓用區域、pod及叢集

1. 以administrator身分登入CloudStack UI
2. 於左側的navigation按鈕中，點選Infrastructure。
3. 於Zones的方框中點選View More
4. 如果您正停用或啓用區域，找到區域名稱，然後點選Enable/Disable 
5. 如果您正停用或啓用pod或叢集，點選包含它們的區域名稱
6. 點選Compute分頁
7. 在圖中的Pods或Clusters node，點選 View All
8. 點選表中的pod或叢集名稱
9. 點選Enable/Disable 

11.4. Removing Hosts

Hosts can be removed from the cloud as needed. The procedure to remove a host depends on the hypervisor type.

11.4.1. Removing XenServer and KVM Hosts

A node cannot be removed from a cluster until it has been placed in maintenance mode. This will ensure that all of the VMs on it have been migrated to other Hosts. To remove a Host from the cloud:

1. Place the node in maintenance mode.

See 節 11.2, “Scheduled Maintenance and Maintenance Mode for Hosts”.

2. For KVM, stop the cloudstack-agent service.

3. Use the UI option to remove the node.

   Then you may power down the Host, re-use its IP address, re-install it, etc

11.4.2. Removing vSphere Hosts

To remove this type of host, first place it in maintenance mode, as described in 節 11.2, “Scheduled Maintenance and Maintenance Mode for Hosts”. Then use CloudStack to remove the host. CloudStack will not direct commands to a host that has been removed using CloudStack. However, the host may still exist in the vCenter cluster.

11.5. 重新安裝主機

在維護模式下，您可以重新安裝主機，然後移除。如果主機故障，無法進入維護模式，即使還沒重新安裝，您仍需移除

11.6. 維護主機的超級監督者

當在主機上執行超級監督者的軟體時，請確定所有hypervisor vendor提供的hotfixes已經被套用了。在hypervisor vendor’s support channel尋找已釋出的hypervisor patches，並在補丁發布後盡速安裝。CloudStack不會自動搜尋或提醒您。對您的主機來說，更新到最新是必要的，因為hypervisor vendor會拒絕支援非最新的系統

注意

缺少最新的hotfixes會導致資料毀損及VM錯誤

(XenServer)更多資訊，詳見Highly Recommended Hotfixes for XenServer in the CloudStack Knowledge Base[1]

11.7. 改變主機密碼

XenServer Node、KVM Node或vSphere Node的密碼可以在資料庫改變。注意，同一叢集的所有節點必須是同一密碼

想要改變節點的密碼:

1. 確認所有主機

2. 改變所有叢集內的主機密碼，現在主機密碼與 CloudStack中的密碼會不一樣，因此任何叢集上的操作都會失敗，請將兩個密碼改成相同的

[1] http://docs.cloudstack.org/Knowledge_Base/Possible_VM_corruption_if_XenServer_Hotfix_is_not_Applied/Highly_Recommended_Hotfixes_for_XenServer_5.6_SP2

3. 取得主機ID的列表，您會需要存取資料庫來決定這些主機ID，對於每個您要改密碼的主機名稱"h"(或vSphere叢集)執行：

```
mysql> select id from cloud.host where name like '%h%';
```

4. 應該會回復一個ID，請記錄這些ID

5. 更新主機密碼，在此範例，我們將主機ID為5、10及12的密碼改為"password"

```
mysql> update cloud.host set password='password' where id=5 or id=10 or id=12;
```

11.8. 主機分配

系統會自動挑選最適當的主機來執行每個虛擬機器，終端使用者可以指定區域來建立虛擬機器。終端使用者沒有權限指定哪台主機執行虛擬機器

CloudStack 管理者可以指定主機給特定的訪客類型。例如，管理者可以指定此主機優先執行Windows訪客。預設主機分配者會依作業系統來分主機，如果沒有這種主機能用，分配者會在有足夠實體空間的地方放置 instance

垂直與平行分配皆允許。垂直分配會在分配任一訪客到第二個主機前，消耗掉現在主機的所有資源，會減低電能消耗。水平分配會將訪客依round-robin的形式放在每個主機，這樣在某些例子可以有更好的效能。CloudStack也允許CPU可以過度配置，由管理者設定。過度配置允許管理者有更多CPU cycles能分配訪客

CloudStack 也提供可插件式介面來增加分配者，這些自訂的分配者可以提供任何管理者想要的政策

11.8.1. Over-Provisioning and Service Offering Limits

CloudStack performs CPU over-provisioning based on an over-provisioning ratio configured by the administrator. This is defined by the cpu.overprovisioning.factor global configuration variable.

CloudStack performs CPU over-provisioning based on an over-provisioning ratio configured by the administrator. This is defined by the cpu.overprovisioning.factor global configuration variable

Service offerings limits (e.g. 1 GHz, 1 core) are strictly enforced for core count. For example, a guest with a service offering of one core will have only one core available to it regardless of other activity on the Host.

Service offering limits for gigahertz are enforced only in the presence of contention for CPU resources. For example, suppose that a guest was created with a service offering of 1 GHz on a Host that has 2 GHz cores, and that guest is the only guest running on the Host. The guest will have the full 2 GHz available to it. When multiple guests are attempting to use the CPU a weighting factor is used to schedule CPU resources. The weight is based on the clock speed in the service offering. Guests receive a CPU allocation that is proportionate to the GHz in the service offering. For example, a guest created from a 2 GHz service offering will receive twice the CPU allocation as a guest created from a 1 GHz service offering. CloudStack does not perform memory over-provisioning.

11.9. 設置VLAN

CloudStack會自動新增或移除主機上的VLAN橋接介面，通常管理者不需要管理此步驟

CloudStack 會依據不同的超級監督者，用不同方法管理VLAN。對於XenServer或KVM，VLAN只會建立在要使用的主機上，如果所有訪客都終止或移到其他主機，VLAN就會被移除

對於vSphere，VLAN會提共給所有叢集的主機，即使沒有任何訪客。此允許管理者執行實時移動及其他功能，不用再建立VLAN到目的地。除此之外，VLAN不會因主機不需要而被移除

您可以在不同實體網路使用相同的VLAN，使實體網路可以有自己的層級-2基礎架構，像是交換器。例如，在進階區域設定部署實體網路A及B時，您可以指定VLAN範圍500到1000。此功能允許您建立一個額外的層級-2實體基礎架構在不同的實體NIC，並且可以使用相同的VLAN。其他優點像是不同客戶可以使用相同組的IP，但是在不同的實體NIC使用自己的路由器及訪客網路

使用模組

模組是虛擬機器的可重複使用組態，當使用者執行VM時，可以選擇CloudStack中的一列模組

尤其，模組是虛擬硬碟映像，包含作業系統、額外的軟體像是office，及設定像是取得模組權限的控制權，每個模組都會連結到一個類型的超級監督者，在加到CloudStack時決定：

CloudStack附有預設的模組，為了要給使用者更多選擇，CloudStack管理者及使用者都可以建立模組及將它們加到CloudStack

12.1. 新增模組：總覽

CloudStack為CentOS搭載預設模組。而管理者及使用者可以用很多方法來新增模組，常用的方法為：

1. 執行有您要的作業系統的VM instance，設定其他您要的設定

2. 停止VM

3. 將volume轉成模組

有很多方式能將模組加到 CloudStack，例如，您可以snapshot您的VM volume並由snapshot建立模組，或是從其他系統匯入VHD到 CloudStack

更多建立模組的技術將在以下章節描述

12.2. Requirements for Templates

- For XenServer, install PV drivers / Xen tools on each template that you create. This will enable live migration and clean guest shutdown.
- For vSphere, install VMware Tools on each template that you create. This will enable console view to work properly.

12.3. 模組的最佳練習

如果您計畫使用大型模組(100GB以上)請確定您有支援大型模組的10-gigabit網路，太慢的網路可能會導致超時或其他錯誤

12.4. The Default Template

CloudStack 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 root password for the default template is "password".

A default template is provided for each of XenServer, KVM, and vSphere. The templates that are downloaded depend on the hypervisor type that is available in your cloud. Each template is approximately 2.5 GB physical size.

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-
```

12.5. Private and Public Templates

When a user creates a template, it can be designated private or public.

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

When a user marks a template as “public,” the template becomes available to all users in all accounts in the user's domain, as well as users in any other domains that have access to the Zone where the template is stored. This depends on whether the Zone, in turn, was defined as private or public. A private Zone is assigned to a single domain, and a public Zone is accessible to any domain. If a public template is created in a private Zone, it is available only to users in the domain assigned to that Zone. If a public template is created in a public Zone, it is available to all users in all domains.

12.6. 從已有的虛擬機器建立模組

當您至少有一個設定好的VM，您就可以將它使用為其他VM的圓形

1. 使用節 10.4, “建立VM”中的技術建立及開始虛擬機器
2. 在執行的VM做任何您想要的設定，然後按Stop
3. 等VM停止，當狀態顯示Stopped，才進行下一步
4. 選擇Create Template 並提供以下資訊:
   - Name and Display Text: 這些會出現在使用者介面
   - OS Type: 這項幫助CloudStack及超級監督者可以執行特定指令，並承擔改善訪客效能的責任，從以下選擇一個
     - 如果您要的停止的VM的作業系統有在裡面，請選它
     - 如果沒有，則選Other
     - 如果您想要從PV模式啓動模組，請選擇Other PV (32-bit) 或Other PV (64-bit)，此選擇僅適用XenServere:

注意

注意：您不該選擇較舊的作業系統版本，例如，選擇CentOS 5.4來支援CentOS 6.2映像通常是不行的，這個情況請選Other

- Public：選擇Yes來使模組能被所有使用者存取，模組會出現在Community Templates列表，詳見節 12.5, “Private and Public Templates”
- Password Enabled：選擇Yes如果您的模組有 CloudStack密碼改變的程式碼，詳見節 12.13, “Adding Password Management to Your Templates”

5. 按Add

當進度完成，新的模組會出現在Templates，此模組就可以拿來建立新的VM

12.7. Creating a Template from a Snapshot

If you do not want to stop the VM in order to use the Create Template menu item (as described in 節 12.6, “從已有的虛擬機器建立模組”), you can create a template directly from any snapshot through the CloudStack UI.

12.8. 上船模組

vSphere 模組及ISOs

如果您上傳使用vSphere Client建立的模組，請確定OVA 檔案不包含ISO，如果有，從模組架設V會失敗

模組藉由URL上傳，HTTP為支援的協定。模組通常為很大的檔案，您可以選擇gzip來減少上傳時間

想要上傳模組：

1. 在左邊的導覽視窗，選擇Templates
2. 選擇 Register template
3. 提供以下：
   - Name and Description：這些會出現在使用者介面
   - URL：管理伺服器會從指定的URL下載檔案，像是 http://my.web.server/filename.vhd.gz
   - Zone：選擇您想要用模組的區域，選擇 All Zones使整個CloudStack都能使用
   - OS Type：這項幫助CloudStack及超級監督者可以執行特定指令，並承擔改善訪客效能的責任，從以下選擇一個
     - 如果您要的停止的VM的作業系統有在裡面，請選它

- 如果沒有，則選Other

注意

您不該選擇較舊的作業系統版本，例如，選擇CentOS 5.4來支援CentOS 6.2映像通常是不行的，這個情況請選Other

- Hypervisor：會列出支援的超級監督者，選擇其一
- Format：上傳模組的格式，像是VHD 或 OVA
- Password Enabled：選擇Yes如果您的模組有 CloudStack密碼改變的程式碼，詳見Adding Password Management to Your Templates
- Extractable：選擇Yes如果模組可解壓縮，如果有選擇，終端使用者可以下載完整的模組映像
- Public：選擇Yes來使模組可以被所有使用者使用，模組會出現在Community Templates列表，詳見節 12.5, “Private and Public Templates”
- Featured：如果您想要模組比較顯眼，請選Yes。模組會在Featured Templates表中出現，這項功能僅管理者能使用

12.9. Exporting Templates

End users and Administrators may export templates from the CloudStack. Navigate to the template in the UI and choose the Download function from the Actions menu.

12.10. 新增Windows 模組

Windows模組必須在使用到多台機器前，使用Sysprep來準備。 Sysprep允許您建立通用的模組並避免任何可能的SID衝突

注意

(XenServer)Windows VMs在XenServer上執行需要PV驅動程式，有可能會在模組中就有，或是在VM建立後新增。PV驅動程式對基礎管理功能如掛在額外的volumes和ISO images、live migration和graceful shutdown是必要的。

以下為流程概述：

1. 上傳您的Windows ISO

   更多資訊，詳見 節 10.11.1, “新增ISO”

2. 使用ISO建立VM Instance

   更多資訊，詳見節 10.4, “建立VM”

3. 使用 Sysprep for Windows Server 2008 R2 (以下)或Sysprep for Windows Server 2003 R2, 這取決於您的Windows Server版本

4. 準備已完成, 現在您可以實際藉由Creating the Windows Template的描述建立模組了

12.10.1. Windows Server 2008 R2的系統準備

對於Windows 2008 R2, 請您執行Windows System Image Manager來建立自訂的sysprep對應 XML檔案, Windows System Image Manager是Windows Automated Installation Kit (AIK)安裝的一部份。 Windows AIK可以在Microsoft Download Center[1]下載

使用以下步驟來執行Windows 2008 R2 系統準備:

注意

這裡的步驟是擷取自Charity Shelbourne的指南, 原始版本 Windows Server 2008 Sysprep Mini-Setup.[2]

1. 下載及安裝 Windows AIK

注意

僅被使用來建立sysprep answer檔案。請不要安裝在Windows 2008 R2 VM, Windows AIK不應該是模組的一部份

2. 複製Windows 2008 R2安裝光碟\sources資料夾中的 install.wim到硬碟, 這是一個非常大的檔案, 會傳有點久, 但 Windows AIK可寫的 WIM檔案, 因此請耐心等候

3. 啓動Windows System Image Manager

4. 在Windows Image方格, 右鍵選擇Select a Windows image或 catalog file option來讀取 install.wim文件

5. 選擇Windows 2008 R2 Edition

   您會被提示catalog file無法被開啓, 選擇Yes建立新的 catalog file

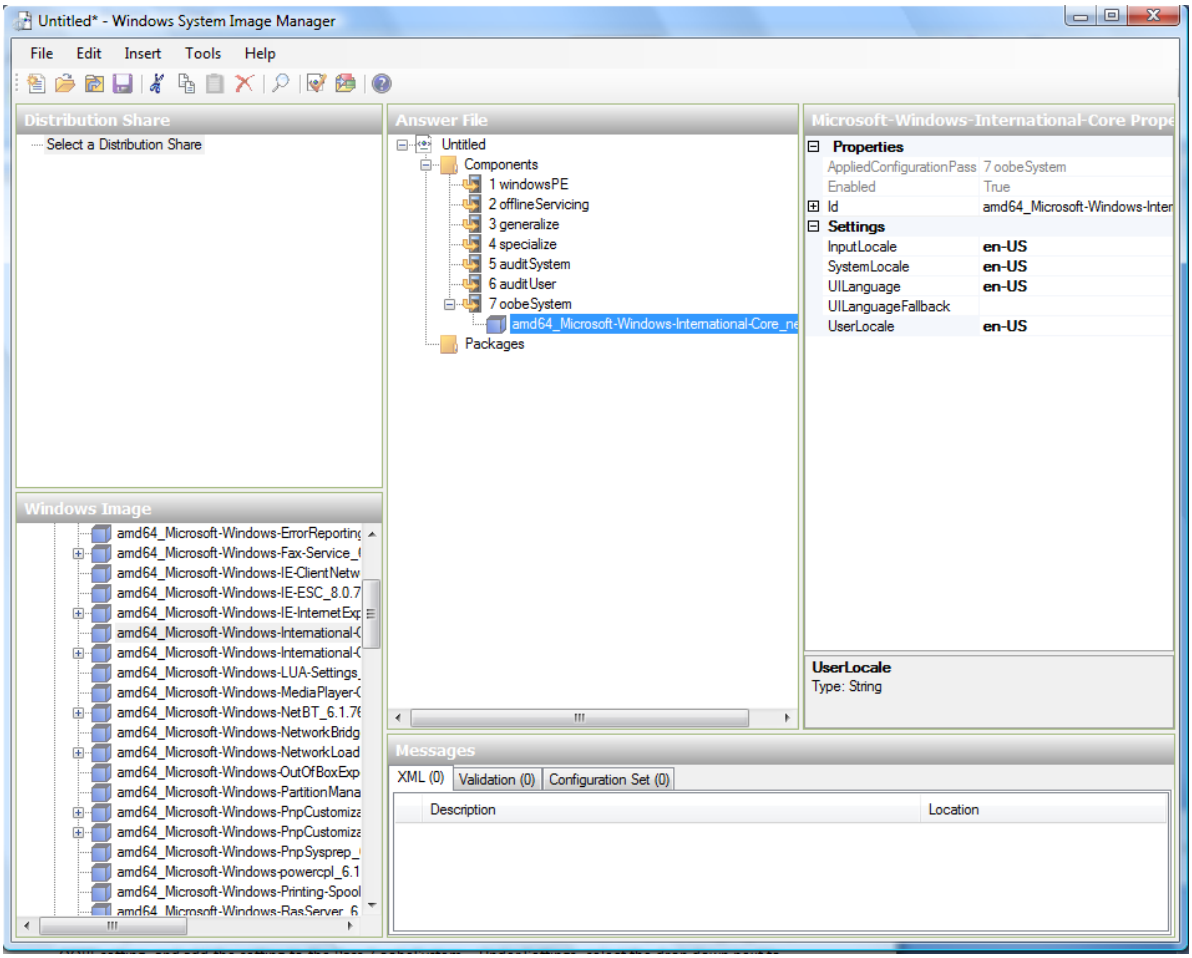
6. 在Answer File格子中, 右鍵點選建立新的answer file

7. 從Windows System Image Manager用以下步驟建立answer file:

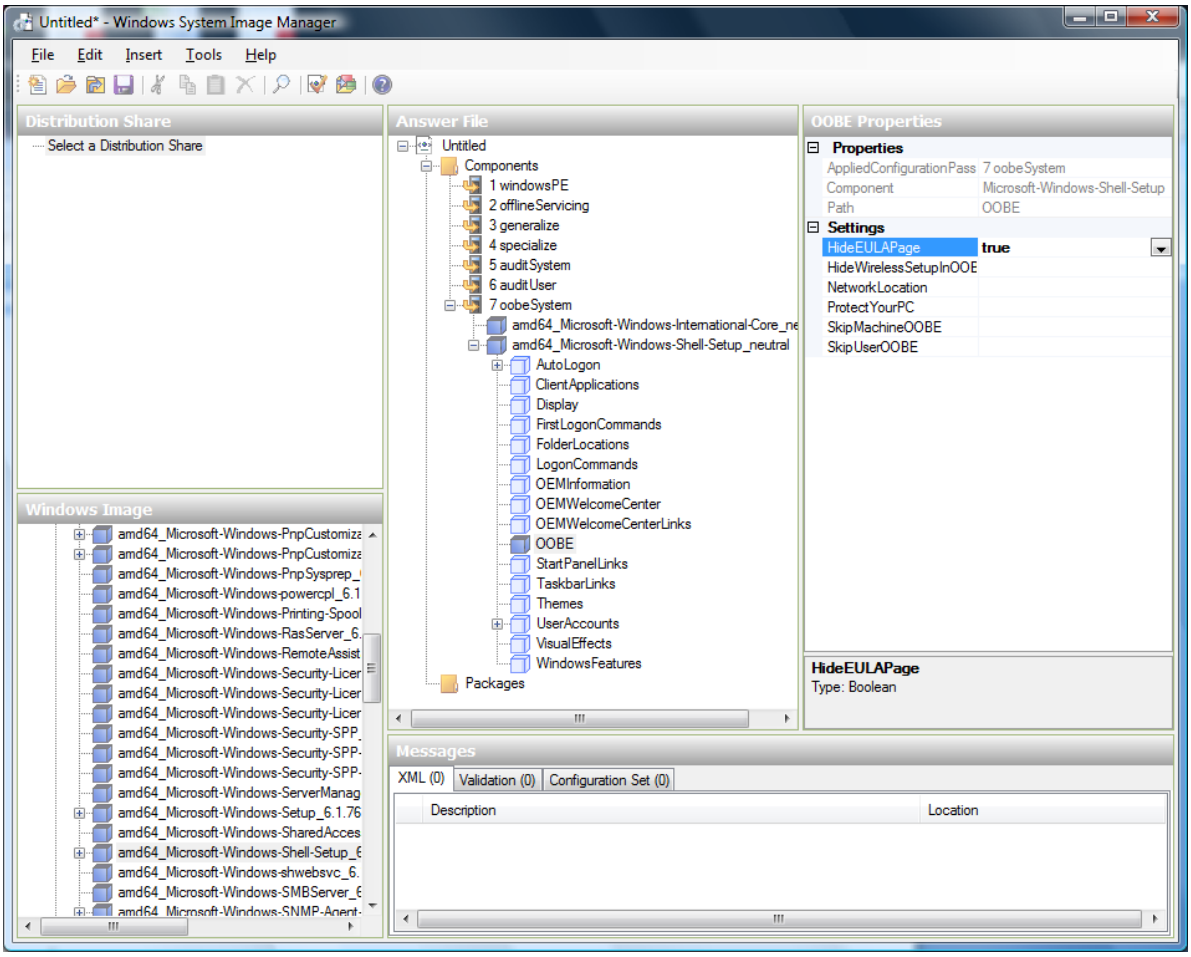
   a. 您需要自動化的頁面是Language and Country or Region Selection, 在Windows Image方格展開Components, 右鍵點選增加Microsoft-Windows-International-Core設定為Pass 7

[1] http://www.microsoft.com/en-us/download/details.aspx?id=9085
[2] http://blogs.technet.com/askcore/archive/2008/10/31/automating-the-oobe-process-during-windows-server-2008-sysprep-mini-setup.aspx

oobeSystem。在Answer File方格設定 InputLocale、SystemLocale、UILanguage及UserLocale為您的語言及地區，如果您對這些設定有疑問，您可以在設定上右鍵點選Help。

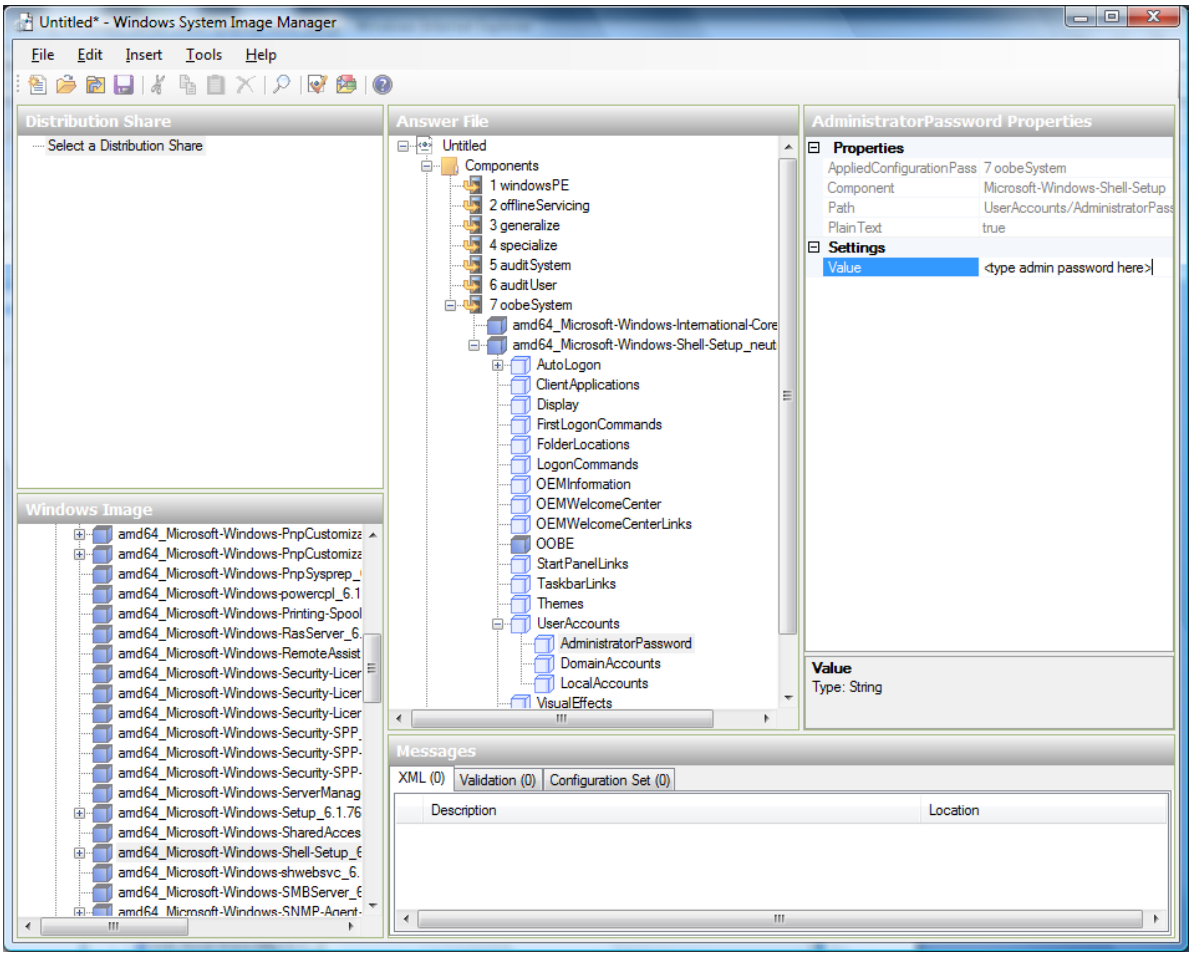


b. 您需要自動化Software License Terms Selection，或是End-User License Agreement (EULA)。展開Microsoft-Windows-Shell-Setup物件，反白 OOBE設定並增加設定到 Pass 7 oobeSystem。在 Settings設定 HideEULAPage為true



c. 確保 license key已經設定好。如果您是使用MAK key，您可以在Windows 2008 R2 VM進入 MAK key，不用先輸入MAK到Windows System Image Manager。如果您是使用KMS主機來啓動license，您不需要輸入Product Key。您可以在http://technet.microsoft.com/en-us/library/bb892849.aspx得到 Windows Volume Activation的詳細資料

d. 您需要自動化Change Administrator Password，展開Microsoft-Windows-Shell-Setup物件(還沒有展開的話)，展開 UserAccounts，右鍵點選AdministratorPassword並增加Pass 7 oobeSystem configuration pass設定到您的 answer file，在Settings下，在 Value旁指定一個密碼



您可以閱讀AIK文件並設定適合您的設定，以上步驟為最少的需求

8. 將answer file存為unattend.xml，您可以忽略警示訊息

9. 複製 unattend.xml到Windows 2008 R2 Virtual Machine的 c:\windows\system32\sysprep資料夾

10. 當您複製好unattend.xml到c:\windows\system32\sysprep資料夾後，請您執行sysprep tool:

```
cd c:\Windows\System32\sysprep
sysprep.exe /oobe /generalize /shutdown
```

Windows 2008 R2 VM會在sysprep完成後自動關機

12.10.2. Windows Server 2003 R2的系統準備

之前的Windows版本有不同的sysprep tool，此為Windows Server 2003 R2的步驟:

1. 從 Windows安裝光碟取出\support\tools\deploy.cab，將其移到Windows 2003 R2虛擬機器的 c:\sysprep資料夾

2. 執行c:\sysprep\setupmgr.exe來新增sysprep.inf檔案

   a. 點選Create New來建立新的 Answer檔案

   b. 輸入 “Sysprep setup” 來設定

   c. 選擇適當的作業系統版本

d. 在License Agreement視窗，選擇 “Yes fully automate the installation"

e. 提供您的名稱及組織

f. 將顯示設定設為預設

g. 設定適當的時區

h. 提供您的產品金鑰

i. 選擇適當的 license模式

j. 選擇 “Automatically generate computer name”

k. 輸入預設的管理者密碼，如果您啓用密碼重設功能，使用者有可能不會使用此密碼。此密碼會被訪客重設

l. 將Network Components設為 “Typical Settings”

m. 選擇 “WORKGROUP”

n. 將Telephony選項設為預設

o. 選擇適當的Regional Settings

p. 選擇適當的語言

q. 不要安裝印表機

r. 不要指定 “Run Once commands”

s. 不要指定相同的字串

t. 將Answer檔案存為 c:\sysprep\sysprep.inf

3. 執行以下指令來準備映像:

```
c:\sysprep\sysprep.exe -reseal -mini -activated
```

此步驟後，機器會自動關機

12.11. Importing Amazon Machine Images

The following procedures describe how to import an Amazon Machine Image (AMI) into CloudStack when using the XenServer hypervisor.

Assume you have an AMI file and this file is called CentOS_6.2_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.

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.

注意

當複製及貼上指令時，請確定指令是貼成單一條線，因為有些文件瀏覽器會多出不必要的中斷

To import an AMI:

1. Set up loopback on image file:

```
# mkdir -p /mnt/loop/centos62
# mount -o loop  CentOS_6.2_x64 /mnt/loop/centos54
```

2. 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/centos62/ -y install kernel-xen
```

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

```
# mkdir -p /mnt/loop/centos62/boot/grub
# touch /mnt/loop/centos62/boot/grub/grub.conf
# echo "" > /mnt/loop/centos62/boot/grub/grub.conf
```

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

```
# cd /mnt/loop/centos62
# 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.

5. 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
```

6. 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
```

7. 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
```

8. 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
```

9. Change the password.

```
# passwd
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

10. Exit out of chroot.

```
# exit
```

11. 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
```

12. 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. See 節 12.13, “Adding Password Management to Your Templates” .

13. Unmount and delete loopback mount.

```
# umount /mnt/loop/centos54
# losetup -d /dev/loop0
```

14. 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_6.2_x64 xenhost:/var/run/sr-mount/a9c5b8c8-536b-a193-a6dc-51af3e5ff799/
```

15. 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_6.2_x64
-rw-r--r-- 1 root root 10G Mar 16 16:49 CentOS_6.2_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 6.2 x86_64"
cad7317c-258b-4ef7-b207-cdf0283a7923
```

16. 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_6.2_x64
 uuid=cad7317c-258b-4ef7-b207-cdf0283a7923
```

17. 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_6.2_x64.vhd.bz2
[root@xenhost a9c5b8c8-536b-a193-a6dc-51af3e5ff799]# scp CentOS_6.2_x64.vhd.bz2 webserver:/var/www/html/
templates/
```

12.12. 將Hyper-V VM轉成模組

想要將 Hyper-V VM轉成相容 • XenServer的CloudStack模組，您需要一個獨立且附帶NFS VHD SR的XenServer主機。您可以用掛載 CloudStack的XenServer任何版本，但是必須使用XenCenter 5.6 FP1或是 SP2(往下相容5.6版)，另外，附帶 NFS ISO SR會有幫助

對Linux VMs，在您想讓VM開始在XenServer啓用前，您需要在Hyper-V做些準備。如果您仍想要在Hyper-V使用VM，您需要複製VM及工作。反安裝Hyper-V Integration Components並檢查是否有任何在 /etc/fstab的相關檔案關連到裝置名稱:

1. 從linux_ic/drivers/dist資料夾，執行make uninstall("linux_ic"是複製Hyper-V Integration Components檔案的路徑)
2. 從備份/boot/回復原始的臨時文件系統(備份檔名為*.backup0)
3. 從/boot/grub/menu.lst移除"hdX=noprobe"
4. 檢查/etc/fsta是否有任何分割掛載了裝置名稱，將這些條目(如果有)改成掛載到LABEL 或 UUID，您可以從blkid 指令取得更多資訊

下一步，確定VM沒有執行，然後將VHD送至XenServer。以下有兩個選擇:

選擇一:

1. 使用XenCenter匯入VHD。在中到Tools>Virtual Appliance Tools>Disk Image Import
2. 選擇VHD，然後按 Next
3. 命名VM，在 Storage下選擇NFS VHD SR，啓用"Run Operating System Fixups"，然後選擇NFS ISO SR
4. 按下Next，然後按Finish。VM建好了

選擇二:

1. 執行XenConvert，在From下選擇VHD，在To下選擇XenServer，然後按Next
2. 選擇VHD，然後按 Next
3. 輸入XenServer主機資訊，然後按Next
4. 命名VM，然後按Next，接著按Convert。VM應該就建立好了

當您從Hyper-V VHD建立VM後，使用以下步驟來準備:

1. 啓動VM，移除Hyper-V Integration Services，然後重新開機
2. 安裝 XenServer Tools，然後重新啓動
3. 將VM準備成我們想要的樣子，例如，執行Windows VMs的sysprep，詳見 節 12.10，“新增Windows模組”

以上選擇都會建立HVM模式的VM，對Windows VMs是沒關係的，但Linux VMs需要最佳化，將Linux VM轉換到PV模式會需要額外的步驟，並且會依產品不同而不一樣

1. 關閉VM並從NFS storage複製VHD到網路伺服器。例如，掛載NFS分享並複製，或是從XenServer主機使用sftp 或 scp上傳
2. 在CloudStack，使用以下數值建立新的模組
   - URL. 給VHD指定URL
   - OS Type。使用適當的系統，對CentOS的PV模式來說，選擇Other PV (32-bit) 或Other PV (64-bit)。這個選擇僅在XenServer適用
   - 超級監督者。XenServer
   - 格式。VHD

模組就建立好了，您可以在其上建立instances

12.13. Adding Password Management to Your Templates

CloudStack 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 CloudStack, you can specify whether reset admin/root password feature should be enabled for this template.

The password management feature works always resets the account password on instance boot. The script does an HTTP call to the virtual router to retrieve the account password that should be set. As long as the virtual router is accessible the guest will have access to the account password that should be used. When the user requests a password reset the management server generates and sends a new password to the virtual router for the account. Thus an instance reboot is necessary to effect any password changes.

If the script is unable to contact the virtual router during instance boot it will not set the password but boot will continue normally.

12.13.1. Linux作業系統安裝

請依下列步驟開始安裝Linux作業系統安裝:

1. 下載cloud-set-guest-password腳本程式:

   - Linux: http://cloudstack.org/dl/cloud-set-guest-password
   - Windows: http://sourceforge.net/projects/cloudstack/files/Password%20Management%20Scripts/CloudInstanceManager.msi/download

2. 將檔案複製到/etc/init.d。

   某些特定的Linux distribution, 請將檔案複製到/etc/rc.d/init.d。

3. 修改腳本程式的執行權限, 請執行以下指令

   ```
   chmod +x /etc/init.d/cloud-set-guest-password
   ```

4. 依據您LInux的distribution, 請繼續以下適當的安裝步驟

   在Fedora、CentOS/RHEL或是Debian請執行:

   ```
   chkconfig --add cloud-set-guest-password
   ```

12.13.2. Windows作業系統安裝

下載安裝檔CloudInstanceManager.msi, 可以從Download page[3]下載, 在新建立的Windows虛擬機器執行安裝檔

12.14. 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.

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

[3] http://cloudstack.org/download.html

Working With Storage

13.1. 儲存裝置簡介

CloudStack定義兩種儲存裝置類型: 主要及次要, 主要可以存取iSCSI 或 NFS, 另外, 直接連結儲存裝置可能會用作主要儲存裝置。次要儲存裝置都使用NFS存取

在CloudStack沒有暫時的儲存裝置, 所有節點的容量都是永久的

13.2. 主要儲存裝置

這個段落會描述 CloudStack主要儲存裝置的概念和技術細節, 如果您需要更多有關透過 CloudStackUI 安裝及設定主要儲存裝置的資訊, 請參閱: Installation Guide

節 2.6, “About Primary Storage”

13.2.1. 主要儲存裝置的最佳練習

・主要儲存裝置的速度會影響訪客的效能。如果可以, 請選擇較小、較高轉速的硬碟

・請確保伺服器端是沒有任何資料的, 新增一個伺服器至 CloudStack 將會刪除所有存在的資料。

13.2.2. 執行時主要儲存裝置的行為

Root容量會在虛擬機器建立時自動產生。當虛擬機器刪除時, 容量也會刪除。資料容量可以新增及連結到VM上, 且不會隨VM刪除而消失

管理者需要監視主要儲存裝置的容量, 並在需要是加入額外的裝置, 詳見Advanced Installation Guide

藉由建立CloudStack 儲存裝置群來增加主要儲存裝置, 每個儲存裝置群都會連結到叢集

13.2.3. 主要儲存裝置的超級監督者支援

以下表格顯示儲存選項及欄位給不同的監督者

	VMware vSphere	Citrix XenServer	KVM	
Format for Disks, Templates, and Snapshots	VMDK	VHD	QCOW2	
iSCSI support	VMFS	Clustered LVM	Yes, via Shared Mountpoint	
Fiber Channel support	VMFS	Yes, via Existing SR	Yes, via Shared Mountpoint	
NFS support	Y	Y	Y	
Local storage support	Y	Y	Y	
Storage over-provisioning	NFS and iSCSI	NFS	NFS	

XenServer使用叢集LVM系統在iSCSI 及 Fiber Channel 容量儲存VM映像，但不支援監督者的over-provisioning。儲存伺服器可以支援 thin-provisioning。綜合以上，CloudStack 可以仍可以藉由執行thin-provisioned儲存容量來支援over-provisioning

KVM支援"Shared Mountpoint"儲存， shared mountpoint是一種檔案系統路徑，此路徑必須所有叢集主機皆相同，例如/mnt/primary1。shared mountpoint是假設像OCFS2的準叢集檔案系統。在此例子中，CloudStack不偏好掛載或卸載儲存裝置， CloudStack需要管理者確保儲存裝置是可用的

使用NFS儲存裝置，CloudStack管理overprovisioning，在此例子中，廣域設定欄位 storage.overprovisioning.factor控制 overprovisioning的程度，這與超級監督者的類型是無關的

本地儲存裝置是vSphere、XenServer和KVM主要儲存裝置的一個選擇，當本地硬碟選項啓用時，本地硬碟儲存裝置群就會自動建立，想要使用本地儲存裝置給 System Virtual Machines(像是虛擬路由器)，將廣域設定system.vm.use.local.storage設為true

CloudStack支援多主要儲存裝置群，例如，您可以提供2個NFS伺服器給主要儲存裝置；或是您可以一開始提供1個 iSCSI LUN，然後在第一個的容量快滿時加入第二個iSCSI LUN

13.2.4. Storage 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 CloudStack. They are matched against tags placed on service and disk offerings. CloudStack requires all tags on service and disk offerings to exist on the primary storage before it allocates root or data disks on the primary storage. 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 can be complex. To simplify the situation, use the same set of tags on the primary storage for all clusters in a pod. Even if different devices are used to present those tags, the set of exposed tags can be the same.

13.2.5. 主要儲存裝置的維護模式

主要儲存裝置有時會進入維護模式，比如說，替換故障的記憶體。維護模式會先停止新的使用者進入儲存裝置，然後會停止所有資料還存放在裝置上使用者。當所有使用者被停止，儲存裝置將進入維護模式或關機。當儲存裝置再度上線，您可以取消維護模式，CloudStack會將裝置上線並嘗試讓之前被停止的使用者繼續使用。

13.3. 設定次要儲存裝置

這個段落會描述CloudStack次要儲存裝置的概念和技術細節，如果您需要更多有關透過CloudStackUI安裝及設定次要儲存裝置的資訊，請參閱： Advanced Installation Guide

節 2.7, “About Secondary Storage”

13.4. 使用容量

容量提供訪客VM儲存空間，可做為root硬碟或額外的資料硬碟，CloudStack也支援為訪客VM新增容量

容量為特定的超級監督者類型建立，連結到使用一種類型(例如XenServer)訪客的容量將不能連到其他不同類型的訪客，例如： vSphere、KVM。這是因為不同超級監督者使用不同的硬碟映像格式

CloudStack 定義容量為儲存裝置的單元，可為root硬碟或資料硬碟。root硬碟的檔案系統有 "/"，通常作為開機裝置；資料硬碟提供額外的儲存空間，例如："/opt" 或 "D:"。每個訪客VM都有root硬碟，並且可以擁有資料硬碟。終端使用者可以掛載多個資料硬碟，使用者可以從管理者建立的硬碟服務選擇資料硬碟；此為建立私人模組的標準流程。容量為限定超級監督者的：兩種不同類型的容量無法互相使用

注意

在XenServer hypervisor versions 6.0或更高，CloudStack支援連結最多13個資料硬碟到VM上。其他類型的VM，限制為6個

13.4.1. 新增容量

您可以隨時新增資料硬碟到訪客VM，直到上限。CloudStack 的使用者及管理者耶可以新增，當您新增容量，它會放在CloudStack，但實際的儲存資源並沒有分配，直到您將容量歸屬。此最佳化允許CloudStack提供容量給最近的訪客

13.4.1.1. 使用本機端儲存的資料磁碟

您現在可以在本地儲存裝置(支援 XenServer、KVM及 VMware)新增資料volumes，它和VM instance位於同一個主機。這些本地資料volumes可以：連結到虛擬機器、不連結、重新連結和刪除。在前些版本的CloudStack，只有root硬碟能夠放到本地儲存裝置

本地儲存裝置對保存資料 volumes的計畫是很理想的，而且不需要HA。還有一些優點，像是減少硬碟I/O延遲和使用本地硬碟來減少成本

為了本地 volumes可以使用，這個功能需要在zone啓用

您可以建立資料硬碟給本地儲存裝置，當使用者建立新的VM時，他們可以選擇這個硬碟來使資料硬碟 volume可以放在本地儲存裝置

您不能遷移含有本地儲存裝置的VM或是volume本身到其他主機上。如果您想要這台主機進入維護模式，您必須先停止所有含有本地資料volume的VM

13.4.1.2. 要新增容量

1. 以使用者或管理者身分登入CloudStack UI
2. 在左邊的導覽視窗，選擇Storage
3. 於Select View中選擇Volumes
4. 選擇 Add Volume，並提供細節來新增容量

   - Name：容量的名稱
   - Availability Zone：儲存裝置的歸屬，必須鄰近使用容量的VM
   - Disk Offering：選擇儲存裝置的屬性

   新的容量會出現在表中，並顯示"Allocated"。容量資料會存在CloudStack中，但是尚未啓用
5. 繼續Attaching a Volume步驟來啓用

13.4.2. 上傳已存在的Volume到虛擬機器

已存在的資料現在可以被虛擬機器存取，這叫上傳a volume到VM。例如，上傳資料到本地資料系統並將資料連到VM。Root、主要管理者、使用者都可以上傳

上傳是使用HTTP，而上傳的volume會被放在zone的次要儲存裝置

如果已達容量限制，您就不能上船容量。預設限制設定在廣域設定欄位max.account.volumes，但管理者可以設定為不同的限制，詳見 Setting Usage Limits

要上傳容量:

1. (選擇性)新增MD5 hash (checksum)硬碟映像檔，上傳資料硬碟後，CloudStack會使用使用此數值來檢查是否有資料中斷
2. 以管理者或終端使用者登入CloudStack UI
3. 在左邊的導覽視窗，選擇Storage
4. 選擇Upload Volume
5. 提供以下:
   - Name and Description: 顯示在使用者介面的名稱及簡述
   - Availability Zone: 選擇您要安置容量的zone，在此zone的VM可以增加容量
   - Format: 選擇指定的硬碟映像格式

超級監督者	硬碟映像格式
XenServer	VHD
VMware	OVA
KVM	QCOW2

   - URL: CloudStack可以存取您的硬碟的安全 HTTP 或 HTTPS URL。檔案形式必須符合在Format選擇的數值，例如，格式為VHD，則URL必須像以下:

     http://yourFileServerIP/userdata/myDataDisk.vhd

   - MD5 checksum: (選擇性)使用您在 1建立的hash
6. 等到容量顯示上傳完成，選擇 Instances - Volumes，找到您在???指定的名稱，並確認狀態為 Uploaded

13.4.3. 連接容量

您可以連接容量到訪客VM來擴充儲存容量，當您新建一個容量、或是移動已存在的容量到其他VM、或是移動容量到另一個儲存裝置群，您會需要連接容量

1. 以使用者或管理者身分登入CloudStack UI
2. 在左邊的導覽視窗，選擇Storage
3. 於Select View中選擇Volumes
4. 4.在容量列表點選容量名稱，然後按下Attach Disk 

5. 在 Instance彈出視窗，選擇您想要連結容量的VM，您只會看到允許連結的instances。例如，使用者只會看到自己創的instances，但管理者有更多選擇

6. 當容量已被連結，點選Instances，到instance name，到 View Volumes，您應該會看到

13.4.4. 分離及移動容量

注意

此步驟不同於群間移動硬碟容量，詳見VM Storage Migration

容量可以分離訪客VM，及連結其他訪客。 CloudStack管理者及使用者都可以分離容量

如果兩個VM在不同叢集，且容量很大，會花很多時間

1. 以使用者或管理者身分登入CloudStack UI

2. 在左方導覽視，選擇 Storage，然後選擇Select View中的Volumes。如果您知道哪個容量連接到哪，您可以點選Instances，選擇 VM名稱，然後點選View Volumes

3. 點選您要分離的容量，然後按Detach Disk 

4. 執行以下步驟 節 13.4.3，“連接容量”來移動容量

13.4.5. 移動虛擬機器儲存裝置

支援XenServer、KVM及VMware

注意

此步驟不同於群間移動硬碟容量，詳見Detaching and Moving Volumes 節 13.4.4，“分離及移動容量”

您可以移動虛擬機器的root硬碟或是其他額外的資料硬碟到其他相同區域的儲存裝置群中

您可以使用移動儲存裝置的功能來達到一些管理者的目標，像是平衡儲存裝置群間的負載，及增加虛擬機器的可靠性，可藉由將儲存裝置從有問題的群組移除來達成

13.4.5.1. 移動資料硬碟容量到新的儲存裝置群

1. 以使用者或管理者身分登入CloudStack 使用者介面

2. 切斷VM與資料硬碟的連結，詳見Detaching and Moving Volumes 節 13.4.4，“分離及移動容量”（請跳過最後的“reattach”步驟，您在移動後才會使用到）

3. 在容量ID及任一儲存裝置ID呼叫 CloudStack API指令migrateVolume及pass

4. 監看VM狀態，移動時為Migrating，停止時為Ready

5. 連結容量到同一cluster的任一VM，做為新的儲存裝置伺服器，詳見 Attaching a Volume 節 13.4.3，“連接容量”

13.4.5.2. 移動VM Root容量到新的儲存裝置群

移動root硬碟容量時，VM必須停止，使用者不能存取該VM，移動後，VM才能重新啓動

1. 以使用者或管理者身分登入CloudStack 使用者介面
2. 切斷VM與資料硬碟的連結，詳見Detaching and Moving Volumes 節 13.4.4，“分離及移動容量”（請跳過最後的“reattach”步驟，您在移動後才會使用到）
3. 停止VM
4. 使用 CloudStack API指令migrateVirtualMachine，要移動的VM ID及目的地主機的ID及目的地儲存裝置群
5. 監看VM狀態，移動時為Migrating，停止時為Stopped
6. 重新啓動VM

13.4.6. 重新規劃容量

CloudStack提供重新規劃容量的功能，CloudStack藉由硬碟服務來控制大小。提供了CloudStack管理者多少空間釋出的彈性。相同儲存裝置tag的容量能被重新規劃，例如，如果您只想要提供10，50，和 100 GB，允許的規劃就不會超過這些限制，也就是您可以定義分別為10 GB、 50 GB及100 GB 的硬碟服務，使用者可以從10 GB 更新到 50 GB或是 50 GB 更新到 100 GB。如果您建立了自訂大小的硬碟服務，那麼您就可以定義新的硬碟容量

除此之外，使用resizeVolume API， 資料容量可以從固定硬碟服務移動到自訂硬碟服務。這個功能允許想要在特定容量需要收費的人將收費訂到這個規則

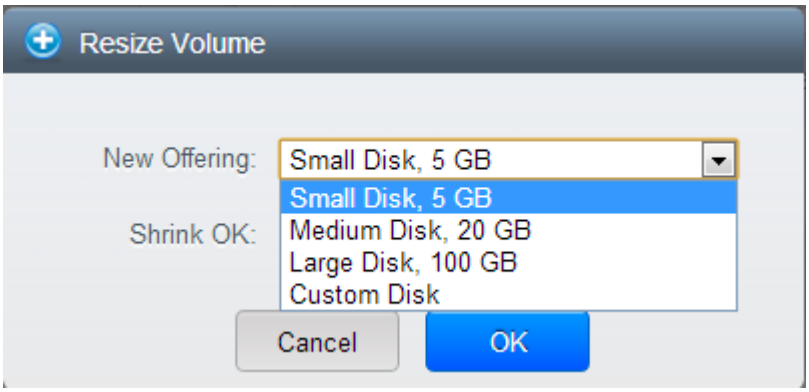
此功能支援KVM，XenServer，及 VMware主機，但縮小容量的功能並不支援VMware 主機

在您重新規劃之前，請先注意：

- 連結容量的VMs已停止
- 連結容量的資料硬碟已經移除
- 當容量縮小時，連結的硬碟也會被截短，並且會有資料遺失的風險。因此，請在縮小資料硬碟前，重新規劃任何分割或是檔案系統

要重新規劃容量：

1. 以使用者或管理者身分登入CloudStack UI
2. 在左邊的導覽視窗，選擇Storage
3. 於Select View中選擇Volumes
4. 在容量列表點選容量名稱，然後按Resize Volume 
5. 在 Resize Volume跳出視窗，選擇想要的儲存裝置特性



a. 如果您選擇Custom Disk，請指定自訂大小

b. 點選Shrink OK來確認您要縮小容量

此欄位避免不小心的失誤，以免資料遺失，您必須知道您在做甚麼

6. 按OK

13.4.7. 容量偵測及回收

刪除容量並不會刪除快取物件

當虛擬機器被刪除後，連結到虛擬機器的資料硬碟容量並不會刪除

使用回收可以永久移除容量，廣域組態變數expunge.delay及expunge.interval決定何時實體刪除會發生

- expunge.delay：決定容量新舊程度，單位為秒
- expunge.interval：決定多常執行回收檢查

管理者需要調整這些參數，根據您的數據保留政策

13.5. 使用快取物件

(支援以下超級監督者： XenServer，VMware vSphere，and KVM)

CloudStack支援硬碟容量的快取物件。快取物件為一時間點的虛擬機器硬碟擷取，記憶體及CPU狀態並不包含

容量，包含root及資料硬碟，可能需要使用快取物件，管理者會限制每個使用者能儲存快取物件的數量，使用者可以從快取物件建立新的容量，用來復原特定檔案；可以從快取物件建立模組，用來啓動復原的硬碟

使用者可以手動新增快取物件，或是建立自動遞迴的快取物件政策。使用者可以從快取物件建立硬碟容量，此容量可能會連結到虛擬機器上，如同其他硬碟容量。root硬碟及資料硬碟皆支援快取物件，但是CloudStack目前並不支援從復原的root硬碟開啓虛擬機器，由root硬碟快取物件復原的硬碟將視為一般資料硬碟，其中的資料可以將硬碟連結到虛擬機器上來存取

完整的快取物件是由主要儲存裝置複製到次要儲存裝置，並會一直儲存在裝置中，除非刪除或是被新的快取物件蓋過去

13.5.1. Snapshot Job 調節

當您要快取虛擬機器的圖案時，snapshot job會在和VM同一台主機上執行，或是最後執行的主機。如果在一台主機上有太多snapshots的工作，會導致這些工作佔用太多主機的資源

雲端的root管理者可以調節有多少snapshot能夠同時執行，利用廣域設定來設定 concurrent.snapshots.threshold.perhost。藉由此設定，管理者可以確定snapshot job不會超時，而超級監督者的主機不會有效能的問題

設定concurrent.snapshots.threshold.perhost 為一個在已知現有資源及VM執行數量的情況下，所猜的最佳值，如果一個主機有很多snapshot要求，則新的要求會排到等待主列

管理者也可以設定 job.expire.minute來規定工作等待的最大值，如果超時了，要求會失敗並回覆錯誤訊息

13.5.2. Automatic Snapshot Creation and Retention

(支援以下超級監督者： XenServer, VMware vSphere, and KVM)

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 interval. One snapshot policy can be set up per disk volume. For example, a user can set up a daily snapshot at 02:30.

With each snapshot schedule, users can also specify the number of scheduled snapshots to be retained. Older snapshots that exceed the retention limit are automatically deleted. This user-defined limit must be equal to or lower than the global limit set by the CloudStack administrator. See 節 14.3, “廣域設定限制”. The limit applies only to those snapshots that are taken as part of an automatic recurring snapshot policy. Additional manual snapshots can be created and retained.

13.5.3. 增加的快取物件及輩分

快取物件在硬碟的主要儲存裝置建立，快取之後，會立即備份到次要儲存裝置，並移除原本的物件以達到主要儲存裝置的最佳使用

CloudStack會為一些超級監督者做增加備份，當增加備份支援時，每N個備份為一個完全的備份黨

	VMware vSphere	Citrix XenServer	KVM
支援增加備份	N	Y	N

13.5.4. 容量狀態

當您藉由重複快取物件政策使用快取物件動作時，如果容量因前一快取物件已快取而成非啓用狀態，則此快取會跳過。如果沒有連結到虛擬機器或是連結到沒在使用的虛擬機器，容量會是非啓用狀態。CloudStack會確保在容量變成非啓用狀態前，會至少有一次快取

手動快取時，快取物件會不管容量是否有啓用，而直接建立

13.5.5. Snapshot Restore

There are two paths to restoring snapshots. Users can create a volume from the snapshot. The volume can then be mounted to a VM and files recovered as needed. Alternatively, 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 root disk.

Working with Usage

Usage Server 是一個選擇性，獨立安裝的CloudStack部分。它提供彙整使用紀錄，讓你可以在CloudStack上建立廣告整合。Usage Server會從事件紀錄擷取資料，然後創立使用記錄總結，你可以用istUsageRecords API call來存取

使用紀錄會告訴你來源總數，像是VM執行時間或是客戶消耗的模組儲存空間

Usage Server 至少每天執行一次，也可以透過設定，每天執行多次

14.1. Configuring the Usage Server

To configure the usage server:

1. Be sure the Usage Server has been installed. This requires extra steps beyond just installing the CloudStack software. See Installing the Usage Server (Optional) in the Advanced Installation Guide.
2. 以administrator身分登入CloudStack UI
3. Click Global Settings.
4. In Search, type usage. Find the configuration parameter that controls the behavior you want to set. See the table below for a description of the available parameters.
5. In Actions, click the Edit icon.
6. Type the desired value and click the Save icon.
7. Restart the Management Server (as usual with any global configuration change) and also the Usage Server:

```
# service cloudstack-management restart
# service cloudstack-usage restart
```

The following table shows the global configuration settings that control the behavior of the Usage Server.

欄位名稱	敘述
enable.usage.server	Whether the Usage Server is active.

usage.aggregation.timezone	Time zone of usage records. Set this if the usage records and daily job execution are in different time zones. For example, with the following settings, the usage job will run at PST 00:15 and generate usage records for the 24 hours from 00:00:00 GMT to 23:59:59 GMT:
	`usage.stats.job.exec.time = 00:15`
	`usage.execution.timezone = PST`
	`usage.aggregation.timezone = GMT`
	Valid values for the time zone are specified in 附錄 A，時區

欄位名稱	敘述
	Default: GMT
usage.execution.timezone	The time zone of usage.stats.job.exec.time. Valid values for the time zone are specified in 附錄 A, 時區 Default: The time zone of the management server.
usage.sanity.check.interval	The number of days between sanity checks. Set this in order to periodically search for records with erroneous data before issuing customer invoices. For example, this checks for VM usage records created after the VM was destroyed, and similar checks for templates, volumes, and so on. It also checks for usage times longer than the aggregation range. If any issue is found, the alert ALERT_TYPE_USAGE_SANITY_RESULT = 21 is sent.
usage.stats.job.aggregation.range	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. CloudStack 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 it is assumed you would like to process records for October 6, from midnight to midnight. CloudStack assumes this "midnight to midnight" is relative to the usage.execution.timezone. Default: 1440
usage.stats.job.exec.time	The time when the Usage Server processing will start. It is specified in 24-hour format (HH:MM) 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". If usage.stats.job.aggregation.range is also set, and its value is not 1440, then its value will be added to

欄位名稱	敘述
	usage.stats.job.exec.time to get the time to run the Usage Server job again. This is repeated until 24 hours have elapsed, and the next day's processing begins again at usage.stats.job.exec.time. Default: 00:15.

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:

- enable.usage.server = true
- usage.execution.timezone = America/New_York
- 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.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.

注意

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. That data will be included in the next day's run.

14.2. 設定使用限制

CloudStack提供多個管理者控制點給隱藏資源使用率，有些限制是廣域設定參數，其他應用在ROOT網域及無視每個帳戶的基礎

累積極限可能會在每個網域基礎上設定，例如，您可以限制網域，並且所有子網域只能建立100VM

這個章節涵蓋以下章節:

14.3. 廣域設定限制

一個區域內，訪客虛擬網路預設上有24位元的CIDR，此限制訪客虛擬機器僅能執行254個instance。可依需要調整，但是必須在任何instance加到區域前調整。例如，10.1.1.0/22會提供~1000個位址

以下表格列出廣域組態的限制:

欄位名稱	定義
max.account.public.ips	可以被一個帳戶擁有的公開IP數量

欄位名稱	定義
max.account.snapshots	一個帳戶中的最多快取物件數量
max.account.templates	一個帳戶中的最多模組數量
max.account.user.vms	一個帳戶中的最多虛擬機器 instance數量
max.account.volumes	一個帳戶中的最多硬碟容量數量
max.template.iso.size	下載的模組或ISO的最大大小，單位為GB
max.volume.size.gb	容量最大的大小，單位為GB
network.throttling.rate	預設的資料傳輸速率，單位為MBit/s(支援 XenServer)
snapshot.max.hourly	容量每小時重複快取的最大數量，如果快達限制，較早的快取物件會被刪除。此限制不適用手動快取。如果設為0，每小時重複快取將無法排程
snapshot.max.daily	容量每天重複快取的最大數量，如果快達限制，較早的快取物件會被刪除。此限制不適用手動快取。如果設為0，每天重複快取將無法排程
snapshot.max.weekly	容量每周重複快取的最大數量，如果快達限制，較早的快取物件會被刪除。此限制不適用手動快取。如果設為0，每周重複快取將無法排程
snapshot.max.monthly	容量每月重複快取的最大數量，如果快達限制，較早的快取物件會被刪除。此限制不適用手動快取。如果設為0，每月重複快取將無法排程

使用CloudStack使用者介面的廣域組態視窗來修改廣域組態參數欄位。詳見Setting Global Configuration Parameters

14.4. 預設帳戶資源限制

您可以使用帳戶來限制資源，預設限制由廣域設定欄位決定。開頭為max.account是重要的參數，例如：max.account.snapshots

設定每個資源限制來超過預設限制

1. 登入 CloudStack UI
2. 在左邊的導覽視窗，選擇Accounts
3. 選擇您想要修改的帳戶，會顯示現在的限制，-1代表在這區沒有限制
4. 按下Edit 

14.5. Domain限制

CloudStack 允許針對domain設定限制，然而於每一個domain中使用者仍然會受到所屬account的限制。例如：不超過domain所能使的資源範圍，domain限制了以下所屬的accouts，當然也包含的子domain底的所有accounts。所有設定於root domain層級的限制，將會套用到所有的domains及accounts。

設定domain限制

1. 登入 CloudStack UI
2. 在左邊的導覽視窗，選擇Domains

3. 選擇您想要修改的domain, 會顯示現在的限制, -1代表在這區沒有限制

4. 按下Edit 

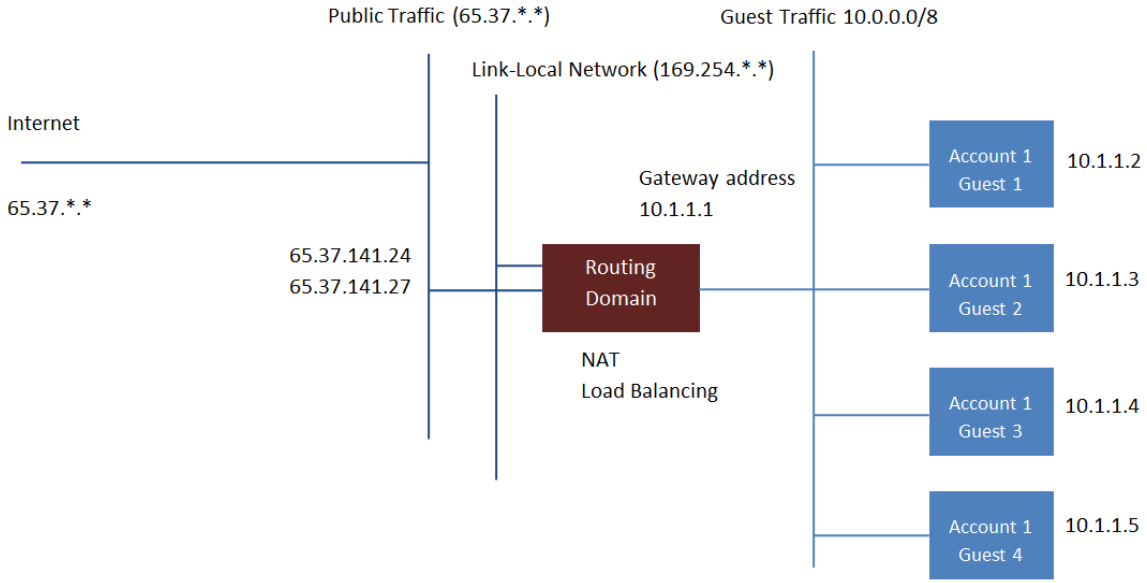
管理網路及流量

在CloudStack，訪客VM可以使用安全分享基礎架構來與其他VM溝通，及使用者能感知到私人的訪客LAN。 CloudStack虛擬路由器使提供訪客網路功能的重要元件

15.1. 訪客流量

網路僅能在一個區域的虛擬機器間搭載訪客流量，在不同區域將無法使用IP互相通信，它們只能透過公開IP來互相通信

此圖描述一個典型的訪客流量設定:



Guest Traffic Setup

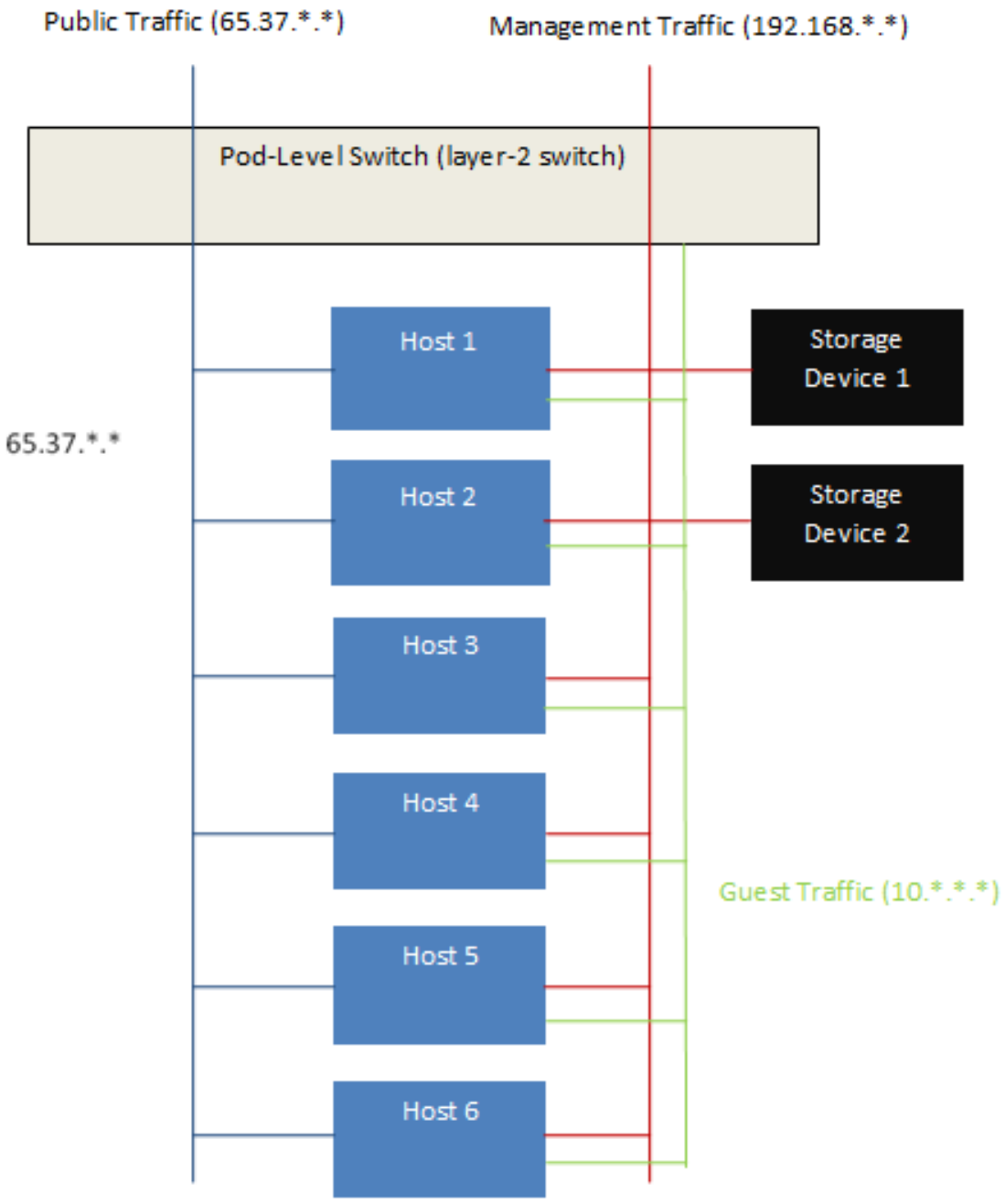
管理伺服器會自動建立虛擬路由器。虛擬路由器是一種在主機上執行的特殊虛擬機器，每個虛擬路由器有三個網路介面。eth0用作訪客流量的閘道，IP位址為10.1.1.1；eth1用作系統設定虛擬路由器的介面；eth2指定為公開流量的IP位址

虛擬路由器提供DHCP，並自動從IP範圍指定IP給每個訪客虛擬機器。使用者可以手動重設訪客虛擬機器來使用其他IP位址

虛擬路由器內的Source NAT會自動設定為轉送所有訪客虛擬機器的對外流量

15.2. Networking in a Pod

The figure below illustrates network setup within a single pod. The hosts are connected to a pod-level switch. At a minimum, the hosts 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.



Network Setup within a Single Pod – Logical View

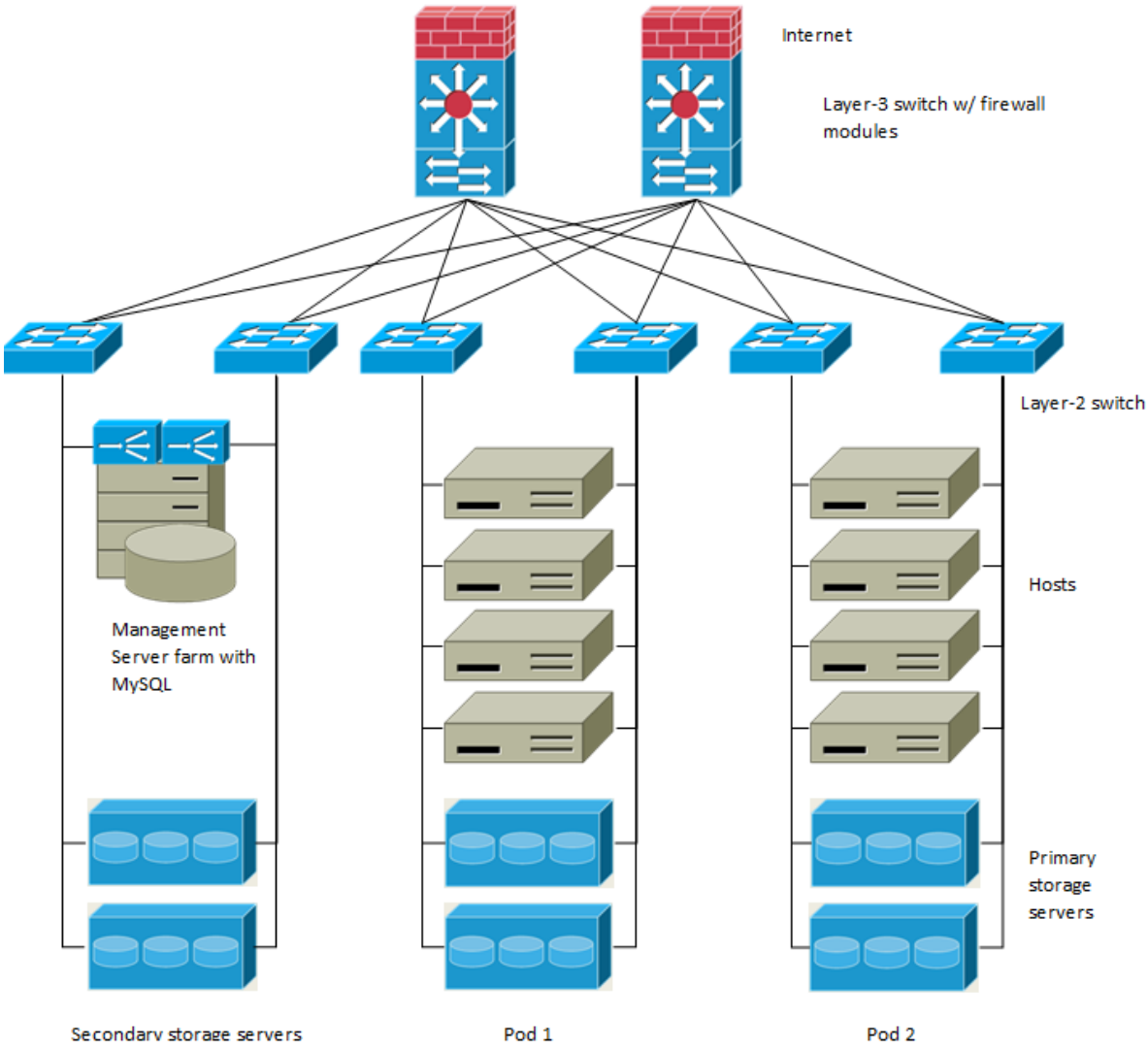
Servers are connected as follows:

- Storage devices are connected to only the network that carries management traffic.
- Hosts are connected to networks for both management traffic and public traffic.
- Hosts are also connected to one or more networks carrying guest traffic.

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.

15.3. Networking in a Zone

The following figure illustrates the network setup within a single zone.



A firewall for management traffic operates in the NAT mode. The 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 zone has its own set of public IP addresses. Public IP addresses from different zones do not overlap.

15.4. 基礎區域的實體網路設定

在基礎網路中，設定設定實體網路很直接，您只需要設定一個訪客網路搭載訪客虛擬機器產生的流量即可。當您第一次將區域加到CloudStack，請在Add Zone視窗建立訪客網路

15.5. Advanced Zone Physical Network Configuration

Within a zone that uses advanced networking, you need to tell the Management Server how the physical network is set up to carry different kinds of traffic in isolation.

15.5.1. 於Advanced Zone下設定Guest Traffic

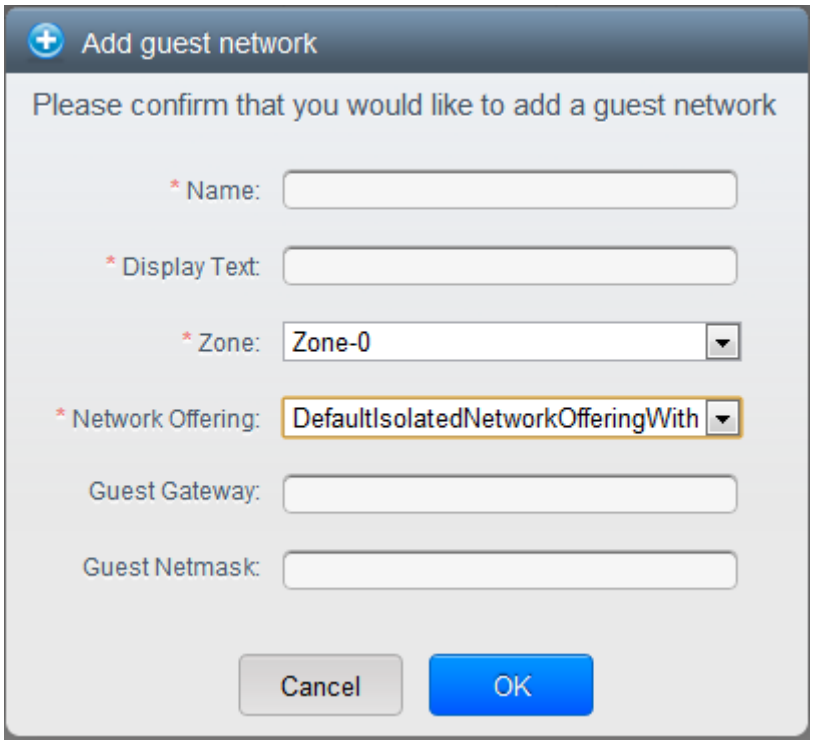
以下步驟將假設您已經登入CloudStack的UI並設定基礎的Guest網段:

1. 於左邊的Navigation按鈕中， 點選Infrastructure按鈕; 並在右方的Zone圖示中選擇More, 接著點選您要加入網段的zone。

2. 選擇Network標籤

3. 選擇Add guest network

   將出現Add guest network的視窗



4. 提供以下資訊:

   - Name. 此網路名稱, 本欄外名稱將會呈現於使用者頁面。
   - Display Text: 此網路的敘述, 本欄外敘述將會呈現於使用者頁面。
   - Zone: 本網路所欲設定之zone
   - Network offering: 如果administrator已經設定了許多network offering, 請為此網路選擇一個您希望的network offering。
   - Guest Gateway: 此網路的gateway
   - Guest Netmask: 此網路的子網路遮罩。

5. 按OK

15.5.2. Configure Public Traffic in an Advanced Zone

In a zone that uses advanced networking, you need to configure at least one range of IP addresses for Internet traffic.

15.6. Using Multiple Guest Networks

In zones that use advanced networking, additional networks for guest traffic may be added at any time after the initial installation. You can also customize the domain name associated with the network by specifying a DNS suffix for each network.

A VM's networks are defined at VM creation time. A VM cannot add or remove networks after it has been created, although the user can go into the guest and remove the IP address from the NIC on a particular network.

Each VM has just one default network. The virtual router's DHCP reply will set the guest's default gateway as that for the default network. Multiple non-default networks may be added to a guest in addition to the single, required default network. The administrator can control which networks are available as the default network.

Additional networks can either be available to all accounts or be assigned to a specific account. Networks that are available to all accounts are zone-wide. Any user with access to the zone can create a VM with access to that network. These zone-wide networks provide little or no isolation between guests.Networks that are assigned to a specific account provide strong isolation.

15.6.1. 新增

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 按Add guest network。提供以下資訊:
   - Name: 使用者可見的網路名稱
   - Display Text: 使用者可見的網路敘述
   - Zone. 欲新增網路的zone; 每一個zone都具有廣播的範圍，因此每一個zone都需具有不同的IP範圍的Guest網路，administrator必須要為每一個zone設定獨立的IP範圍。
   - Network offering: 如果管理者已經設定多個網路產品，選擇一個你想要套用到這個網路的產品
   - Guest Gateway: 客戶要用的閘道
   - Guest Netmask: 客戶要使用的子網路遮罩
4. 按Create

15.6.2. 改變訪客網路的服務

使用者及管理者可以改變連結到已知的訪客網路服務

- 以管理者或終端使用者登入CloudStack 使用者介面
- 如果您要將使用 CloudStack虛擬路由器的網路服務，改用到像網路服務提供者這樣的外部裝置，您必須停止所有網路上的VM See 節 10.6, “Stopping and Starting VMs”.
- 在左邊的導覽視窗，選擇Network
- 選擇你想要修改的網路
- 在 Details標籤，按下Edit 

- 在Network Offering中，選擇新的網路服務，然後按Apply
- 出現提示詢問您是否要保留已存在的CIDR。這是告訴您，如果您改變了網路服務，CIDR也會受影響，選擇No來完成變更
- 等待更新完畢，請不要中途重新啓動VM
- 重新啓動停止的VM

15.7. Security Groups

15.7.1. 關於安全群組

安全群組提供隔開VM及流量的方法。安全群組是根據規則過濾輸入輸出流量的一組VM，這些規則根據來源IP來過濾。安全群組在基本網路的區域中特別有用，因為僅有一個訪客網路對所有訪客VM。在進階區域中，安全群組僅支援KVM超級監督者

注意

在使用進階網路的區域，您可以定義多訪客網路來隔離VM及流量

每個 CloudStack帳戶帶有預設安全群組，拒絕所有輸入流量及允許所有輸出流量。此預設安全群組可以修改，使所有新的VM繼承以些其他想要的規則

任何CloudStack使用者都可以建立任一數量的額外安全群組。執行新的VM時，此VM會使用預設安全群組，除非有使用者定義的安全群組。一個VM可以為多個安全群組的成員，一旦指定了一個群組，將會終生在群組中。您無法將執行中的VM移動到其他安全群組中

您可以藉由刪除或增加輸入及輸出規則來修改安全群組。此變更將套用到所有群組中的VM，不管是執行中還是停止

如果沒有指定輸入規則，將沒有任何流量允許輸入，除了輸出規則允許的流量

15.7.2. 新增

使用者或管理員可以定義一個新的security group

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select中，選擇Security Groups
4. 選擇Add Security Grou
5. 提供名稱及敘述
6. 按OK

   新的security group會出現在Security Groups Details標籤

7. 為使security group有用，新增Ingress and Egress Rule到Security Group

15.7.3. (僅限KVM)進階Zone的Security Groups

CloudStack 提供使用security groups來隔離進階zone中分享且zone-wide網路的訪客互相來往的功能，而KVM為超級監督者。使用security groups在進階zone可以比用在多個VLANs能有更大的設定選擇

限制

以下不支援此功能:

- 在相同的VLAN有兩個IP範圍，及security group啓用的分享網路中有不同的閘道或遮罩
- 在相同的VLAN有兩個IP範圍，及 account-specific的分享網路中有不同的閘道或遮罩
- security group啓用的分享網路中有多個VLAN範圍
- account-specific的分享網路中有多個VLAN範圍

Security groups必須要在zone中啓用

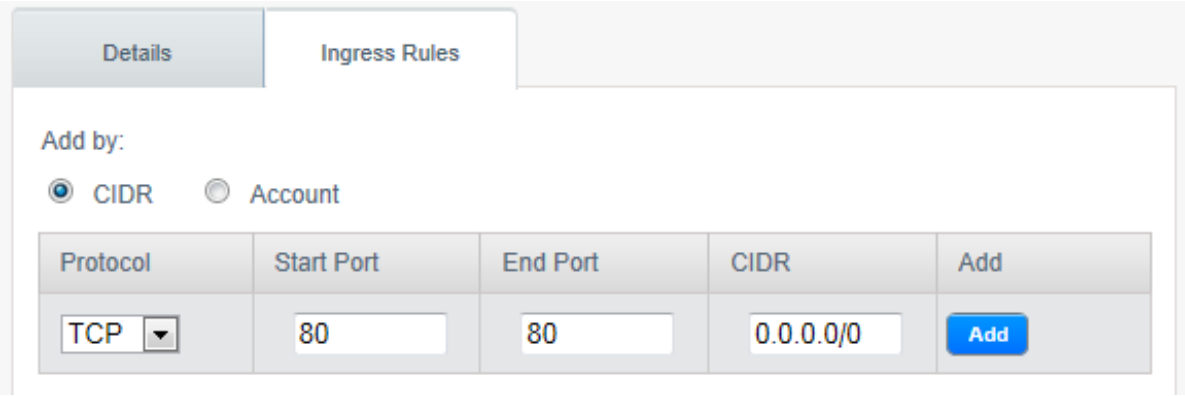
15.7.4. 啓用Security Groups

為了讓security groups能夠正常運作，security groups的功能必須要在zone中啓用。藉由選擇包含 network offering的網路，管理者可以在建立新的zone時啓用功能。此步驟在Advanced Installation Guide的Basic Zone Configuration部分有詳加敘述。注意，管理者只能在新的zone才能啓用，已存在的zone不能啓用

15.7.5. 在安全群組增加輸入及輸出規則

1. 以管理者或終端使用者登入CloudStack 使用者介面
2. 在左邊的導覽視窗，選擇Network
3. 在Select中，選擇 Security Groups，然後選擇您想要的安全群組
4. 想要增加輸入規則，選擇Ingress Rules標籤，然後填入以下欄位指定哪一種流量在此安全層級能夠送進VM。如果沒有Ingress規則被指定，所有流量就都不允許送進，除了有被egress規則定義的流量
   - Add by CIDR/Account: 流量來源是否被IP 位址 (CIDR)定義，或CloudStack 帳戶 (Account)中已有的安全群組。如果您想要允許其他安全群組VM的輸入流量，請選擇Account
   - Protocol: 來源送流量到安全群組的網路協定。TCP和UDP協定常被用作資料交換和終端使用者傳輸，ICMP常被用作傳送錯誤訊息或網路監視資料
   - Start Port (TCP，UDP限定): 一個範圍內，輸出流量目標的正在等候埠，如果你要開啓一個埠，在所有欄位內使用同一數字
   - ICMP Type，ICMP Code: (ICMP限定)資料型態及被接受的錯誤碼
   - CIDR: (只能被CIDR新增)為了送流量到特定區域裡的IP位址，進入CIDR或是CIDR的comma-separated list。CIDR是輸入流量的基礎IP位址，比如說， 192.168.0.0/22，為了允許所有CIDR，設定 0.0.0.0/0
   - Account，Security Group: (僅能被Account新增)輸入CloudStack帳號及張祐中安全群組名稱，來允許從其他安全群組來的流量，在步驟7輸入相同的名稱來允許安全群組的VM互相傳輸

   以下範例為允許從任何地方回來的HTTP存取



5. 想要增加輸出規則，選擇Egress Rules標籤，然後填入以下欄位指定哪一種流量在此安全層級能夠送出VM。如果沒有輸出規則被指定，所有流量就都允許送出；如果有指定，只有以下類型可以被送出：規則規定的流量；DNS及DHCP伺服器的貯列；輸入規則允許的流量

   - Add by CIDR/Account：流量來源是否被IP 位址 (CIDR)定義，或CloudStack 帳戶 (Account)中已有的安全群組。如果您想要允許其他安全群組VM的輸入流量，請選擇Account
   - Protocol：VM送出流量的網路協定。TCP和UDP協定常被用作資料交換和終端使用者傳輸，ICMP協定常被用作傳送錯誤訊息或網路監視資料
   - Start Port (TCP, UDP限定)：一個範圍內，輸出流量目標的正在等候埠，如果你要開啓一個埠，在所有區內使用同一數字
   - ICMP Type, ICMP Code：(ICMP限定)資料型態及送出的錯誤碼
   - CIDR：(只能被CIDR新增)為了送流量到特定區域裡的IP位址，進入CIDR或是CIDR的comma-separated list。CIDR是目的地的基礎IP位址，比如說， 192.168.0.0/22，為了允許所有CIDR，設定 0.0.0.0/0
   - Account, Security Group：(僅能被Account增加)輸入CloudStack 帳戶及安全群組名稱來允許流量送到另一個安全群組；輸入安全群組名稱來允許其包含的VM可以互通

6. 按Add

15.8. External Firewalls and Load Balancers

CloudStack is capable of replacing its Virtual Router with an external Juniper SRX device and an optional external NetScaler or F5 load balancer for gateway and load balancing services. In this case, the VMs use the SRX as their gateway.

15.8.1. About Using a NetScaler Load Balancer

Citrix NetScaler is supported as an external network element for load balancing in zones that use advanced networking (also called advanced zones). Set up an external load balancer when you want to provide load balancing through means other than CloudStack's provided virtual router.

The NetScaler can be set up in direct (outside the firewall) mode. It must be added before any load balancing rules are deployed on guest VMs in the zone.

The functional behavior of the NetScaler with CloudStack is the same as described in the CloudStack documentation for using an F5 external load balancer. The only exception is

that the F5 supports routing domains, and NetScaler does not. NetScaler can not yet be used as a firewall.

The Citrix NetScaler comes in three varieties. The following table summarizes how these variants are treated in CloudStack.

NetScaler ADC Type	Description of Capabilities	CloudStack Supported Features
MPX	Physical appliance. Capable of deep packet inspection. Can act as application firewall and load balancer	In advanced zones, load balancer functionality fully supported without limitation. In basic zones, static NAT, elastic IP (EIP), and elastic load balancing (ELB) are also provided
VPX	Virtual appliance. Can run as VM on XenServer, ESXi, and Hyper-V hypervisors. Same functionality as MPX	Supported only on ESXi. Same functional support as for MPX. CloudStack will treat VPX and MPX as the same device type
SDX	Physical appliance. Can create multiple fully isolated VPX instances on a single appliance to support multi-tenant usage	CloudStack will dynamically provision, configure, and manage the lifecycle of VPX instances on the SDX. Provisioned instances are added into CloudStack automatically — no manual configuration by the administrator is required. Once a VPX instance is added into CloudStack, it is treated the same as a VPX on an ESXi host.

15.8.2. 在RHEL伺服器設定SNMP Community String

SNMP Community String 類似使用者ID或密碼，用作存取網路裝置，像是路由器。此string隨著所有SNMP要求傳送，如果 community string 正確，裝置會回應要求資訊；如果不正確，裝置會丟棄要求及不回應

NetScaler裝置使用SNMP來與VM通信，您必須安裝SNMP及設定SNMP Community string 來建立安全的通訊

1. 確保您在RedHat安裝SNMP，如果沒有，請依照以下指令:

```
yum install net-snmp-utils
```

2. 編輯/etc/snmp/snmpd.conf 來允許SNMP從NetScaler 裝置採樣

   a. 對照community名稱到一個security 名稱(本地及mynetwork，取決於要求從哪來):

注意

您在編輯表格時，請使用高強度密碼，不要用公開

```
#          sec.name    source          community
com2sec     local       localhost       public
com2sec    mynetwork    0.0.0.0         public
```

注意

設定0.0.0.0允許所有IP poll NetScaler server

b. 對照 security 名稱到群組名稱:

```
#      group.name    sec.model  sec.name
group    MyRWGroup      v1          local
group    MyRWGroup      v2c         local
group    MyROGroup      v1        mynetwork
group    MyROGroup      v2c       mynetwork
```

c. 建立view讓群組有許可:

```
incl/excl subtree mask view all included .1
```

d. 允許兩個不同群組的存取給您建立的view

```
# context     sec.model      sec.level     prefix     read     write     notif
  access      MyROGroup ""  any noauth     exact      all      none      none
  access      MyRWGroup ""  any noauth     exact      all      all       all
```

3. 解除封鎖iptables的SNMP

```
iptables -A INPUT -p udp --dport 161 -j ACCEPT
```

4. 啓動SNMP服務:

```
service snmpd start
```

5. 確定SNMP服務有隨開機自動啓動

```
chkconfig snmpd on
```

15.8.3. 外部防火牆及負載平衡器的初始設定

在為新帳戶建立第一個VM時，CloudStack規劃外部防火牆及負載平衡器給VM，以下物件會建立在防火牆上：

- 新的邏輯介面連結到帳戶私人VLAN，介面IP為帳戶私人子網域(e.g. 10.1.1.1)的第一個IP
- source NAT rule，轉送所有私人VLAN的輸出流量到公開網路，使用帳戶公開IP為來源位址
- 測量輸出流量的位元組數量的防火牆過濾計數器

以下物件會新增到負載平衡器：

- 新的VLAN，符合帳戶提供的區域VLAN
- VLAN自己的IP，為帳戶私人子網路(e.g. 10.1.1.2)的第二個IP

15.8.4. 持續設定外部防火牆及

額外的使用者動作(例如設定port forward)會導致更多防火牆及load balancer的程式執行。使用者可能會要求額外的公開IP及IP的順向流量來指定VM，藉由啓用static NAT，指定IP到VM及指定一組協定及埠範圍開啓，我們可以達到這個要求，當static NAT rule建立時，CloudStack會用以下物件來載入zone的外部防火牆：

- 對照公開IP位址和私人IP位址的 static NAT rule
- 在一組協定及埠範圍中允許流量的security policy
- 測量輸出到公開IP的流量位元組數量的防火牆過濾計數器

輸入輸出位元組的數量，會在通過source NAT，static NAT及 load balancing rules被測量並存在外部元件中，這些資料會被收集及儲存在CloudStack資料庫

15.8.5. 設定 AutoScale

AutoScaling allows you to scale your back-end services or application VMs up or down seamlessly and automatically according to the conditions you define. With AutoScaling enabled, you can ensure that the number of VMs you are using seamlessly scale up when demand increases, and automatically decreases when demand subsides. Using AutoScaling, you can automatically shut down instances you don't need, or launch new instances, depending on demand.

NetScaler AutoScaling設計為無縫執行或根據使用者定義情況終止VM，觸發變動的情況會依據像監控CPU使用率等簡單的規則，或是監控伺服器的反應及CPU使用率等複雜的規則而有所不同，例如，您想要想要在CPU使用率在15分鐘超過80%就增加VM，或是CPU使用率在30分鐘低於20%就移除VM

CloudStack uses the NetScaler load balancer to monitor all aspects of a system's health and work in unison with CloudStack to initiate scale-up or scale-down actions.

注意

AutoScale is supported on NetScaler Release 10 Build 73.e and beyond.

事前準備

在您設定 AutoScale 規則之前，請先考慮:

- 確保必要的模組已經準備好，當VM使用模組部署時，應用程式需要出現並執行

注意

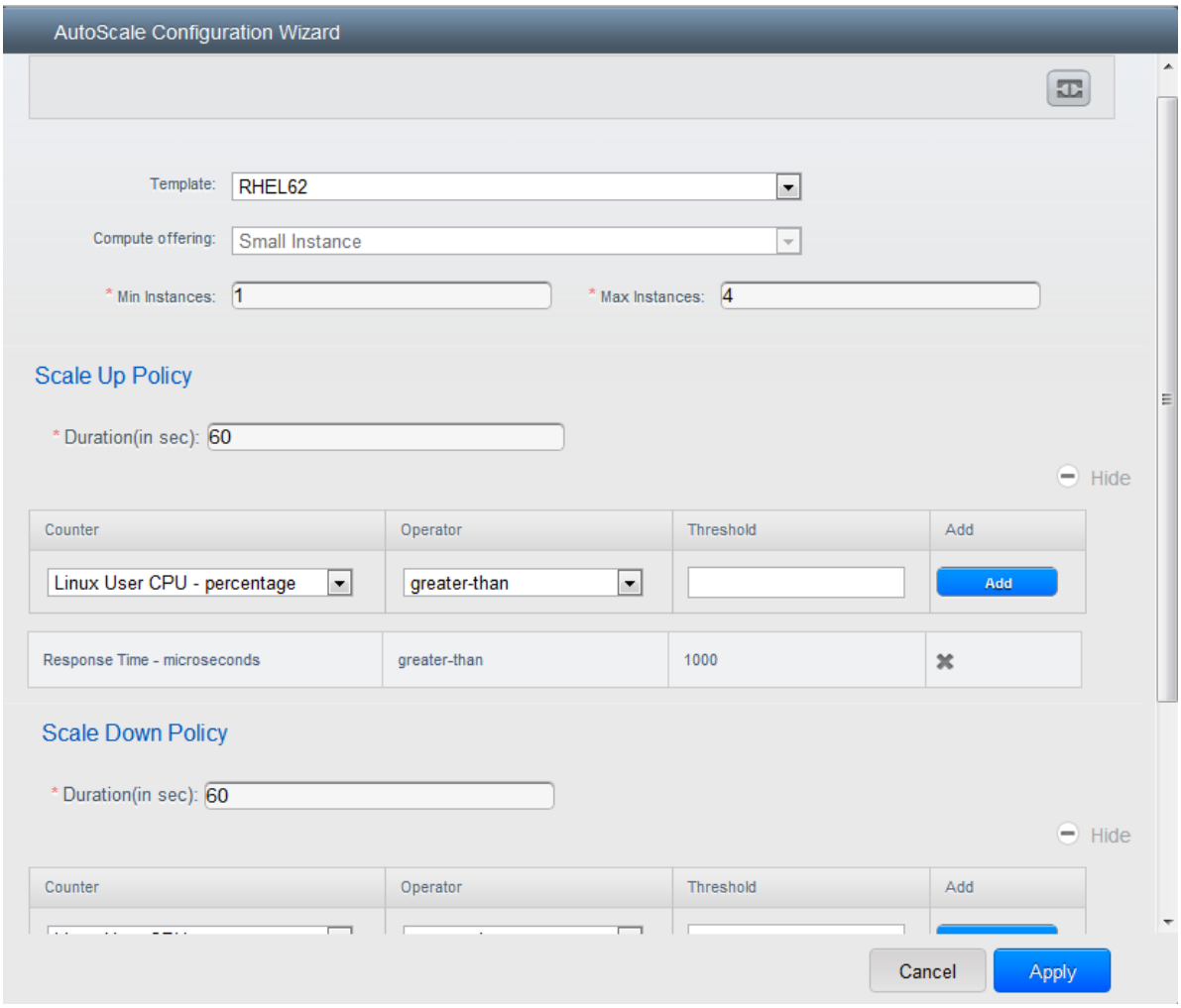
如果應用程式並未執行，NetScaler裝置會認為VM是無效的，並繼續無條件的配置VM，直到資源耗盡

- 部署您準備的模組，確定應用程式在開機時有出現，並可以處理流量。觀察部署模組需要的時間，用來考慮設定AutoScale時是否正常
- AutoScale功能支援SNMP計數器，可使用為定義狀況，想要監視 SNMP-based 計數器，請確保SNMP agent已安裝在模組中，及 使用標準SNMP管理器，使 SNMP運作單元可以在設定後的SNMP 群組及通訊埠正常運作，例如，詳見節 15.8.2, “在RHEL伺服器設定SNMP Community String ”來設定RHEL機器上的SNMP
- 確定endpointe.url 欄位有出現在Global Setting，並設定為Management Server API URL。例如，http://10.102.102.22:8080/client/api。對於多節點管理伺服器，使用虛擬IP，在管理伺服器叢集的負載平衡器中設定。另外，確定NetScaler 裝置可以存取此IP，藉此提供AutoScale支援

  如果您更新endpointe.url，請停用系統的負載平衡規則的AutoScale功能，然後再啓用，使變更生效，更多資訊，詳見Updating an AutoScale Configuration
- 如果API Key 及 Secret Key為AutoScale 使用者重新產生，請確定使用者參與的負載平衡器的AutoScale功能，有先停用後再啓用，以使變更生效
- 在進階區域中，確定在設定AutoScale的負載平衡規則前，至少有一個VM顯示，此確定網路是在執行狀態

系統設定

具體說明以下:



- Template: 模組包含作業系統映像及應用程式。用來提供新 instance 擴增動作，當VM部署後，VM可以開始由負載平衡器接收流量，例如，如果VM部署為網頁服務，網頁伺服器應會開始執行，資料庫開始連結，然後繼續下去

- Compute offering: 一組先定義的虛擬硬體，包含CPU速度、CPU數量及記憶體大小，讓使用者可以在建立新的虛擬機器時選擇，配置VM instance為擴增動作的一部份時，選擇一個計算服務

- Min Instance: The minimum number of active VM instances that is assigned to a load balancing rule. The active VM instances are the application instances that are up and serving the traffic, and are being load balanced. This parameter ensures that a load balancing rule has at least the configured number of active VM instances are available to serve the traffic.

注意

If an application, such as SAP, running on a VM instance is down for some reason, the VM is then not counted as part of Min Instance parameter, and the AutoScale feature initiates a scaleup action if the number of active VM instances is below the configured value. Similarly, when an application instance comes up from its earlier down state, this application instance is counted as part of the active instance count and the AutoScale process initiates a scaledown action when the active instance count breaches the Max instance value.

- Max Instance: Maximum number of active VM instances that should be assigned to a load balancing rule. This parameter defines the upper limit of active VM instances that can be assigned to a load balancing rule.

  Specifying a large value for the maximum instance parameter might result in provisioning large number of VM instances, which in turn leads to a single load balancing rule exhausting the VM instances limit specified at the account or domain level.

注意

If an application, such as SAP, running on a VM instance is down for some reason, the VM is not counted as part of Max Instance parameter. So there may be scenarios where the number of VMs provisioned for a scaleup action might be more than the configured Max Instance value. Once the application instances in the VMs are up from an earlier down state, the AutoScale feature starts aligning to the configured Max Instance value.

Specify the following scale-up and scale-down policies:

- Duration: The duration, in seconds, for which the conditions you specify must be true to trigger a scaleup action. The conditions defined should hold true for the entire duration you specify for an AutoScale action to be invoked.
- Counter: The performance counters expose the state of the monitored instances. By default, CloudStack offers four performance counters: Three SNMP counters and one NetScaler counter. The SNMP counters are Linux User CPU, Linux System CPU, and Linux CPU Idle. The NetScaler counter is ResponseTime. The root administrator can add additional counters into CloudStack by using the CloudStack API.
- Operator: The following five relational operators are supported in AutoScale feature: Greater than, Less than, Less than or equal to, Greater than or equal to, and Equal to.
- Threshold: Threshold value to be used for the counter. Once the counter defined above breaches the threshold value, the AutoScale feature initiates a scaleup or scaledown action.

・Add: Click Add to add the condition.

Additionally, if you want to configure the advanced settings, click Show advanced settings, and specify the following:

・Polling interval: Frequency in which the conditions, combination of counter, operator and threshold, are to be evaluated before taking a scale up or down action. The default polling interval is 30 seconds.

・Quiet Time: This is the cool down period after an AutoScale action is initiated. The time includes the time taken to complete provisioning a VM instance from its template and the time taken by an application to be ready to serve traffic. This quiet time allows the fleet to come up to a stable state before any action can take place. The default is 300 seconds.

・Destroy VM Grace Period: The duration in seconds, after a scaledown action is initiated, to wait before the VM is destroyed as part of scaledown action. This is to ensure graceful close of any pending sessions or transactions being served by the VM marked for destroy. The default is 120 seconds.

・Security Groups: Security groups provide a way to isolate traffic to the VM instances. A security group is a group of VMs that filter their incoming and outgoing traffic according to a set of rules, called ingress and egress rules. These rules filter network traffic according to the IP address that is attempting to communicate with the VM.

・Disk Offerings: A predefined set of disk size for primary data storage.

・SNMP Community: The SNMP community string to be used by the NetScaler device to query the configured counter value from the provisioned VM instances. Default is public.

・SNMP Port: The port number on which the SNMP agent that run on the provisioned VMs is listening. Default port is 161.

・User: This is the user that the NetScaler device use to invoke scaleup and scaledown API calls to the cloud. If no option is specified, the user who configures AutoScaling is applied. Specify another user name to override.

・Apply: Click Apply to create the AutoScale configuration.

Disabling and Enabling an AutoScale Configuration

If you want to perform any maintenance operation on the AutoScale VM instances, disable the AutoScale configuration. When the AutoScale configuration is disabled, no scaleup or scaledown action is performed. You can use this downtime for the maintenance activities.

To disable the AutoScale configuration, click the Disable AutoScale  button.

The button toggles between enable and disable, depending on whether AutoScale is currently enabled or not. After the maintenance operations are done, you can enable the AutoScale configuration back. To enable, open the AutoScale configuration page again, then click the Enable AutoScale  button.

Updating an AutoScale Configuration

You can update the various parameters and add or delete the conditions in a scaleup or scaledown rule. Before you update an AutoScale configuration, ensure that you disable the AutoScale load balancer rule by clicking the Disable AutoScale button.

After you modify the required AutoScale parameters, click Apply. To apply the new AutoScale policies, open the AutoScale configuration page again, then click the Enable AutoScale button.

Runtime Considerations

- An administrator should not assign a VM to a load balancing rule which is configured for AutoScale.
- Before a VM provisioning is completed if NetScaler is shutdown or restarted, the provisioned VM cannot be a part of the load balancing rule though the intent was to assign it to a load balancing rule. To workaround, rename the AutoScale provisioned VMs based on the rule name or ID so at any point of time the VMs can be reconciled to its load balancing rule.
- Making API calls outside the context of AutoScale, such as destroyVM, on an autoscaled VM leaves the load balancing configuration in an inconsistent state. Though VM is destroyed from the load balancer rule, NetScaler continues to show the VM as a service assigned to a rule.

15.9. Load Balancer Rules

CloudStack的使用者或管理者應創造一個對一至多個VM的負載平衡規則來平衡在公開IP的傳輸。使用者創立規則，指定一組演算法，然後套用規則到一組VM上

注意

如果你在使用像NetScaler，這種會改變其他正在用CloudStack虛擬路由器使用者的網路服務的外部負載平衡裝置，你必須在虛擬路由器上，為每一個存在的規則建立防火牆，好讓它們能正確執行

15.9.1. 增加 Load Balancer Rule

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 選擇你想要流量負載平衡的網路
4. 按 View IP Addresses.
5. 選擇你想要新增規則的IP，按下Configuration標籤
6. 在 Load Balancing 點，按 View All

   在 Basic中，你也可以不用獲得或選擇IP來建立規則。 CloudStack 在你建立規則時，就已經指定一個IP了，並列在IP Addresses葉面

選擇網路名稱，然後按下Add Load Balancer標籤， 7繼續

7. 填寫以下：

   - Name: load balancer rule的名稱
   - Public Port: 應被平衡流量的埠
   - Private Port: VM接收流量的不
   - Algorithm 選擇你想要CloudStack使用的演算法，CloudStack支援很多已知的演算法，如果你不熟悉這些選擇，你可以在網際網路上找到詳細資料
   - Stickiness.（選擇性）點選Configure並選擇stickiness policy的演算法，請參Sticky Session Policies for Load Balancer Rules章節
   - AutoScale：點選Configure並如節 15.8.5, “設定 AutoScale ”說明完成AutoScale的設定

8. 按Add VMs，然後選擇兩個以上要分流量的VMs，然後按Apply

   新的規則會出現在表單中，你可以重複以上步驟來新增多個規則

15.9.2. Sticky Session Policies for Load Balancer Rules

Sticky sessions are used in Web-based applications to ensure continued availability of information across the multiple requests in a user's session. For example, if a shopper is filling a cart, you need to remember what has been purchased so far. The concept of "stickiness" is also referred to as persistence or maintaining state.

Any load balancer rule defined in CloudStack can have a stickiness policy. The policy consists of a name, stickiness method, and parameters. The parameters are name-value pairs or flags, which are defined by the load balancer vendor. The stickiness method could be load balancer-generated cookie, application-generated cookie, or source-based. In the source-based method, the source IP address is used to identify the user and locate the user’s stored data. In the other methods, cookies are used. The cookie generated by the load balancer or application is included in request and response URLs to create persistence. The cookie name can be specified by the administrator or automatically generated. A variety of options are provided to control the exact behavior of cookies, such as how they are generated and whether they are cached.

For the most up to date list of available stickiness methods, see the CloudStack UI or call listNetworks and check the SupportedStickinessMethods capability.

15.10. 訪客IP範圍

訪客網路流量IP範圍是在每個帳戶上設定的值，允許使用者設定自己的網路為可在訪客網路及客戶間使用VPN連結

15.11. 獲得新的IP

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 選擇你想要套用的網路

4. 按

5. 按下Acquire New IP，然後按下Yes

   由於IP位址是有限的資源，因此你需要立即得確認。不久後IP位址應該就會顯示Allocated。現在你可以在 port forwarding,或 static NAT rules下使用你的IP

15.12. 釋出IP位址

當所有套用在IP上的規則都被移除時，您將可以釋出IP。而IP仍屬於VPC，且能被訪客網路再次使用

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 選擇你想要套用的網路
4. 按 View IP Addresses.
5. 選擇你想要釋出的IP
6. 按下Release IP 

15.13. Static NAT

static NAT rule 配對一個公衆IP到VM上的私人IP，並允許網路連結。因為公開IP位址永遠維持相同，因此稱為。這個章節教你如何對特定IP開啓或關閉 static NAT

15.13.1. 開啓/關閉Static NAT

如果port forwarding rules已經開啓，你將不能開啓static NAT

如果客戶的VM是多個網路的一部份，static NAT rules只有定義在預設網路時才能正常運作

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 選擇你想要套用的網路
4. 按 View IP Addresses.
5. 選擇你想要套用的IP
6. 按下Static NAT  button.

   按鈕會依照static NAT 的狀態來顯示開啓或關閉

7. 如果你正在使用static NAT，會跳出選擇目標VM的對話框，然後按Apply

15.14. IP轉送及防火牆

By default, all incoming traffic to the public IP address is rejected. All outgoing traffic from the guests is also blocked by default.

To allow outgoing traffic, follow the procedure in 節 15.14.1, “建立Advanced區內的”.

To allow incoming traffic, users may set up firewall rules and/or port forwarding rules. For example, you can use a firewall rule to open a range of ports on the public IP address, such as 33 through 44. Then use port forwarding rules to direct traffic from individual ports within that range to specific ports on user VMs. For example, one port forwarding rule could route incoming traffic on the public IP's port 33 to port 100 on one user VM's private IP. For more information, see 節 15.14.2, “Firewall Rules” and 節 15.14.3, “Port Forwarding”.

15.14.1. 建立Advanced區內的

注意

Egress firewall rules 僅支援虛擬路由器

Egress traffic 是從私人網路到公用網路, 例如Internet。Egress traffic在預設上是關閉的, 也就是訪客網路無法輸出流量到Internet。然而, 您可以在 Advanced 新增Egress traffic rule來控制Egress traffic, 而套用此規則的流量將允許通過, 其他則保持原樣。當所有防火牆規則被移除時, 將會回到預設值

考慮套用Egress firewall rules 的情形:

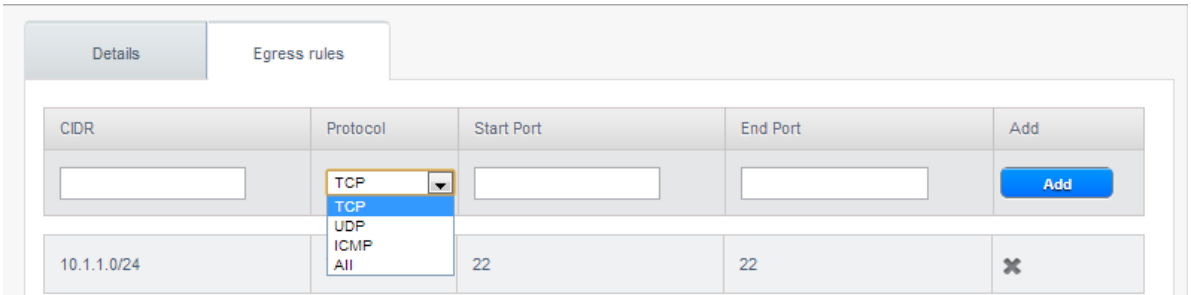
・允許屬於訪客網路的特定CIDR的輸出流量

・允許終端協定為 TCP,UDP,ICMP, 或 ALL的輸出流量

・允許終端協定及埠的範圍屬於TCP, UDP 或 ICMP形式的輸出流量

設定Egress firewall rules:

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗, 選擇Network
3. 在Select中, 選擇您想要的Guest networks
4. 選擇 Egress rules標籤並填入以下區域來指定哪一種型態的流量是被允許送出訪客網路的VM



・CIDR: (只能被CIDR新增)為了送流量到特定區域裡的IP位址, 進入CIDR或是CIDR的comma-separated list。CIDR是目的地的基礎IP位址, 比如說, 192.168.0.0/22, 為了允許所有CIDR, 設定 0.0.0.0/0

・Protocol: VM送流量到層級的網路協定。TCP和UDP協定常被用作資料交換和終端使用者傳輸, ICMP協定常被用作傳送錯誤訊息或網路監視資料

- Start Port (TCP, UDP限定): 一個範圍內, 輸出流量目標的正在等候埠, 如果你要開啓一個埠, 在所有區內使用同一數字
- ICMP Type, ICMP Code: (ICMP限定)資料型態及送出的錯誤馬

5. 按Add

15.14.2. Firewall Rules

所有公開IP的輸入流量預設上是被防火牆隔絕的, 您可以定訂防火牆規則來開啓防火牆的埠。您可以選擇性的指定一至多個CIDR來過濾來源IP。當你想要只允許特定IP的輸入請求時, 是很有用的

您不行用防火牆規則來開啓埠給彈性IP。當彈性IP被使用時, 外部存取將會被security group所控制, 詳見

在一個具有advanced zone的環境下, 你可以藉由virtual router新增egress firewall rules, 更多資訊請參閱: 節 15.14.1, “建立Advanced區內的”

防火牆規則可以藉由Management Server UI中的 Firewall標籤建立。 CloudStack 後, 標籤並不是預設顯示的。 CloudStack 管理員必須要設定在總體系統設定中的參數 firewall.rule.ui.enabled為True才會顯示

建立防火牆規則:

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗, 選擇Network
3. 選擇你想要套用的網路
4. 按 View IP Addresses.
5. 選擇你想要套用的IP
6. 選擇Configuration標籤, 然後填入以下數值
   - Source CIDR(選擇性)為了在特定位址區域中允許流量自IP位址, 進入CIDR或CIDR的comma-separated list, 比如說, 192.168.0.0/22, 為了允許所有CIDR
   - Protocol: 開放埠(一至多個)之間使用的通訊協定
   - Start Port and End Port, 您想要在防火牆上開啓的埠(一至多個)的數量, 如果你要開啓一個埠, 在所有區內使用同一數字
   - ICMP Type and ICMP Code, 僅在協定已經設定給ICMP後使用。提供ICMP協定需要的形式和程式碼來填入標頭。如果您不清楚的話, 可以參閱ICMP文件
7. 按Add

15.14.3. Port Forwarding

Port forward 服務是一組定義方針的port forwarding rules。Port forward 服務套用在一至多個客戶VM。客戶VM會根據方針將本地網路存取做管理, 您可以指定一至多個CIDR來過濾來源IP, 當您想只允許特定IP的請求通過時, 是很有用的。

客戶VM可以在任意數目的port forward服務中。Port forward 服務也可以被定義, 但沒有任何成員。如果客戶的VM是多個網路的一部分, port forward rule 只定義在預設網路時才能正常運作

您不行用port forwarding 來開啓埠給彈性IP。當彈性IP被使用時，外部存取將會被security group所控制，詳見security group

設定port forwarding

1. 以管理者或終端使用者登入CloudStack UI
2. 如果您還沒達到此，請在CloudStack的一個zone中增加公衆IP範圍，詳見安裝指南中的Adding a Zone and Pod
3. 增加一至多個VM instances到CloudStack
4. 在左邊的導覽視窗，選擇Network
5. 選擇VM正在運作的客戶網路
6. 選擇一個存在的IP或是取得一個新的IP，詳見節 15.11，“獲得新的IP”
7. 選擇Configuration標籤
8. 在 Port Forwarding節點，按 View All
9. 填寫以下:
   - Public Port:公開傳輸的埠會定址在前一步驟獲得的IP上
   - Private Port: instance正在聆聽公開流量的不
   - Protocol: 兩個埠之間使用的通訊協定
10. 按Add

15.15. IP Load Balancing

使用者可能會想把多個訪客連結到同一個公用IP，CloudStack 以以下策略實現TCP層級的附載平衡

- Round-robin
- Least connection
- Source IP

這很類似port forwarding，但是目的地可能是多個IP位址

15.16. DNS 及 DHCP

虛擬路由器提供DNS及DHCP服務，它會代理DNS詢問DNS伺服器，此DNS伺服器在Availability Zone設定

15.17. VPN

CloudStack帳戶擁有者可以建立虛擬私人網路(VPN)來存取虛擬機器，如果訪客網路從提供Remote Access VPN服務的network offering建立，虛擬路由器(建於System VM)將被用來提供服務。CloudStack提供 L2TP-over-IPsec-based remote access VPN服務給訪客虛擬網路。由於每個網路有自己的虛擬路由器，VPNs不會跨網域分享。源自Windows、Mac OS X 和iOS的VPN客戶可以連上訪客網路。帳戶擁有者可以建立及管理自己的VPN使用者，CloudStack不會在此用途使用自己的帳戶資料庫，但會使用分割表。VPN使用者資料庫會在帳戶擁有者的所有VPN做跨領域分享，所有VPN使用者可以存取帳戶擁有者的所有VPNs

注意

確定VPN沒有流量，也就是VPN建立的路線只能給訪客網路

- Road Warrior / Remote Access：使用者想要從家中或辦公室到雲端私人網路能夠安全的連線，因此IP位址通常為動態的，並且不能在VPN伺服器先設定
- Site to Site：在此例子，兩個私人子網路藉由安全VPN通道連到公開網路，雲端使用者的子網路(例如，辦公室的網路)藉由閘道連線到雲端的網路，閘道的位址必須先在VPN伺服器上設定。注意，雖然L2TP-over-IPsec可以用來設定 Site-to-Site VPNs，但這不是這個功能的主要目的。更多資訊，詳見節 15.17.4，“設定 Site-to-Site VPN連線”

15.17.1. 設定VPN

為雲端設定VPN

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Global Settings
3. 設定以下全域設定參數
   - remote.access.vpn.client.ip.range — The range of IP addresses to be allocated to remote access VPN clients. The first IP in the range is used by the VPN server.
   - remote.access.vpn.psk.length，IPSec key的長度
   - remote.access.vpn.user.limit，每個帳戶最多的VPN使用者

想要開啓VPN給特定網路

1. 以使用者或管理者登入
2. 在左邊的導覽視窗，選擇Network
3. 選擇你想要套用的網路
4. 按 View IP Addresses.
5. 選擇其中一個顯示出來的IP位址
6. 按Enable VPN

   IPsec key會顯示在彈跳視窗

15.17.2. 在Windows使用VPN

在不同的Wondows版本有不同的VPN使用步驟，一般來說，使用者必須編輯VPN性質，必確定預設路由器不是VPN，以下步驟為Windows Vista的Windows L2TP客戶端，指令應與其他版本相似

1. 登入 CloudStack使用者介面，點選source NAT IP，VPN標籤會顯示 IPsec preshared key。記下這個金鑰與IP，使用者介面也會列出一至多個使用者及他們的密碼，選擇其中一個使用者或新增使用者及密碼

2. 在Windows box, 到Control Panel, 然後選擇Network and Sharing center, 點選Setup a connection network
3. 在下一個對話框, 選擇No, create a new connection
4. 在下一個對話框, 選擇Use my Internet Connection (VPN)
5. 在下一個對話框, 輸入步驟 1記下的source NAT IP, 並給予連結名稱, 先勾選Don't connect
6. 在下一個對話框, 輸入在步驟1選擇的使用者名稱及密碼
7. 按Create
8. 回到Control Panel並點選Network Connections來看新的連結, 此連結應還未啓用
9. 右鍵點選新連結, 並點選Properties。在Properties對話框, 選擇 Networking標籤
10. 在Type of VPN, 選擇L2TP IPsec VPN, 然後點選IPsec settings。選擇Use preshared key, 輸入從步驟1記下的preshared key
11. 此連結已可以啓動, 回到Control Panel -> Network Connections, 然後雙點擊建立的連結
12. 輸入從步驟1記下的使用者名稱及密碼

15.17.3. Using VPN with Mac OS X

First, be sure you've configured the VPN settings in your CloudStack install. This section is only concerned with connecting via Mac OS X to your VPN.

Note, these instructions were written on Mac OS X 10.7.5. They may differ slightly in older or newer releases of Mac OS X.

1. On your Mac, open System Preferences and click Network.
2. Make sure Send all traffic over VPN connection is not checked.
3. If your preferences are locked, you'll need to click the lock in the bottom left-hand corner to make any changes and provide your administrator credentials.
4. You will need to create a new network entry. Click the plus icon on the bottom left-hand side and you'll see a dialog that says "Select the interface and enter a name for the new service." Select VPN from the Interface drop-down menu, and "L2TP over IPSec" for the VPN Type. Enter whatever you like within the "Service Name" field.
5. You'll now have a new network interface with the name of whatever you put in the "Service Name" field. For the purposes of this example, we'll assume you've named it "CloudStack." Click on that interface and provide the IP address of the interface for your VPN under the Server Address field, and the user name for your VPN under Account Name.
6. Click Authentication Settings, and add the user's password under User Authentication and enter the pre-shared IPSec key in the Shared Secret field under Machine Authentication. Click OK.
7. You may also want to click the "Show VPN status in menu bar" but that's entirely optional.
8. Now click "Connect" and you will be connected to the CloudStack VPN.

15.17.4. 設定 Site-to-Site VPN連線

Site-to-Site VPN幫助您在企業資料庫及雲端間建立一個安全的連結。藉由建立VPN連結到企業資料庫帳戶的虛擬路由器，可以允許使用者存取訪客VM。有了這個功能，我們就不需要再建立VPN到獨立VM的連結了

支援遠端資料庫的端點為:

・Cisco ISR 版本IOS 12.4或之後。

・Juniper J-Series routers韌體JunOS 9.5或之後的版本

注意

除了以上特定的Cisco及Juniper裝置，其他任何Cisco或是Juniper應該都能在相容的作業系統上建立VPN連結

執行以下步驟來建立Site-to-Site VPN連結

1. 建立Virtual Private Cloud (VPC)

   請參閱: 節 15.19, “設定虛擬私人雲端”

2. 建立VPN Customer Gateway.

3. 創建一個VPN閘道給VPC

4. 建立VPN連結給VPC; VPN閘道給客戶VPN閘道

注意

當 Site-to-Site VPN連結從連線變成斷線，CloudStack UI會出現提示，反之亦然。如果為失敗或判定中則不會有提示

15.17.4.1. 建立及更新VPN客戶閘道

注意

VPN客戶閘道僅能一時連上VPN閘道

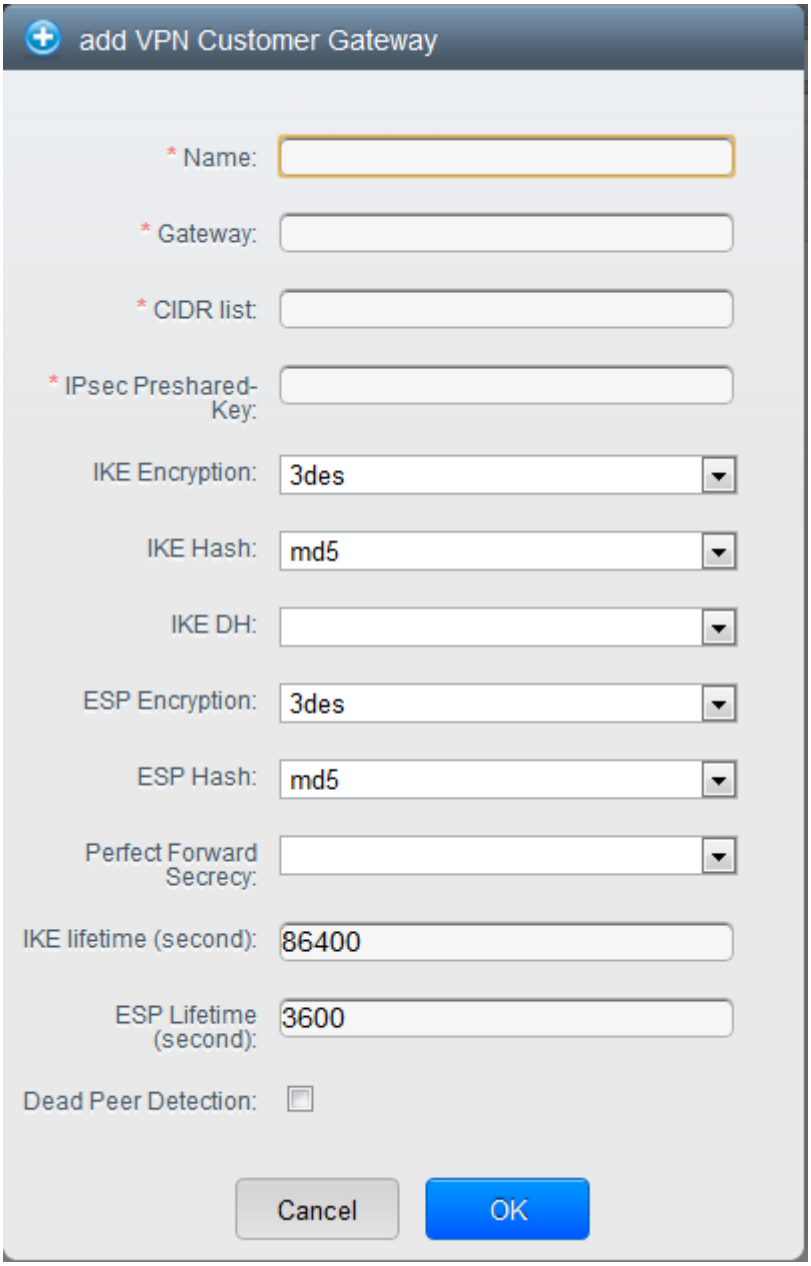
增加VPN客戶閘道:

1. 以管理者或終端使用者登入CloudStack UI

2. 在左邊的導覽視窗，選擇Network

3. 在Select視窗選擇VPC Customer Gateway

4. 按Add site-to-site VPN



提供以下資訊:

- Name: 您建立的VPN客戶閘道的名稱
- Gateway: 遠端閘道的IP位址
- CIDR list: 訪客 CIDR列表, 輸入CIDR或CIDR的comma-separated list, 確保訪客 CIDR列表沒有與VPC CIDR或其他訪客CIDR重疊, CIDR必須是RFC1918-compliant
- IPsec Preshared Key: Preshared keying是VPN終端分享祕密金鑰的方法, 此金鑰用於認證客戶閘道及VPC VPN閘道

注意

IKE peers(VPN終端)藉由運算及送出Preshared key包含keyed hash資料來互相認證，如果收到相同的hash，則表示分享相同的秘密

- IKE Encryption： Internet Key Exchange (IKE) 政策為phase-1，支援的加密演算法為AES128，AES192，AES256，及 3DES。認證藉由 Preshared Keys完成

注意

phase-1是 IKE過程的第一相位。在此交涉的相位，兩個VPN端點同意此方法來提供安全IP流量。 藉由確認遠端閘道有符合的 Preshared Key，phase-1互相認證兩個VPN閘道

- IKE Hash：給phase-1的IKE hash，支援演算法為SHA1 及 MD5
- IKE DH：公開密碼協定，允許兩方在不安全通訊通道建立分享的祕密，1536-bit Diffie-Hellman使用為IKE工作金鑰，支援選項為 None，Group-5 (1536-bit) and Group-2 (1024-bit)
- ESP Encryption：Encapsulating Security Payload (ESP)演算法為 phase-2，支援加密演算法為 AES128，AES192，AES256,及 3DES

注意

phase-2是在 IKE過程的第二相位，用意為交涉IPSec security associations (SA) 來建立IPSec通道。從 phase-1交換的Diffie-Hellman key萃取出新的keying material，來提供工作金鑰保護VPN資料流

- IKE Hash：給phase-2的Encapsulating Security Payload (ESP) hash，支援演算法為SHA1 及 MD5
- Perfect Forward Secrecy： Perfect Forward Secrecy (or PFS) 是確保工作金鑰不會被超長的公開及私人金鑰連累。此特性強迫Diffie-Hellman key交換。提供更長生命時間的keying material，提升加密攻擊的持久性。可用選項為None，Group-5 (1536-bit) and Group-2 (1024-bit)。DH groups越大或是交換時間越久，安全性越好

注意

When PFS is turned on, for every negotiation of a new phase-2 SA the two gateways must generate a new set of phase-1 keys. This adds an extra layer of protection that PFS adds, which ensures if the phase-2 SA's have expired, the keys used for new phase-2 SA's have not been generated from the current phase-1 keying material.

- IKE Lifetime (seconds): The phase-1 lifetime of the security association in seconds. Default is 86400 seconds (1 day). Whenever the time expires, a new phase-1 exchange is performed.
- ESP Lifetime (seconds): The phase-2 lifetime of the security association in seconds. Default is 3600 seconds (1 hour). Whenever the value is exceeded, a re-key is initiated to provide a new IPsec encryption and authentication session keys.
- Dead Peer Detection: A method to detect an unavailable Internet Key Exchange (IKE) peer. Select this option if you want the virtual router to query the liveliness of its IKE peer at regular intervals. It's recommended to have the same configuration of DPD on both side of VPN connection.

5. 按OK

Updating and Removing a VPN Customer Gateway

You can update a customer gateway either with no VPN connection, or related VPN connection is in error state.

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗, 選擇Network
3. 在Select視窗選擇VPC Customer Gateway
4. Select the VPN customer gateway you want to work with.
5. To modify the required parameters, click the Edit VPN Customer Gateway button 
6. To remove the VPN customer gateway, click the Delete VPN Customer Gateway button 
7. 按OK

15.17.4.2. 創建一個VPN閘道給VPN

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗, 選擇Network
3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁

4. 對想要配置VM的VPC按下"Configure"

   VPC 頁面會顯示所有你創建的層級

5. 按下"Settings"圖示

   會顯示出以下選項

   - IP Addresses
   - Gateways
   - Site-to-Site VPN
   - Network ACLs

6. 選擇"Site-to-Site VPN"

   如果你是第一次創建VPN閘道，請選擇"Site-to-Site VPN"來引導你新創VPN閘道

7. 在確認對話框中，按"Yes"來確定

   經過一小段時間，VPN閘道就創建好了。你將會被提示瀏覽剛創建的VPN閘道中的細節，按"Yes"來確認

   以下細節在VPN閘道頁面展示

   - IP Address
   - Account
   - Domain

15.17.4.3. 建立 VPN Connection

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select視窗選擇VPC

   所有為帳戶創建的VPC會表列在本頁

4. 對想要配置VM的VPC按下"Configure"

   VPC 頁面會顯示所有你創建的層級

5. 按下"Settings"圖示

   會顯示出以下選項

   - IP Addresses
   - Gateways
   - Site-to-Site VPN
   - Network ASLs

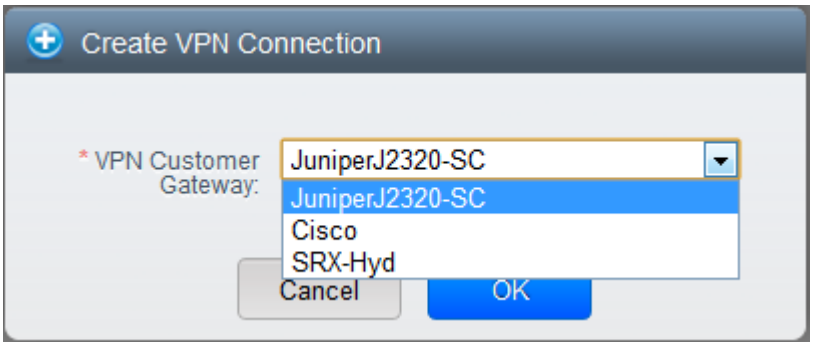
6. 選擇"Site-to-Site VPN"

會顯示Site-to-Site VPN頁面

7. 從 Select View下拉式選單，確定以選擇VPN Connection

8. 按下Create VPN Connection

   會顯示創建的VPN Connection對話框



9. 選擇希望的客戶閘道，按OK

   過不久，會顯示VPN Connection

   會顯示以下VPN connection的資訊

   - IP Address
   - Gateway
   - State
   - IPSec Preshared Key
   - IKE Policy
   - ESP Policy

15.17.4.4. 重新啓動和移除VPN Connection

1. 以管理者或終端使用者登入CloudStack UI

2. 在左邊的導覽視窗，選擇Network

3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁

4. 對想要配置VM的VPC按下"Configure"

   VPC 頁面會顯示所有你創建的層級

5. 按下"Settings"圖示

   會顯示出以下選項

   - IP Addresses
   - Gateways

- Site-to-Site VPN
- Network ASLs

6. 選擇"Site-to-Site VPN"

   會顯示Site-to-Site VPN頁面

7. 從 Select View下拉式選單，確定已選擇 VPN Connection

   會顯示所有你建立的VPN connections

8. 選擇你想要套用的VPN connection

   會顯示Details標籤

9. 想移除VPN connection，按下 Delete VPN connection button 

   想要重新啓動VPN connection，按下Details標籤內的 Reset VPN connection 

15.18. 關於 Inter-VLAN Routing

Inter-VLAN Routing是在網路流量及VLANs間建立路線的功能。此功能允許您設定Virtual Private Clouds (VPC)，一個您雲端的獨立部分，使它能夠控制多tier的應用。架設在不同VLAN的這些tier就能夠互相溝通。您可以提供VLAN給tiers，以及VMs可以架設在不同的tier上，例如Web、 Application或 Database。這些VLANs是連接到一個促進VM溝通的虛擬路由器上，您可以藉由VLAN將VM分段為不同網路，因而能夠執行多tier的應用，這種分割邏輯上是為了更高的安全性及更低的廣播性，但維持同樣的實體連結

此特色支援了XenServer以及VMware的hypervisors。

主要優點為:

- 管理者可以部署一組VLAN，及允許使用者在這些VLAN部署VM，訪客VLAN是隨機分配到帳戶，所有特定層級的VM會坐落於份配到帳戶的訪客VLAN

  注意

  非配給帳戶的VLAN不能再多帳戶間分享

- 管理者允許使用者建立他們自己的VPC，及安裝應用程式，在此範本，屬於帳戶的VM部署在分配到的VLAN上
- 管理者及使用者都可以建立多VPC，訪客網路的網路卡在第一台VM部署到層級後，插進VPC虛擬路由器
- 管理者可以建立以下閘道來送出或收到VM的流量:
  - VPN Gateway: 更多資訊，詳見節 15.17.4.2, “創建一個VPN閘道給VPN”
  - Public Gateway: VPC的公開閘道，在VPC的虛擬路由器建立時加入，公開閘道無法給終端使用者看到，您不允許列出它或是建立任何固定路徑

- Private Gateway: 更多資訊，詳見 節 15.19.5, “在VPC新增Private Gateway”.

- 管理者及使用者都可以建立多種destinations-gateway 組合，但是，只有一種閘道能使用

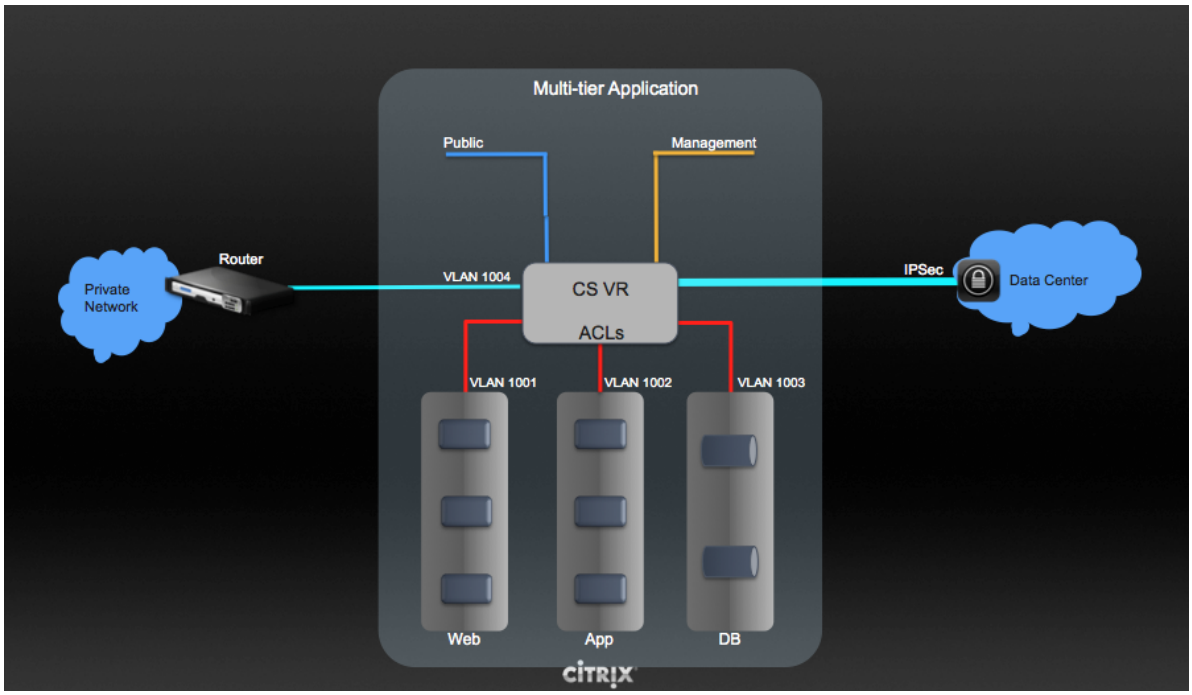
  例如:

  - VLANs and Public Gateway: 例如，應用程式安裝在雲端，以及Web application VMs與網際網路溝通

  - VLANs, VPN Gateway, and Public Gateway: 例如，應用程式安裝在雲端，以及Web application VMs與網際網路溝通，以及資料庫VM與內部裝置溝通

- 管理者可以在虛擬路由器定義 Access Control List (ACL)，來過濾VLAN的流量，或網際網路及VLAN間的流量。您可以基於CIDR、通訊埠範圍、type code(如果選擇ICMP協定)及輸入/輸出形式來定義ACL

以下圖示顯示可用的Inter-VLAN 設定範本:



想要建立多層級 Inter-VLAN，詳見 節 15.19, “設定虛擬私人雲端”

15.19. 設定虛擬私人雲端

15.19.1. 關於虛擬私人雲端

CloudStack 虛擬私人雲端是一種私人、獨立的CloudStack部分，一個VPC可以有自己的虛擬網路拓樸，如同傳統實體網路。您可以在虛擬網路上執行虛擬機器，虛擬網路可以有私人位址，例如: 10.0.0.0/16。您可以在VPC網路中定義網路層級，反過來，您可以基於IP位置範圍聚集相似種類的 instance

例如。如果VPC有私人範圍10.0.0.0/16，訪客網路可以有網路範圍 10.0.1.0/24、10.0.2.0/24、10.0.3.0/24...等等

VPC主要組件

VPC由以下網路組件組成:

- VPC: VPC作為多個獨立網路的容器，可以經由虛擬路由器與其他VPC通信
- Network Tiers: 每個層級作為獨立的網路，擁有自己的VLAN及CIDR表，您可以在此放置資源，像是虛擬機器。層級藉由VLAN來分割。每個層級的NIC作為閘道
- Virtual Router: 虛擬路由器會自動產生，並在VPC產生時啓動。虛擬路由器在公開閘道、VPC閘道及NAT instance上連接層級與直接流量。對於每個層級，會在虛擬路由器有相對應的NIC及IP。虛擬路由器藉由自己的IP提供DNS及DHCP服務
- Public Gateway: 經由公開閘道，從網際網路到VPC或是從VPC到網際網路的流量。對於VPC，因終端使用者看不到公開閘道，因此公開閘道並不支援固定路線
- Private Gateway: 經由私人閘道，從私人網路到VPC或是從VPC到私人網路的流量。更多資訊，詳見 節 15.19.5, “在VPC新增Private Gateway”
- VPN Gateway: VPN連線的VPC端
- Site-to-Site VPN Connection: 硬體基礎的VPN連結，在您的VPC與資料中心、家用網路或co-location設施之間。更多資訊，詳見 節 15.17.4, “設定 Site-to-Site VPN連線”
- Customer Gateway: VPN連線的客戶端。更多資訊，詳見節 15.17.4.1, “建立及更新VPN客戶閘道”
- NAT Instance: 提供通訊埠位址轉譯的 instance，可經由公開閘道存取網路。更多資訊，詳見 節 15.19.9, “開啓/關閉Static NAT”

VPC中的網路架構

以下為四個基礎的網路架構選項:

- 僅有公開閘道的VPC
- 有公開及私人閘道的VPC
- 有公開及私人閘道與站對站VPN存取的VPC
- 有私人閘道及站對站VPN存取的VPC

VPC的連結選項

您可以將您的VPC連接到:

- 透過公開閘道連接到網際網路
- 透過VPN閘道，使用站對站VPN連線來使用企業資料中心
- 使用公開閘道及VPN閘道來使用網際網路及企業資料中心

VPN網路注意事項

建立VPC前，請注意以下事項:

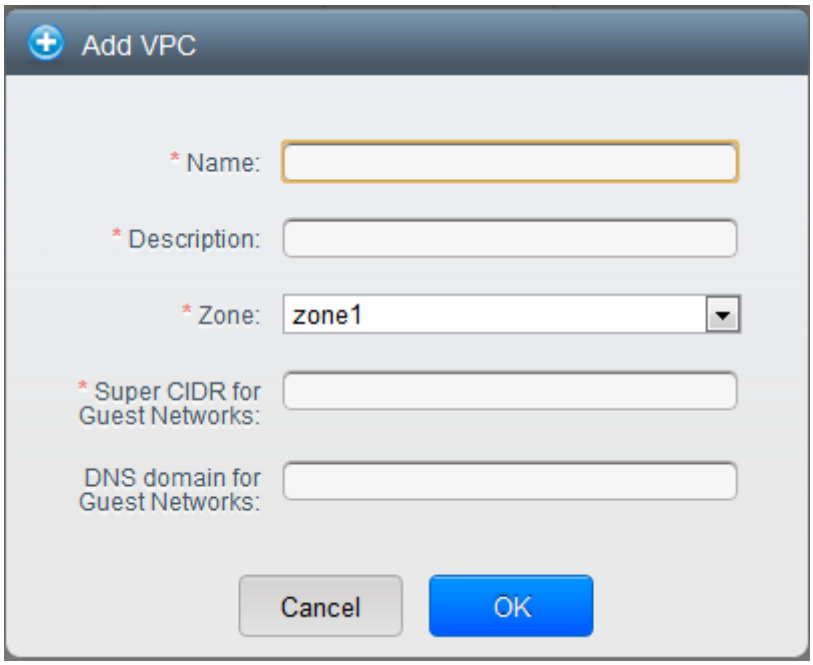
- 建立VPC後，預設為啓用狀態
- VPC僅能在進階區域建立，不能同時屬於多個區域

- 一個帳戶的VPC預設數量為20個。但是您可以使用max.account.vpcs廣域參數欄位來改變限制，此參數控制可新增的VPC最大數量
- 一個帳戶能新增的層級預設數量為3，您可以使用vpc.max.networks參數欄位來改變
- 每個層級都有唯一的CIDR，確保這些CIDR在VPC的CIDR範圍內
- 層級僅屬於一個VPC
- 所有網路層級應屬於同一個帳戶
- 建立VPC後，預設上會分配一個Source NAT IP，Source NAT IP只會在VPC移除時才會釋出
- 公開IP每次僅可使用在一個目的，如果IP為sourceNAT，則不能用作 StaticNAT或通訊埠轉送
- instances只會有您提供的私人IP位址，請啓用NAT給您要在VPC上執行的 instance，使 instance能與網際網路通信
- 只有新的網路能加到VPC。每個VPC的網路數量上限由vpc.max.networks參數來瘸定，預設為3
- 負載平衡服務僅可支援一個層級
- 如果IP位址分配到一個層級:
  - 此IP不能給其他層級同時使用。例如，如果您有層級A與層級B，以及公開IP1，您可以使用IP或A或B來建立通訊部轉送規則，但不能同時使用
  - 此IP不能用作StaticNAT、負載平衡或通訊埠轉送規則給其他訪客網路
- VPC網路不支援遠端存取VPN

15.19.2. 增加Virtual Private Cloud

建立VPC時，您只需要提供zone及一組IP位址。您需要以Classless Inter-Domain Routing (CIDR)方格的形式來設定這組IP

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select視窗選擇VPC
4. 按下 Add VPC， Add VPC頁面會顯示如下:



提供以下資訊:

- Name: 您想要建立的VPC名稱
- Description: VPC的簡述
- Zone: 選擇您要使用VPC的zone
- Super CIDR for Guest Networks: 對VPC內的所有tier(訪客網路)定義CIDR範圍。當您新增一個tier時, 請確定它的CIDR是在 Super CIDR數值中, CIDR必須適應RFC1918
- DNS domain for Guest Networks: 如果您想指定一個特別的domain名稱, 請指定DNS suffix。這個欄位套用到所有VPC中的tier, 亦即所有tier皆屬於同一個DNS domain。如果欄位沒有指定, 則名稱會自動產生

15.19.3. 新增層級

Tier在VPC中是個獨立的網路區域, 預設上是不能存取其他tier的。藉由虛擬路由器, Tier可以架設在VLAN上與其他溝通, Tier提供一個便宜且低延遲的VPC內部網路

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗, 選擇Network
3. 在Select視窗選擇VPC

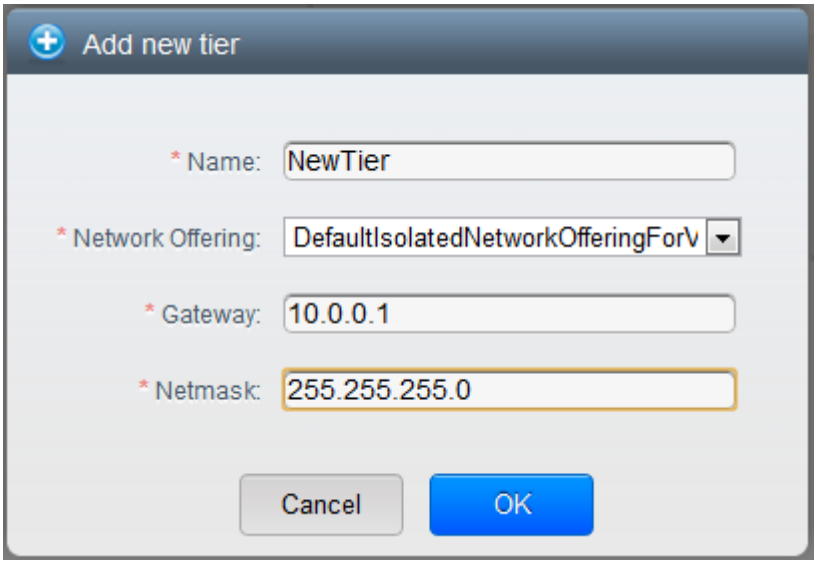
帳戶所有創建的VPC會表列在本頁

注意

終端使用者可以看見自己的VPC, 而root和主要管理者可以看見所有被授權的VPC

4. 對想要設置層級的VPC按下"Configure"

   會顯示Add new tier 對話框如下:



   如果你已經建立tier, 會顯示VPC的圖示, 按下Create Tie來新增

5. 具體說明以下:

   所有的欄位都必須填寫。

   - Name: 您建立的tier的名稱
   - Network Offering: 列出以下預設的網路服務:
     DefaultIsolatedNetworkOfferingForVpcNetworksNoLB,
     DefaultIsolatedNetworkOfferingForVpcNetworks

     在VPC, 只有用LB-enabled network offering才能建立一個tier
   - Gateway: 您新增的tier用的閘道, 請確定閘道在您建立VPC時指定的 Super CIDR範圍內, 並且沒有與其他在VPC內的tier重疊CIDR
   - Netmask: 您新增的tier用的網路遮罩

     例如, 如果VPC的CIDR是10.0.0.0/16, 而新的tier的CIDR是10.0.1.0/24, 閘道為10.0.1.1, 遮罩為255.255.255.0

6. 按OK

7. 繼續設定tier的access control list

15.19.4. 設定Access Control List

在VPC虛擬路由器上定義Network Access Control List (ACL), 並在VPC層級、層級和網際網路間控制輸入 (ingress)和輸出 (egress)流量, 預設上, 客戶網路的輸入、輸出流量是被阻擋的。你必須要建立新的network ACL來打開埠。只有在支援network ACL服務時才能在層級創立Network ACL

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗, 選擇Network
3. 在Select視窗選擇VPC

帳戶所有創建的VPC會表列在本頁

4. 按下"Settings"圖示

會顯示出以下選項

- IP Addresses
- Gateways
- Site-to-Site VPN
- Network ACLs

5. 選擇 Network ACLs.

會顯示Network ACLs頁面

6. 按下Add Network ACLs.

填入以下區域來指定哪種流量在此層級是被允許的

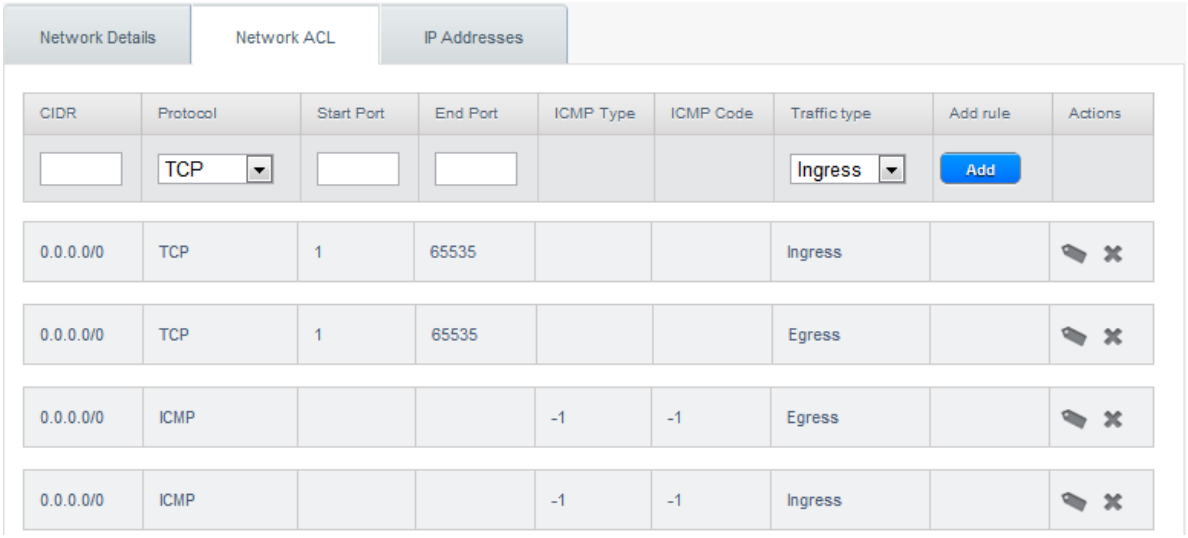
- CIDR: CIDR在 Ingress rules中扮演Source CIDR的腳色; 在Egress rules扮演Destination CIDR的腳色。為了在特定位址區域中允許流量自或到IP位址, 進入CIDR或CIDR的comma-separated list。CIDR是輸入流量的基礎IP。比如說, 192.168.0.0/22, 為了允許所有CIDR, 設定 0.0.0.0/0.
- Protocol: 來源送流量到層級的網路協定。TCP和UDP協定常被用作資料交換和終端使用者傳輸, ICMP協定常被用作傳送錯誤訊息或網路監視資料
- Start Port, End Port (TCP, UDP only): 一個範圍內, 輸入流量目標的正在等候埠, 如果你要開啓一個埠, 在所有區內使用同一數字
- Select Tier: 選擇您想要新增此ACL規則的層級
- ICMP Type, ICMP Code(限ICMP): 訊息的形式及送出錯誤碼
- Traffic Type: 選擇您想要套用的流量型態
  - Egress: 從Traffic type下拉式選單選擇Egress , 然後按Add, 這會指定哪一種流量在此層級能夠送出VM。如果沒有Egress規則被指定, 所有流量就都可以允許送出VM虛擬路由器, 一旦規則被指定, 只有規則指定的流量及其他被ingress規則允許的流量能被送出。如果同一層級間的VMs需要互相溝通, 就不能有egress規則
  - Ingress: 從Traffic type下拉式選單選擇Ingress, 然後按Add。 這會指定哪一種流量在此層級能夠送進VM。如果沒有Ingress規則被指定, 所有流量就都不允許送進, 除了有被egress規則定義的流量

注意

預設上, 所有訪客網路的輸入輸出流量都是被封鎖的。新增一個ACL網路可以開啓不

7. 按下Add, ACL規則就會被加入

從Network ACLs頁面，選擇想要瀏覽的層級，然後選擇Network ACL標籤，可以看到您新增的ACL規則



您可以編輯ACL規則的標籤和刪除規則。在Actions欄位按下適當的按鈕

15.19.5. 在VPC新增Private Gateway

private gateway只能被系統管理者新增。VPC私人網路和NIC實體網路有1：1的關係，在同一個資料中心不允許複製VLAN和IP的閘道

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select視窗選擇VPC

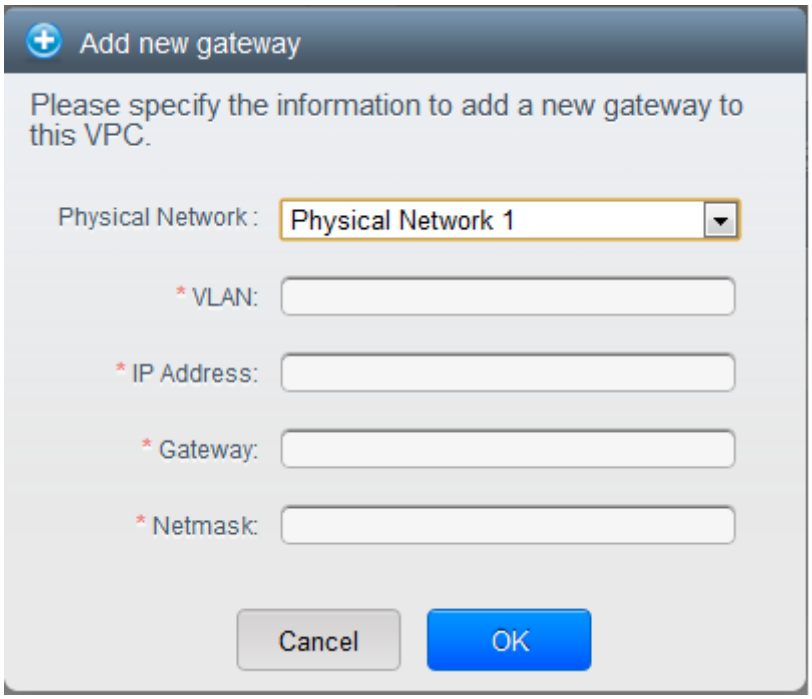
   帳戶所有創建的VPC會表列在本頁
4. 對想要設定load balancing rules的VPC按下"Configure"

   VPC 頁面會顯示所有你創建的層級
5. 按下"Settings"圖示

   會顯示出以下選項

   - IP Addresses
   - Private Gateways
   - Site-to-Site VPN
   - Network ACLs
6. 選擇Private Gateways.

   會顯示Gateways葉面
7. 按Add new gateway:



8. 具體說明以下:

   • Physical Network: 在這區域中你創的實體網路

   • IP Address: 與VPC閘道關聯的IP位址

   • Gateway: 流量路由到和自VPC的閘道

   • Netmask: 和VPC閘道關聯的網路遮罩

   • VLAN:和VPC閘道關聯的VLAN

   新的閘道會出現在表單中, 你可以重複以上步驟來新增多個規則

15.19.6. 配置VM到層級

1. 以管理者或終端使用者登入CloudStack UI

2. 在左邊的導覽視窗, 選擇Network

3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁

4. 對想要配置VM的VPC按下"Configure"

   VPC 頁面會顯示所有你創建的層級

5. 在要新增VM的層級, 按下 Add VM

   會顯示Add Instance葉面

   依循螢幕上的指示來增加一個instance, 更多資訊, 詳見安裝指南中的Adding Instances章節

15.19.7. 為VPC取得一個新的IP

當你取得一個IP時，所有IP位址將被分配到VPC，而不是到VPC內的客戶網路。IP只有在port-forwarding，load balancing，或Static NAT rule被建立時才會連結到客戶網路。同時，IP每次只能連結到一個網路

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁
4. 對想要配置VM的VPC按下"Configure"

   VPC 頁面會顯示所有你創建的層級
5. 按下"Settings"圖示

   會顯示出以下選項

   • IP Addresses

   • Gateways

   • Site-to-Site VPN

   • Network ACLs
6. 選擇IP Addresses

   顯示IP Address葉面
7. 按下Acquire New IP，然後按下Yes

   由於IP位址是有限的資源，因此你需要立即得確認。不久後IP位址應該就會顯示Allocated。現在你可以使用你的IP來 port forwarding，load balancing，和 static NAT rules.

15.19.8. 釋出一個IP給VPC

IP位址是有限的，如果你已經不需要固定IP，你可以切斷IP與VPC的連結，使IP成為可用位址。IP位址只有在所有規則（ port forwarding，load balancing，or StaticNAT ）都移除的情況下才能被釋出。釋出的IP仍屬於同一個VPC

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁
4. 對想要釋出IP的VPC按下 Configure

   VPC 頁面會顯示所有你創建的層級
5. 按下"Settings"圖示

   會顯示出以下選項

- IP Addresses
- Gateways
- Site-to-Site VPN
- Network ACLs

6. 選擇IP Addresses

   顯示IP Address葉面

7. 選擇你想要釋出的IP

8. 在Details標籤，按下Release IP 

15.19.9. 開啓/關閉Static NAT

static NAT rule 配對一個公衆IP到VM上的私人IP，並允許網路連結。這個章節教你如何對特定IP開啓或關閉 static NAT

如果port forwarding rules已經開啓，你將不能開啓static NAT

如果客戶的VM是多個網路的一部份，static NAT rules只有定義在預設網路時才能正常運作

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁

4. 對想要配置VM的VPC按下"Configure"

   VPC 頁面會顯示所有你創建的層級

5. 按下"Settings"圖示

   會顯示出以下選項

   - IP Addresses
   - Gateways
   - Site-to-Site VPN
   - Network ACLs

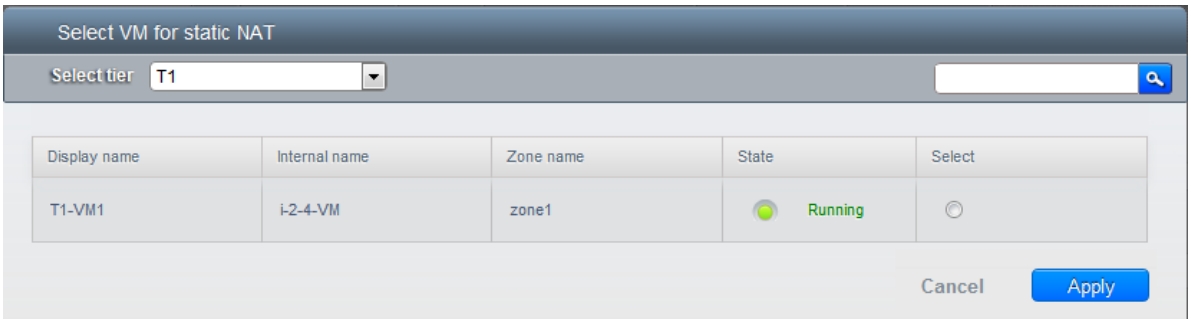
6. 選擇IP Addresses

   顯示IP Address葉面

7. 選擇你想要套用的IP

8. 在Details標籤，按下Static NAT  按鈕會依據static NAT是否開啓而變動

9. 如果你開啓static NAT會跳出以下對話框



10. 選擇層級及目標VM，然後按下 Apply

15.19.10. 在VPC新增 Load Balancing Rules

CloudStack的使用者或管理者創建規則來平衡一至多個提供負載平衡服務的網路等級VM的流量，使用者創立規則，指定一組演算法，然後套用規則到VPC中一組VM上

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁
4. 對想要設定load balancing rules的VPC按下"Configure"

   VPC 頁面會顯示所有你創建的層級
5. 按下"Settings"圖示

   會顯示出以下選項

   - IP Addresses
   - Gateways
   - Site-to-Site VPN
   - Network ACLs
6. 選擇IP Addresses

   顯示IP Address葉面
7. 選擇你想要新增規則的IP，按下Configuration標籤
8. 在 Load Balancing 點，按 View All
9. 選擇你想要套用規則的層級

注意

在VPC，負仔平衡服務僅支援一個層級

10. 具體說明以下：

- Name: load balancer rule的名稱
- Public Port: 應被平衡流量的埠
- Private Port: VM接收流量的不
- Algorithm 選擇你想要CloudStack使用的演算法，CloudStack支援以下已知的演算法
  - Round-robin
  - Least connections
  - Source
- Stickiness. (非必須) 點選Configure並選擇stickiness policy的演算法，請參Sticky Session Policies for Load Balancer Rules章節
- Add VMs: 按Add VMs，然後選擇兩個以上要分流量的VMs，然後按Apply

新的規則會出現在表單中，你可以重複以上步驟來新增多個規則

15.19.11. 在VPC新增 Port Forwarding Rule

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁
4. 對想要配置VM的VPC按下"Configure"

   VPC 頁面會顯示所有你創建的層級
5. 按下"Settings"圖示

   會顯示出以下選項
   - IP Addresses
   - Gateways
   - Site-to-Site VPN
   - Network ACLs
6. 選擇一個存在的IP或是取得一個新的IP

顯示IP Address頁面

7. 選擇你想要新增規則的IP，按下Configuration標籤

8. 在 Port Forwarding 點，按 View All

9. 選擇你想要套用規則的層級

10. 具體說明以下：

    • Public Port:公開傳輸的埠會定址在前一步驟獲得的IP上

    • Private Port: 虛擬機實例於此網路中傾聽的port。

    • Protocol: 通訊協定使用在兩個埠之間

      • TCP

      • UDP

    • Add VM: 按Add VM，選擇規則要套用的實例，然後按Apply

      你可以開啓 ssh session來測試規則

15.19.12. 移除Tiers

您可以從VPC移除層級，被移除的層級將不能回復，當層級被刪除時，只有層級內的資源會被刪除。所有網路規則(port forwarding，load balancing and staticNAT) 和關聯的IP位址將會被移除，但IP位址仍屬於同一個VPC

1. 以管理者或終端使用者登入CloudStack UI

2. 在左邊的導覽視窗，選擇Network

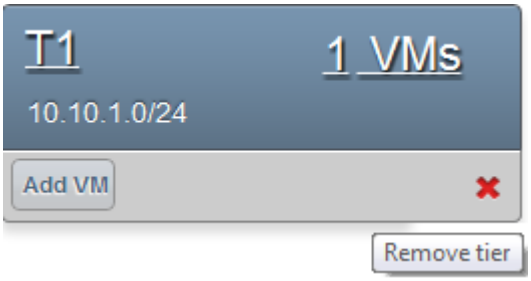
3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁

4. 對想要設置層級的VPC按下"Configure"

   Configure VPC 頁面會顯示，選擇您想要套用的層級

5. 按下



   等待層級被移除

15.19.13. 編輯、重新啓動和移除Virtual Private Cloud

注意

移除VPC前，先確保所有層級已經移除

1. 以管理者或終端使用者登入CloudStack UI
2. 在左邊的導覽視窗，選擇Network
3. 在Select視窗選擇VPC

   帳戶所有創建的VPC會表列在本頁
4. 選擇你想要套用的IVPC
5. 想移除VPN ， 按下 Remove VPN connection button 

   你可以編輯VPC的名稱和描述，選擇VPC然後按下Edit 

   To restart a VPC, select the VPC, then click the Restart button.  i

15.20. 持續網路

The network that you can provision without having to deploy any VMs on it is called a persistent network. A persistent network can be part of a VPC or a non-VPC environment.

When you create other types of network, a network is only a database entry until the first VM is created on that network. When the first VM is created, a VLAN ID is assigned and the network is provisioned. Also, when the last VM is destroyed, the VLAN ID is released and the network is no longer available. With the addition of persistent network, you will have the ability to create a network in CloudStack in which physical devices can be deployed without having to run any VMs. Additionally, you can deploy physical devices on that network.

One of the advantages of having a persistent network is that you can create a VPC with a tier consisting of only physical devices. For example, you might create a VPC for a three-tier application, deploy VMs for Web and Application tier, and use physical machines for the Database tier. Another use case is that if you are providing services by using physical hardware, you can define the network as persistent and therefore even if all its VMs are destroyed the services will not be discontinued.

15.20.1. Persistent Network Considerations

- Persistent network is designed for isolated networks.
- All default network offerings are non-persistent.
- A network offering cannot be editable because changing it affects the behavior of the existing networks that were created using this network offering.

- When you create a guest network, the network offering that you select defines the network persistence. This in turn depends on whether persistent network is enabled in the selected network offering.
- An existing network can be made persistent by changing its network offering to an offering that has the Persistent option enabled. While setting this property, even if the network has no running VMs, the network is provisioned.
- An existing network can be made non-persistent by changing its network offering to an offering that has the Persistent option disabled. If the network has no running VMs, during the next network garbage collection run the network is shut down.
- When the last VM on a network is destroyed, the network garbage collector checks if the network offering associated with the network is persistent, and shuts down the network only if it is non-persistent.

15.20.2. Creating a Persistent Guest Network

To create a persistent network, perform the following:

1. Create a network offering with the Persistent option enabled.

   詳見節 9.4.1, “新增新的網路服務”

2. 在左方導覽方格, 選擇Network
3. 選擇您要提供服務的訪客網路
4. 按下Edit
5. 從Network Offering下拉式選單, 選擇您剛建立的持續網路服務
6. 按OK

使用系統虛擬機器

CloudStack使用多種類型的系統虛擬機器來在雲端執行任務。通常CloudStack管理這些系統虛擬機器，以及建立、啓動及停止，依據擴展或立即需求時使用。但是管理者應該要注意這些虛擬機器，以及它們協助除錯的功能

注意

您可以設定ystem.vm.random.password欄位來建立隨機的系統虛擬機器密碼，以達到更高的安全性。如果您重設數值system.vm.random.password為true，並重新啓動管理伺服器，隨機的密碼就會產生，並存在加密的資料庫中。您可以檢查解密的密碼，可以在CloudStack使用者介面檢查system.vm.password廣域參數欄位，或是呼叫listConfigurations API

16.1. 系統虛擬機器模組

系統虛擬機器由一個模組產生，並有以下特性:

- Debian 6.0 ("Squeeze")，2.6.32核心，擁有最新的安全性補丁，補丁出自於Debian security APT repository
- 有最小的組件組，從而減少能攻擊的地方
- 增强效能的32位元Xen/VMWare
- 擁有Xen PV驅動程式、KVM virtio 驅動程式及最佳化效能的VMware tools 的pvops核心
- Xen tools inclusion 允許效能監視功能
- 最新版的HAProxy、iptables、IPsec及 Apache from debian repository 確保安全性及速度
- 最新版的JRE from Sun/Oracle確保安全性及速度

16.2. Multiple System VM Support for VMware

Every CloudStack zone has single System VM for template processing tasks such as downloading templates, uploading templates, and uploading ISOs. In a zone where VMware is being used, additional System VMs can be launched to process VMware-specific tasks such as taking snapshots and creating private templates. The CloudStack management server launches additional System VMs for VMware-specific tasks as the load increases. The management server monitors and weights all commands sent to these System VMs and performs dynamic load balancing and scaling-up of more System VMs.

16.3. Console Proxy

The Console Proxy is a type of System Virtual Machine that 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 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 Host hosting the guest.

注意

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 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.

16.3.1. Using a SSL Certificate for the Console Proxy

The console viewing functionality uses a dynamic DNS service under the domain name realhostip.com 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://aaa-bbb-ccc-ddd.realhostip.com. You will see this URL during console session creation. CloudStack includes the realhostip.com SSL certificate in the console proxy VM. Of course, CloudStack cannot know about the DNS A records for our customers' public IPs prior to shipping the software. CloudStack therefore runs a dynamic DNS server that is authoritative for the realhostip.com domain. It maps the aaa-bbb-ccc-ddd part of the DNS name to the IP address aaa.bbb.ccc.ddd 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.

16.3.2. 改變控制台代理SSL認證及網域

如果管理者想要，有可能客戶的控制台工作的URL會顯示不同於realhostip.com的網路。管理者可以自訂顯示的網域，藉由選擇不同的網域，並上傳新的SSL認證與私人金鑰。往玉必須執行DNS服務，能夠解析位址查詢，位址形式為aaa-bbb-ccc-ddd.your.domain，並轉成IPv4 IP位址，位址形式為aaa.bbb.ccc.ddd。例如，202.8.44.1。想要改變控制台代理網域、SSL認證及私人金鑰：

1. 建立動態名稱解析或填充所有您公開IP範圍中可能的DNS名稱到已有的DNS伺服器，格式為aaa-bbb-ccc-ddd.company.com -> aaa.bbb.ccc.ddd

2. 產生私人金鑰及certificate signing request (CSR)，當您要使用openss1來產生私人/公開金鑰對及CSRs時，對於您要貼到CloudStack使用者介面的私人金鑰，請確定已轉為PKCS#8 格式

a. 產生新的2048位元私人金鑰

```
openssl genrsa -des3 -out yourprivate.key 2048
```

b. 產生新的認證CSR

```
openssl req -new -key yourprivate.key -out yourcertificate.csr
```

c. 前往您信任的認證機構網站，購買SSL認證，然後交給CSR，您會收到合法的認證

d. 將您的私人金鑰格式轉為 PKCS#8加密格式

```
openssl pkcs8 -topk8 -in yourprivate.key -out yourprivate.pkcs8.encrypted.key
```

e. 將您的PKCS#8加密私人金鑰轉為PKCS#8格式，符合CloudStack的格式

```
openssl pkcs8 -in yourprivate.pkcs8.encrypted.key -out yourprivate.pkcs8.key
```

3. In the Update SSL Certificate screen of the CloudStack UI, paste the following:

   • The certificate you've just generated.

   • The private key you've just generated.

   • 新的網域名稱，例如，company.com

4. 新的網域名稱，例如，company.com

   This stops all currently running console proxy VMs, then restarts them with the new certificate and key. Users might notice a brief interruption in console availability.

The Management Server generates URLs of the form "aaa-bbb-ccc-ddd.company.com" after this change is made. The new console requests will be served with the new DNS domain name, certificate, and key.

16.4. 虛擬路由器

虛擬路由器使一種System Virtual Machine。它是最常被CloudStack服務提供者使用的服務。端點使用者沒有直接的存取，使用者可以先檢查虛擬路由器是否存在，然後開始動作(例如設定port forwarding)，但是使用者無法使用SSH存取

虛擬路由器沒有伺服機制給管理者登入。虛擬路由器可以被管理者重新啓動，但會中斷公衆網路存取及使用者的服務，最簡單的檢查網路方式為先檢查訪客VM的虛擬路由器是否存在，有些虛擬路由器的特徵由其關聯的網路服務決定

16.4.1. Configuring the Virtual Router

You can set the following:

• IP range

• Supported network services

- Default domain name for the network serviced by the virtual router
- Gateway IP address
- How often CloudStack fetches network usage statistics from CloudStack virtual routers. If you want to collect traffic metering data from the virtual router, set the global configuration parameter router.stats.interval. If you are not using the virtual router to gather network usage statistics, set it to 0.

16.4.2. 使用System Service Offerings升級虛擬路由器

當CloudStack建立虛擬路由器時，會使用預設設定。參見節 8.2, “系統服務”。所有單一個訪客網路內的虛擬路由器都使用相同的system service offering。您可以藉由新增及套用自訂的system service offering來提升虛擬路由器的相容性

1. 定義您自訂的system service offering。參見 節 8.2.1, “建立新的系統服務”，在System VM Type選擇Domain Router
2. 使用network offering連結 system service offering
3. 套用network offering到您想要虛擬路由器套用的新system service offering的網路。如果是新網路，請按照Adding an Additional Guest Network 第66頁步驟。想要變更已存在的虛擬路由器 service offering，請照節 15.6.2, “改變訪客網路的服務”步驟

16.4.3. 虛擬路由器的最佳練習

- 注意：從超級監督者控制台重新啓動虛擬路由器會刪除所有iptables規則。停止虛擬路由器並由 CloudStack 使用者介面啓動，來處理此問題
- 注意：當您只有一個路由器可用時，不要使用destroyRouter API，因為 restartNetwork API帶有cleanup=false參數，會無法重新建立。如果您要移除並重新建立路由器，請使用restartNetwork API，含有cleanup=true參數

16.5. Secondary Storage VM

In addition to the hosts, CloudStack’s Secondary Storage VM mounts and writes to secondary storage.

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

The secondary storage VM provides a background task that takes care of a variety of secondary storage activities: downloading a new template to a Zone, copying templates between Zones, and snapshot backups.

The administrator can log in to the secondary storage VM if needed.

系統可靠性及高可用性

17.1. 管理伺服器的HA

CloudStack管理伺服器應部署在多節點的組態中，以使伺服器不會易受單一主機故障影響。管理伺服器本身(不同於MySQL資料庫)是無歸屬的，且應置於負載平衡器之後

正常運作的主機不會受所有管理伺服器的停止運轉影響，所有訪客虛擬網路會持續工作

當管理伺服器離線後，就不能新增虛擬機器，及終端使用者、管理使用者介面、API、動態負載分配，HA會停止工作

17.2. Management Server Load Balancing

CloudStack可以使用負載平衡器來為管理伺服器提供虛擬IP，管理者負責建立負載平衡規則，此應用需要在多通訊任務能持續及固定，以下圖表列出應套用負載平衡的埠，及是否要持續

即使不需要持續套用，您也可以啓用

Source Port	Destination Port	Protocol	Persistence Required?
80 or 443	8080 (or 20400 with AJP)	HTTP (or AJP)	Yes
8250	8250	TCP	Yes
8096	8096	HTTP	No

In addition to above settings, the administrator is responsible for setting the 'host' global config value from the management server IP to load balancer virtual IP address. If the 'host' value is not set to the VIP for Port 8250 and one of your management servers crashes, the UI is still available but the system VMs will not be able to contact the management server.

17.3. HA-Enabled Virtual Machines

使用者可以指定虛擬機器為啓用HA。預設，所有虛擬路由器虛擬機器及彈性負載平衡虛擬機器會自動設定為啓用HA。當啓用HA的虛擬機器故障時，在同一可用區域內的CloudStack會偵測到故障並自動重新啓動虛擬機器，HA無法跨區域操作。CloudStack對重新啓動虛擬機器有個保守的策略，並且確保沒有同時兩個擁有相同VM的instance能夠同時操作，管理伺服器會傾向於在同一叢集中的其他主機啓動虛擬機器

HA功能使用iSCSI 或 NFS主要儲存裝置，不支援本地儲存裝置

17.4. 主機的HA

使用者可以指定虛擬機器為啓用HA。預設，所有虛擬路由器虛擬機器及彈性負載平衡虛擬機器會自動設定為啓用HA。當啓用HA的虛擬機器故障時，在同一可用區域內的CloudStack會偵測到故障並自動重新啓動虛擬機器，HA無法跨區域操作。CloudStack對重新啓動虛擬機器有個保守的策略，並且確保沒有同時兩個擁有相同VM的instance能夠同時操作，管理伺服器會傾向於在同一叢集中的其他主機啓動虛擬機器

HA功能使用iSCSI 或 NFS主要儲存裝置，不支援本地儲存裝置

17.4.1. Dedicated HA Hosts

One or more hosts can be designated for use only by HA-enabled VMs that are restarting due to a host failure. Setting up a pool of such dedicated HA hosts as the recovery destination for all HA-enabled VMs is useful to:

- Make it easier to determine which VMs have been restarted as part of the CloudStack high-availability function. If a VM is running on a dedicated HA host, then it must be an HA-enabled VM whose original host failed. (With one exception: It is possible for an administrator to manually migrate any VM to a dedicated HA host.).
- Keep HA-enabled VMs from restarting on hosts which may be reserved for other purposes.

The dedicated HA option is set through a special host tag when the host is created.
To allow the administrator to dedicate hosts to only HA-enabled VMs, set the global configuration variable ha.tag to the desired tag (for example, "ha_host"), and restart the Management Server. Enter the value in the Host Tags field when adding the host(s) that you want to dedicate to HA-enabled VMs.

注意

If you set ha.tag, be sure to actually use that tag on at least one host in your cloud. If the tag specified in ha.tag is not set for any host in the cloud, the HA-enabled VMs will fail to restart after a crash.

17.5. 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.Primary storage is not designed to be backed up. Individual volumes in primary storage can be backed up using snapshots.

17.6. Secondary Storage Outage and Data Loss

For a Zone that has only one secondary storage server, 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. Secondary storage should be backed up periodically. Multiple secondary storage servers can be provisioned within each zone to increase the scalability of the system.

17.7. Limiting the Rate of API Requests

You can limit the rate at which API requests can be placed for each account. This is useful to avoid malicious attacks on the Management Server, prevent performance degradation, and provide fairness to all accounts.

If the number of API calls exceeds the threshold, an error message is returned for any additional API calls. The caller will have to retry these API calls at another time.

17.7.1. Configuring the API Request Rate

To control the API request rate, use the following global configuration settings:

- api.throttling.enabled - Enable/Disable API throttling. By default, this setting is false, so API throttling is not enabled.
- api.throttling.interval (in seconds) - Time interval during which the number of API requests is to be counted. When the interval has passed, the API count is reset to 0.
- api.throttling.max - Maximum number of APIs that can be placed within the api.throttling.interval period.
- api.throttling.cachesize - Cache size for storing API counters. Use a value higher than the total number of accounts managed by the cloud. One cache entry is needed for each account, to store the running API total for that account.

17.7.2. Limitations on API Throttling

The following limitations exist in the current implementation of this feature.

注意

Even with these limitations, CloudStack is still able to effectively use API throttling to avoid malicious attacks causing denial of service.

- In a deployment with multiple Management Servers, the cache is not synchronized across them. In this case, CloudStack might not be able to ensure that only the exact desired number of API requests are allowed. In the worst case, the number of API calls that might be allowed is (number of Management Servers) * (api.throttling.max).
- The API commands resetApiLimit and getApiLimit are limited to the Management Server where the API is invoked.

管理雲端

18.1. 使用Tags來管理雲端資源

Tag是儲存雲端中繼資料的key-value pair，用來分類資源很有用。例如，您可以tag一個值給使用者的VM來標記使用者的城市所在，在這個例子，key就是"city"，value就是"Toronto"或"Tokyo"，您可以請CloudStack找所有有tag的資源，例如，給一個城市名稱，找所有使用者的VM

您可以tag使用者的虛擬機器、容量、快取圖片、訪客網路、模組、ISO、防火牆規則、port forwarding rule、公開IP位址、security group、 load balancer rule、計畫、VPC、network ACL或static route。您不行tag遠端存取的VPN

您可以藉由使用者介面或使用API指令createTags、deleteTags和listTags來操作tag。您也可以為每個資源定義多個tags，並沒有數量限制。每一個tag可以長達255個字元，使用者可以在自己的資源上定義tags，而管理者可以定義所有雲端上的資源

選擇性的欄位 "tags"在很多 list* API 指令都有，以下範例演示如何使用這些新欄位來找到所有volumn tag region=canada 或 tag city=Toronto:

```
command=listVolumes
    &listAll=true
    &tags[0].key=region
    &tags[0].value=canada
    &tags[1].key=city
    &tags[1].value=Toronto
```

以下有"tags"輸入欄位的API指令:

- listVirtualMachines
- listVolumes
- listSnapshots
- listNetworks
- listTemplates
- listIsos
- listFirewallRules
- listPortForwardingRules
- listPublicIpAddresses
- listSecurityGroups
- listLoadBalancerRules
- listProjects
- listVPCs
- listNetworkACLs
- listStaticRoutes

18.2. 改變資料庫設定

CloudStack 管理伺服器在/etc/cloud/management/db.properties中儲存了資料庫的設定資訊(例如:主機名稱、通訊埠、credentials)。請在每個管理伺服器編輯此檔案，並重新啓動使變更生效

18.3. 改變資料庫密碼

您可能需要改變 CloudStack使用的MySQL帳戶密碼。如果是，您需要改變MySQL的密碼，並加入加密的密碼到/etc/cloud/management/db.properties

1. 改變密碼前，請先停止CloudStack的管理伺服器，如果您有部署使用引擎，也請停止

```
# service cloudstack-management stop
# service cloudstack-usage stop
```

2. 接下來，更新MySQL伺服器的CloudStack使用者密碼

```
# mysql -u root -p
```

在MySQL shell，改變密碼及清除優先權:

```
update mysql.user set password=PASSWORD("newpassword123") where User='cloud';
flush privileges;
quit;
```

3. 下一步，將密碼加密，然後複製到CloudStack的資料庫設定(/etc/cloud/management/db.properties)

```
# java -classpath /usr/share/java/cloud-jasypt-1.8.jar \ org.jasypt.intf.cli.JasyptPBEStringEncryptionCLI
 encrypt.sh \ input="newpassword123" password="`cat /etc/cloud/management/key`" \ verbose=false
```

檔案加密類型

注意，這是給檔案加密類型的設定。如果您使用網頁加密類型，您需要使用 password="management_server_secret_key"

4. 現在，使用新的 ciphertext更新 /etc/cloud/management/db.properties。使用記事本開啓/etc/cloud/management/db.properties 並更新這些欄位:

```
db.cloud.password=ENC(encrypted_password_from_above)
db.usage.password=ENC(encrypted_password_from_above)
```

5. 複製新密碼後，您可以啓動CloudStack(及使用引擎)

```
# service cloudstack-management start
# service cloudstack-usage start
```

18.4. Administrator Alerts

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.

Emails will be sent to administrators under the following circumstances:

- The Management Server cluster runs low on CPU, memory, or storage resources
- The Management Server loses heartbeat from a Host for more than 3 minutes
- The Host cluster runs low on CPU, memory, or storage resources

18.5. Customizing the Network Domain Name

The root administrator can optionally assign a custom DNS suffix at the level of a network, account, domain, zone, or entire CloudStack installation, and a domain administrator can do so within their own domain. To specify a custom domain name and put it into effect, follow these steps.

1. Set the DNS suffix at the desired scope
   - At the network level, the DNS suffix can be assigned through the UI when creating a new network, as described in 節 15.6.1, “新增” or with the updateNetwork command in the CloudStack API.
   - At the account, domain, or zone level, the DNS suffix can be assigned with the appropriate CloudStack API commands: createAccount, editAccount, createDomain, editDomain, createZone, or editZone.
   - At the global level, use the configuration parameter guest.domain.suffix. You can also use the CloudStack API command updateConfiguration. After modifying this global configuration, restart the Management Server to put the new setting into effect.
2. To make the new DNS suffix take effect for an existing network, call the CloudStack API command updateNetwork. This step is not necessary when the DNS suffix was specified while creating a new network.

The source of the network domain that is used depends on the following rules.

- For all networks, if a network domain is specified as part of a network's own configuration, that value is used.
- For an account-specific network, the network domain specified for the account is used. If none is specified, the system looks for a value in the domain, zone, and global configuration, in that order.

- For a domain-specific network, the network domain specified for the domain is used. If none is specified, the system looks for a value in the zone and global configuration, in that order.
- For a zone-specific network, the network domain specified for the zone is used. If none is specified, the system looks for a value in the global configuration.

18.6. 停止與重啓管理伺服器

root管理者需要時常停止和重啓管理伺服器

例如，改變廣域設定後，會需要重新啓動。如果您有多個管理伺服器節點，請全部重新啓動

要停止管理伺服器，在管理伺服器節點的作業系統提示輸入以下指令:

```
# service cloudstack-management stop
```

要啓動管理伺服器:

```
# service cloudstack-management start
```

要停止管理伺服器:

```
# service cloudstack-management stop
```

Global Configuration Parameters

19.1. 設定廣域設定欄位

CloudStack提供很多欄位給您控制很多東西，當CloudStack第一次安裝，您需要修改這些設定

1. 以administrator身分登入CloudStack UI
2. 於左側的navigation按鈕中，點選Global Settings。
3. 於Select View中選擇其中一項:
   - Global Settings: 欄位列表，附有簡述及現在的數值
   - Hypervisor Capabilities: 超級監督者版本列表，附有最大支援訪客數量
4. 使用搜尋欄縮小列表
5. 點選Edit圖示來修改數值，如果您正瀏覽Hypervisor Capabilities，請先點選超級監督者的名稱

19.2. About Global Configuration Parameters

CloudStack provides a variety of settings you can use to set limits, configure features, and enable or disable features in the cloud. Once your Management Server is running, you might need to set some of these global configuration parameters, depending on what optional features you are setting up.

To modify global configuration parameters, use the steps in "Setting Global Configuration Parameters."

The documentation for each CloudStack feature should direct you to the names of the applicable parameters. Many of them are discussed in the CloudStack Administration Guide. The following table shows a few of the more useful parameters.

Field	數值
management.network.cidr	A CIDR that describes the network that the management CIDRs reside on. This variable must be set for deployments that use vSphere. It is recommended to be set for other deployments as well. Example: 192.168.3.0/24.
xen.setup.multipath	For XenServer nodes, this is a true/false variable that instructs CloudStack to enable iSCSI multipath on the XenServer Hosts when they are added. This defaults to false. Set it to true if you would like CloudStack to enable multipath.

Field	数値
	If this is true for a NFS-based deployment multipath will still be enabled on the XenServer host. However, this does not impact NFS operation and is harmless.
secstorage.allowed.internal.sites	This is used to protect your internal network from rogue attempts to download arbitrary files using the template download feature. This is a comma-separated list of CIDRs. If a requested URL matches any of these CIDRs the Secondary Storage VM will use the private network interface to fetch the URL. Other URLs will go through the public interface. We suggest you set this to 1 or 2 hardened internal machines where you keep your templates. For example, set it to 192.168.1.66/32.
use.local.storage	Determines whether CloudStack will use storage that is local to the Host for data disks, templates, and snapshots. By default CloudStack will not use this storage. You should change this to true if you want to use local storage and you understand the reliability and feature drawbacks to choosing local storage.
host	This is the IP address of the Management Server. If you are using multiple Management Servers you should enter a load balanced IP address that is reachable via the private network.
default.page.size	Maximum number of items per page that can be returned by a CloudStack API command. The limit applies at the cloud level and can vary from cloud to cloud. You can override this with a

Field	数値
	lower value on a particular API call by using the page and pagesize API command parameters. For more information, see the Developer's Guide. Default: 500.
ha.tag	The label you want to use throughout the cloud to designate certain hosts as dedicated HA hosts. These hosts will be used only for HA-enabled VMs that are restarting due to the failure of another host. For example, you could set this to ha_host. Specify the ha.tag value as a host tag when you add a new host to the cloud.

CloudStack API

CloudStack API是低層級的API，使用為實踐 CloudStack網頁使用者介面，也是好的實現其他API，像是EC2/S3及新的DMTF standards，的基礎

許多CloudStack API呼叫是非同步性的，這些API會立即回復工作ID，此工作ID可以用來詢問工作情況，同時，詢問受影響的資源，會提供一些跡象

API有REST-like 詢問激出，並回覆結果以 XML 或 JSON格式

詳見the Developer's Guide[1] and the API Reference[2]

20.1. Provisioning and Authentication API

CloudStack 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 CloudStack to add/remove users..

CloudStack supports pluggable authenticators. By default, CloudStack assumes it is provisioned with the user's password, and as a result authentication is done locally. However, external authentication is possible as well. For example, see Using an LDAP Server for User Authentication.

20.2. Allocators

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

20.3. User Data and Meta Data

CloudStack 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
```

2. 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/meta-data/{metadata type}. (For backwards compatibility, the previous URL http://10.1.1.1/latest/{metadata type} is also supported.) For metadata type, use one of the following:

・service-offering. A description of the VMs service offering

[1] http://docs.cloudstack.org/CloudStack_Documentation/Developer's_Guide%3A_CloudStack
[2] http://docs.cloudstack.org/CloudStack_Documentation/API_Reference%3A_CloudStack

- 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

Tuning

This section provides tips on how to improve the performance of your cloud.

21.1. 效能監視

使用者及管理者可以存取主機和來賓的效能監視，這可以讓使用者監視資源的使用率，並決定何時該選擇更有力的服務或更大的硬碟

21.2. 增加管理伺服器記憶體

如果管理伺服器是高使用率，預設的JVM記憶體可能會不夠，為增加記憶體:

1. 編輯 Tomcat系統設定檔:

```
/etc/cloud/management/tomcat6.conf
```

2. 將指令欄-XmxNNNm改為更高數值的N

   例如，如果現在數值為-Xmx128m，改成-Xmx1024m或更高

3. 重新啓動伺服器使變更生效

```
# service cloudstack-management restart
```

更多資訊，詳見Tomcat Wiki.[1]的"FAQ: Memory"

21.3. 設定資料庫緩衝群大小

提供MySQL資料庫足夠的記憶體使很重要的，因為資料庫需要快取檔案及編排目錄:

1. Edit the MySQL configuration file:

```
/etc/my.cnf
```

2. 在 [mysqld] 插入以下行數到datadir，使用適合您的數值。建議設定緩衝群為 40% o的記憶體，如果MySQL與管理伺服器為同一伺服器；或是70% o的記憶體，如果MySQL是獨立的伺服器，以下範例假設為獨立的，記憶體為 1024M:

```
innodb_buffer_pool_size=700M
```

3. 重新啓動 MySQL

```
# service mysqld restart
```

更多資訊，詳見 MySQL Reference Manual[2]的 "The InnoDB Buffer Pool"

[1] http://wiki.apache.org/tomcat/FAQ/Memory
[2] http://dev.mysql.com/doc/refman/5.5/en/innodb-buffer-pool.html

21.4. Set and Monitor Total VM Limits per Host

CloudStack 管理者需要監視每台叢集上有多少虛擬機器，如果接近超級監督者能負荷的最大量，管理者需要停止分配到此叢集。請確定遠離安全界線，以增加主機故障的容忍程度，主機故障會增加其他主機的虛擬機器負擔。參照您選擇的超級監督者文件，取得允許的最大量，然後使用 CloudStack廣域組態設定將其設為預設值。隨時監視虛擬機器的活動，並保持虛擬機器總數在安全界線之下，以允許偶而的主機故障。例如，如果有N台主機，然後您想要隨時關閉一台主機，而能夠允許的虛擬機器總量最多為(N-1) *(每台主機限制)，一旦叢集達到限制數量，請使用 CloudStack使用者介面來停止更多虛擬機器分配到此叢集

21.5. 設定XenServer dom0記憶體

設定XenServer dom0來分配更多記憶體到dom0，使XenServer可以處理更多虛擬機器。建議2940 MB。有關設定指南，詳閱Citrix Knowledgebase Article[3]，此文章為 XenServer 5.6版本，但適用6版

[3] http://support.citrix.com/article/CTX126531

疑難雜症

22.1. Events

An event is essentially a significant or meaningful change in the state of both virtual and physical resources associated with a cloud environment. Events are used by monitoring systems, usage and billing systems, or any other event-driven workflow systems to discern a pattern and make the right business decision. In CloudStack an event could be a state change of virtual or psychical resources, an action performed by an user (action events), or policy based events (alerts).

22.1.1. Event Logs

There are two types of events logged in the CloudStack Event Log. Standard events log the success or failure of an event and can be used to identify jobs or processes that have failed. There are also long running job events. Events for asynchronous jobs log when a job is scheduled, when it starts, and when it completes. Other long running synchronous jobs log when a job starts, and when it completes. Long running synchronous and asynchronous event logs can be used to gain more information on the status of a pending job or can be used to identify a job that is hanging or has not started. The following sections provide more information on these events..

22.1.2. 事件通知

事件通知架構提供管理伺服器元件公開即訂閱 CloudStack 事件的方法，事件通知藉由提示事件匯流排抽象化的概念來達成。事件匯流排允許CloudStack元件和擴充插件訂閱事件，藉由使用Advanced Message Queuing Protocol (AMQP)客戶端來達成，預設的事件匯流排提示使用RabbitMQ AMQP客戶端來提供，如同一個插件。AMQP客戶端會推進公開事件到相容的AMQP伺服器。因此CloudStack 事件會在AMQP伺服器交換

新的狀態或資源狀態改變事件，被引進微事件通知架構的一部份，每個資源，像是使用者VM、容量、網路卡、網路、公開IP、快取物件及模組，會連結到一個狀態機器，並產生事件，作為事件變更的一部份，即如果有改變的話，會導致事件變更，以及事件會公開到事件匯流排，所有CloudStack事件(警告、動作事件、使用事件)即額外的分類資源狀態改變事件，都會公開到事件匯流排

使用例子

以下為一些使用例子:

- Usage or Billing Engines: 第三方雲端使用方案可以執行一個連結CloudStack訂閱CloudStack事件，並產生使用資料的插件，使用資料會被它們的軟體消耗
- AMQP插件可以在訊息貯列放置所有事件，AMQP message broker可以提供 topic-based提示給訂閱者
- 公開及訂閱提示服務可以使用在CloudStack中作為可插入式服務，提供豐富的APIs，像是topics-based訂閱及通知，除此之外，可插入式服務可以用於多租賃、認證及授權服務

系統設定

身為 CloudStack管理者，執行以下一次性的設定來啓用事件通知架構，執行階段就不能變更

1. 開啓'componentContext.xml

2. 定義bean，名為eventNotificationBus，如下:

- name : 指定一個名稱
- server: RabbitMQ AMQP伺服器的名稱或IP位址
- port: RabbitMQ伺服器執行的通訊埠
- username: 存取RabbitMQ 伺服器的帳戶使用者名稱
- password : 存取RabbitMQ 伺服器的帳戶密碼
- exchange: 在RabbitMQ伺服器的交換名稱

一個範例bean如下:

```
<bean id="eventNotificationBus" class="org.apache.cloudstack.mom.rabbitmq.RabbitMQEventBus">
    <property name="name" value="eventNotificationBus"/>
    <property name="server" value="127.0.0.1"/>
    <property name="port" value="5672"/>
    <property name="username" value="guest"/>
    <property name="password" value="guest"/>
   <property name="exchange" value="cloudstack-events"/>
   </bean>
```

The eventNotificationBus bean 代表org.apache.cloudstack.mom.rabbitmq.RabbitMQEventBus 等級

3. 重新啓動 Management Server

22.1.3. Standard Events

The events log records three types of standard events.

- INFO. This event is generated when an operation has been successfully performed.
- WARN. This event is generated in the following circumstances.
  - When a network is disconnected while monitoring a template download.
  - When a template download is abandoned.
  - When an issue on the storage server causes the volumes to fail over to the mirror storage server.
- ERROR. This event is generated when an operation has not been successfully performed

22.1.4. Long Running Job Events

The events log records three types of standard events.

- INFO. This event is generated when an operation has been successfully performed.
- WARN. This event is generated in the following circumstances.
  - When a network is disconnected while monitoring a template download.
  - When a template download is abandoned.
  - When an issue on the storage server causes the volumes to fail over to the mirror storage server.

- ERROR. This event is generated when an operation has not been successfully performed

22.1.5. Event Log Queries

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

22.2. 操作伺服器紀錄

The CloudStack Management Server logs all web site, middle tier, and database activities for diagnostics purposes in /var/log/cloudstack/management/. The CloudStack logs a variety of error messages. We recommend this command to find the problematic output in the Management Server log:.

注意

當複製及貼上指令時，請確定指令是貼成單一條線，因為有些文件瀏覽器會多出不必要的中斷

```
grep -i -E 'exception|unable|fail|invalid|leak|warn|error' /var/log/cloudstack/management/management-server.log
```

CloudStack需要工作ID，如果您發現錯誤，您想要修正它的話，您可以找其工作ID，例如，如果您找到以下錯誤訊息:

```
2010-10-04 13:49:32,595 ERROR [cloud.vm.UserVmManagerImpl] (Job-Executor-11:job-1076) Unable to find any host for [User|i-8-42-VM-untagged]
```

工作ID即為1076，您可以追蹤事件相關的工作，使用以下搜尋:

```
grep "job-1076)" management-server.log
```

The CloudStack Agent Server logs its activities in /var/log/cloudstack/agent/.

22.3. 匯出主要儲存裝置時資料遺失

症狀

主要儲存裝置的資料遺失，主要為Linux NFS 伺服器匯出到 iSCSI容量

原因

有可能是外來客戶掛載儲存裝置，發生時LVM會清理，然後所有容量的資料都會遺失

解決方案

當建立LUN匯出時，限制允許存取IP的範圍，藉由指定子網路遮罩來達成，例如：

```
echo “/export 192.168.1.0/24(rw,async,no_root_squash)” > /etc/exports
```

修正以上指令為適合您的需求

更多資訊

詳見CloudStack Installation Guide的"Secondary Storage"章節中的匯出步驟

22.4. Recovering a Lost Virtual Router

症狀

A virtual router is running, but the host is disconnected. A virtual router no longer functions as expected.

原因

The Virtual router is lost or down.

解決方案

If you are sure that a virtual router is down forever, or no longer functions as expected, destroy it. You must create one afresh while keeping the backup router up and running (it is assumed this is in a redundant router setup):

- Force stop the router. Use the stopRouter API with forced=true parameter to do so.
- Before you continue with destroying this router, ensure that the backup router is running. Otherwise the network connection will be lost.
- Destroy the router by using the destroyRouter API.

Recreate the missing router by using the restartNetwork API with cleanup=false parameter. For more information about redundant router setup, see Creating a New Network Offering.

For more information about the API syntax, see the API Reference at http://docs.cloudstack.org/CloudStack_Documentation/API_Reference%3A_CloudStackAPI Reference.

22.5. 維護模式在vCenter無法正常運作

症狀
將主機設為維護模式，但是在vCenter仍為活動中

原因
CloudStack 管理者使用者介面用來將主機放到排程的維護模式，此模式與 vCenter的維護模式是不同的

解決方案
使用 vCenter將主機進入維護模式

更多資訊
詳見節 11.2, “Scheduled Maintenance and Maintenance Mode for Hosts”

22.6. Unable to deploy VMs from uploaded vSphere template

症狀
When attempting to create a VM, the VM will not deploy.

原因
If the template was created by uploading an OVA file that was created using vSphere Client, it is possible the OVA contained an ISO image. If it does, the deployment of VMs from the template will fail.

解決方案
Remove the ISO and re-upload the template.

22.7. Unable to power on virtual machine on VMware

症狀
Virtual machine does not power on. You might see errors like:

- Unable to open Swap File
- Unable to access a file since it is locked
- Unable to access Virtual machine configuration

原因
A known issue on VMware machines. ESX hosts lock certain critical virtual machine files and file systems to prevent concurrent changes. Sometimes the files are not unlocked when

the virtual machine is powered off. When a virtual machine attempts to power on, it can not access these critical files, and the virtual machine is unable to power on.

解決方案

See the following:

VMware Knowledge Base Article[1]

22.8. Load balancer rules fail after changing network offering

症狀

After changing the network offering on a network, load balancer rules stop working.

原因

Load balancing rules were created while using a network service offering that includes an external load balancer device such as NetScaler, and later the network service offering changed to one that uses the CloudStack virtual router.

解決方案

Create a firewall rule on the virtual router for each of your existing load balancing rules so that they continue to function.

[1] http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=10051/

附錄 A. 時區

CloudStack可使用以下時區確認器，許多時區有要求或選擇的欄位，這些包含在Configuration表中排程常用快取物件、建立使用者及指定使用時區

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/Halifax	America/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/Cairo	Asia/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	

附錄 B. Event Types

VM.CREATE	TEMPLATE.EXTRACT	SG.REVOKE.INGRESS
VM.DESTROY	TEMPLATE.UPLOAD	HOST.RECONNECT
VM.START	TEMPLATE.CLEANUP	MAINT.CANCEL
VM.STOP	VOLUME.CREATE	MAINT.CANCEL.PS
VM.REBOOT	VOLUME.DELETE	MAINT.PREPARE
VM.UPGRADE	VOLUME.ATTACH	MAINT.PREPARE.PS
VM.RESETPASSWORD	VOLUME.DETACH	VPN.REMOTE.ACCESS.CREATE
ROUTER.CREATE	VOLUME.UPLOAD	VPN.USER.ADD
ROUTER.DESTROY	SERVICEOFFERING.CREATE	VPN.USER.REMOVE
ROUTER.START	SERVICEOFFERING.UPDATE	NETWORK.RESTART
ROUTER.STOP	SERVICEOFFERING.DELETE	UPLOAD.CUSTOM.CERTIFICATE
ROUTER.REBOOT	DOMAIN.CREATE	UPLOAD.CUSTOM.CERTIFICATE
ROUTER.HA	DOMAIN.DELETE	STATICNAT.DISABLE
PROXY.CREATE	DOMAIN.UPDATE	SSVM.CREATE
PROXY.DESTROY	SNAPSHOT.CREATE	SSVM.DESTROY
PROXY.START	SNAPSHOT.DELETE	SSVM.START
PROXY.STOP	SNAPSHOTPOLICY.CREATE	SSVM.STOP
PROXY.REBOOT	SNAPSHOTPOLICY.UPDATE	SSVM.REBOOT
PROXY.HA	SNAPSHOTPOLICY.DELETE	SSVM.H
VNC.CONNECT	VNC.DISCONNECT	NET.IPASSIGN
NET.IPRELEASE	NET.RULEADD	NET.RULEDELETE
NET.RULEMODIFY	NETWORK.CREATE	NETWORK.DELETE
LB.ASSIGN.TO.RULE	LB.REMOVE.FROM.RULE	LB.CREATE
LB.DELETE	LB.UPDATE	USER.LOGIN
USER.LOGOUT	USER.CREATE	USER.DELETE
USER.UPDATE	USER.DISABLE	TEMPLATE.CREATE
TEMPLATE.DELETE	TEMPLATE.UPDATE	TEMPLATE.COPY
TEMPLATE.DOWNLOAD.START	TEMPLATE.DOWNLOAD.SUCCESS	TEMPLATE.DOWNLOAD.FAILED
ISO.CREATE	ISO.DELETE	ISO.COPY
ISO.ATTACH	ISO.DETACH	ISO.EXTRACT
ISO.UPLOAD	SERVICE.OFFERING.CREATE	SERVICE.OFFERING.EDIT
SERVICE.OFFERING.DELETE	DISK.OFFERING.CREATE	DISK.OFFERING.EDIT
DISK.OFFERING.DELETE	NETWORK.OFFERING.CREATE	NETWORK.OFFERING.EDIT
NETWORK.OFFERING.DELETE	POD.CREATE	POD.EDIT
POD.DELETE	ZONE.CREATE	ZONE.EDIT
ZONE.DELETE	VLAN.IP.RANGE.CREATE	VLAN.IP.RANGE.DELETE
CONFIGURATION.VALUE.EDIT	SG.AUTH.INGRESS	

附錄 C. 警告

The following is the list of alert type numbers. The current alerts can be found by calling listAlerts.

```
MEMORY = 0
```

```
CPU = 1
```

```
STORAGE =2
```

```
STORAGE_ALLOCATED = 3
```

```
PUBLIC_IP = 4
```

```
PRIVATE_IP = 5
```

```
HOST = 6
```

```
USERVM = 7
```

```
DOMAIN_ROUTER = 8
```

```
CONSOLE_PROXY = 9
```

```
ROUTING = 10// lost connection to default route (to the gateway)
```

```
STORAGE_MISC = 11 // lost connection to default route (to the gateway)
```

```
USAGE_SERVER = 12 // lost connection to default route (to the gateway)
```

```
MANAGMENT_NODE = 13 // lost connection to default route (to the gateway)
```

```
DOMAIN_ROUTER_MIGRATE = 14
```

```
CONSOLE_PROXY_MIGRATE = 15
```

```
USERVM_MIGRATE = 16
```

```
VLAN = 17
```

```
SSVM = 18
```

```
USAGE_SERVER_RESULT = 19
```

```
STORAGE_DELETE = 20;
```

```
UPDATE_RESOURCE_COUNT = 21; //Generated when we fail to update the resource count
```

```
USAGE_SANITY_RESULT = 22;
```

```
DIRECT_ATTACHED_PUBLIC_IP = 23;
```

```
LOCAL_STORAGE = 24;
```

```
RESOURCE_LIMIT_EXCEEDED = 25; //Generated when the resource limit exceeds the limit. Currently used for
 recurring snapshots only
```

附錄 D. 修訂記錄

修訂 0-0 Tue May 29 2012 Jessica Tomechak
初始版本