Apache CloudStack 4.1.0

CloudStack 安装指南

Apache CloudStack

Apache CloudStack 4.1.0 CloudStack 安装指南

作者 Apache CloudStack

CloudStack安装指南

1. 概念 1
1.1. 甚麼是CloudStack? 1
1.2. What Can CloudStack Do? 1
1.3. 架設架構總攬 2
1.3.1. Management Server Overview 3
1.3.2. 雲端基礎架構簡介 3
1.3.3. 網路簡介 4
2. 雲端基礎架構概念 5
2.1. About Regions 5
2.2. 關於區域 5
2.3. 關於Pods 7
2.4. 關於Clusters 7
2.5. About Hosts 8
2.6. About Primary Storage 9
2.7. About Secondary Storage 9
2.8. About Physical Networks 9
2.8.1. Basic Zone Network Traffic Types 10
2.8.2. Basic Zone Guest IP Addresses 11
2.8.3. Advanced Zone Network Traffic Types 11
2.8.4. Advanced Zone Guest IP Addresses 12
2.8.5. Advanced Zone Public IP Addresses 12
2.8.6. 系統保留IP位址 12
3. 從來源建立 13
3.1. 取得release 13
3.2. 辨認下載的 release 13
3.2.1. 取得KEYS 13
3.2.2. GPG 13
3.2.3. MD5 14
3.2.4. SHA512 14
3.3. 建立Apache CloudStack的先決條件 14
3.4. 解壓縮原始碼 14
3.5. 建立DEB packages 14
3.5.1. 建立APT repo 15
3.5.2. 使用APT repository設定您的機器 16
3.6. 從原始碼建立RPM 16
3.6.1. 產生RPM 17
3.7. Building Non-OSS 18
4. 安裝 21
4.1. 誰該閱讀本手冊 21
4.2. Overview of Installation Steps 21
4.3. 最低系統需求 21
4.3.1. 管理伺服器、資料庫及儲存系統需求 21
4.3.2. 主機/超級監督者 系統需求 22
4.4. 設定package repository 23
4.4.1. DEB package repository 23
4.4.2. RPM package repository 23
4.5. 管理伺服器安裝 24
4.5.1. 管理伺服器安裝簡介 24
4.5.2. 準備作業系統 24
4.5.3. 在第一台主機安裝管理伺服器 25
4.5.4. 安裝資料庫伺服器 26
4.5.5. 關於密碼及金要加密 30

4.5.6. 準備NFS Shares 31
4.5.7. 準備及啓動其他管理伺服器 34
4.5.8. 準備系統VM模組 35
4.5.9. 安裝完成! 下一步 36

5. 使用者介面 37
5.1. 登入使用者介面 37
5.1.1. End User's UI Overview 37
5.1.2. Root Administrator's UI Overview 37
5.1.3. 以Root Administrator的身分登入 37
5.1.4. 改變root密碼 38
5.2. 使用SSH Key授權 39
5.2.1. 建立支援SSH Key的Instance Template 39
5.2.2. 新增SSH Keypair 39
5.2.3. 新增Instance 40
5.2.4. 用 SSH Keypair登入 41
5.2.5. 重設 41

6. Steps to Provisioning Your Cloud Infrastructure 43
6.1. Overview of Provisioning Steps 43
6.2. Adding Regions (optional) 44
6.2.1. The First Region: The Default Region 44
6.2.2. Adding a Region 44
6.2.3. Adding Third and Subsequent Regions 45
6.2.4. Deleting a Region 47
6.3. 新增Zone 47
6.3.1. 基礎區域設定 48
6.3.2. 進階Zone設定 51
6.4. 新增Pod 54
6.5. 新增一個Cluster 55
6.5.1. 新增Cluster: KVM 或 XenServer 55
6.5.2. 加入叢集: vSphere 55
6.6. 增加主機 57
6.6.1. (XenServer 或 KVM)增加主機 57
6.6.2. Adding a Host (vSphere) 59
6.7. 新增Primary Storage 59
6.7.1. 系統需求 59
6.7.2. 新增主要儲存裝置 60
6.8. 新增次要儲存裝置 61
6.8.1. 次要儲存裝置系統需求 61
6.8.2. 新增次要儲存裝置 61
6.9. 初始化及測試 61

7. Global Configuration Parameters 63
7.1. 設定廣域設定欄位 63
7.2. About Global Configuration Parameters 63

8. 超級監督者安裝流程 67
8.1. KVM超級監督者主機安裝 67
8.1.1. KVM Hypervisor主機系統需求 67
8.1.2. KVM 安裝簡介 67
8.1.3. 準備作業系統 68
8.1.4. 安裝及設定 Agent 69
8.1.5. 安裝及設定libvirt 69
8.1.6. 設定 Security Policies 70
8.1.7. 設定網路橋接器 71

8.1.8. Configure the network using OpenVswitch 74
8.1.9. 設定防火牆 77
8.1.10. 將主機加到CloudStack 78
8.2. CloudStack的Citrix XenServer安裝 78
8.2.1. XenServer主機系統需求 78
8.2.2. XenServer安裝步驟 79
8.2.3. 設定XenServer dom0記憶體 79
8.2.4. 使用者名稱與密碼 79
8.2.5. 時間同步 79
8.2.6. 授權 80
8.2.7. 安裝CloudStack XenServer Support Package (CSP) 80
8.2.8. XenServer主要儲存裝置設定 81
8.2.9. XenServer iSCSI 多通道設定(選擇性) 82
8.2.10. XenServer實體網路設定 82
8.2.11. 更新XenServer版本 85
8.3. VMware vSphere安裝與設定 88
8.3.1. vSphere主機系統需求 88
8.3.2. VMware的準備清單 90
8.3.3. vSphere安裝步驟 91
8.3.4. ESXi主機設定 91
8.3.5. 實體主機網路 91
8.3.6. vSphere的儲存裝置準備工作(限) 95
8.3.7. 新增主機 或 設定 Clusters (vSphere) 98
8.3.8. 套用Hotfixes到 VMware vSphere主機 98

9. 額外安裝選項 101
9.1. 安裝使用伺服器(選擇性) 101
9.1.1. 安裝需求 101
9.1.2. 安裝步驟 101
9.2. SSL(選擇性) 101
9.3. 複製資料庫(選擇性) 101
9.3.1. Failover 103

10. 選擇部署架構 105
10.1. Small-Scale Deployment 105
10.2. 大尺度的Redundant設定 106
10.3. Separate Storage Network 107
10.4. Multi-Node Management Server 107
10.5. 多站點部署 107

11. Amazon Web Services相容的界面 111
11.1. Amazon Web Services相容的界面 111
11.2. 支援的API版本 111
11.3. 啓用 EC2 及 S3相容介面 111
11.3.1. 啓用服務 112
11.3.2. 建立EC2相容服務 112
11.3.3. 修改AWS API 通訊埠 113
11.4. AWS API User Setup 114
11.4.1. AWS API User Registration 114
11.4.2. AWS API Command-Line Tools Setup 115
11.5. 使用Timeouts來確保AWS API Command Completion 115
11.6. 支援AWS API的呼叫 115
11.7. 範例 117
11.7.1. Boto 範例 117
11.7.2. JClouds範例 119

12. 網路設定 121
12.1. 基本與進階網路 121
12.2. VLAN Allocation Example 121
12.3. 硬體設定範例 122
12.3.1. Dell 62xx 122
12.3.2. Cisco 3750 122
12.4. Layer-2交換器 123
12.4.1. Dell 62xx 123
12.4.2. Cisco 3750 124
12.5. 硬體防火牆 124
12.5.1. 通用防火牆規則 124
12.5.2. Juniper SRX的外部訪客防火牆累積(選擇性) 124
12.5.3. 外部訪客負載平衡器累積(選擇性) 127
12.6. Management Server Load Balancing 128
12.7. 拓樸需 128
12.7.1. 安全性需求 128
12.7.2. 執行期間的內部通訊需求 128
12.7.3. 儲存網路拓樸需求 128
12.7.4. External Firewall Topology Requirements 129
12.7.5. 進階區域拓樸需求 129
12.7.6. XenServer拓樸需求 129
12.7.7. VMware拓樸需求 129
12.7.8. KVM拓樸需求 129
12.8. Traffic Sentinel的訪客網路使用累計 129
12.9. 設定Zone VLAN與執行VM最大值 130

13. 管理網路及流量 131
13.1. 訪客流量 131
13.2. Networking in a Pod 131
13.3. Networking in a Zone 133
13.4. 基礎區域的實體網路設定 133
13.5. Advanced Zone Physical Network Configuration 133
13.5.1. 於Advanced Zone下設定Guest Traffic 134
13.5.2. Configure Public Traffic in an Advanced Zone 134
13.6. Using Multiple Guest Networks 135
13.6.1. 新增 135
13.6.2. 改變訪客網路的服務 135
13.7. Security Groups 136
13.7.1. 關於安全群組 136
13.7.2. 新增 136
13.7.3. (僅限KVM)進階Zone的Security Groups 137
13.7.4. 啓用Security Groups 137
13.7.5. 在安全群組增加輸入及輸出規則 137
13.8. External Firewalls and Load Balancers 138
13.8.1. About Using a NetScaler Load Balancer 138
13.8.2. 在RHEL伺服器設定SNMP Community String 139
13.8.3. 外部防火牆及負載平衡器的初始設定 141
13.8.4. 持續設定外部防火牆及 141
13.8.5. 設定 AutoScale 141
13.9. Load Balancer Rules 146
13.9.1. 增加 Load Balancer Rule 146
13.9.2. Sticky Session Policies for Load Balancer Rules 147
13.10. 訪客IP範圍 147
13.11. 獲得新的IP 147

13.12. 釋出IP位址 148
13.13. Static NAT 148
13.13.1. 開啓/關閉Static NAT 148
13.14. IP轉送及防火牆 148
13.14.1. 建立Advanced區內的 149
13.14.2. Firewall Rules 150
13.14.3. Port Forwarding 150
13.15. IP Load Balancing 151
13.16. DNS 及 DHCP 151
13.17. VPN 151
13.17.1. 設定VPN 152
13.17.2. 在Windows使用VPN 152
13.17.3. Using VPN with Mac OS X 153
13.17.4. 設定 Site-to-Site VPN連線 154
13.18. 關於 Inter-VLAN Routing 160
13.19. 設定虛擬私人雲端 161
13.19.1. 關於虛擬私人雲端 161
13.19.2. 增加Virtual Private Cloud 163
13.19.3. 新增層級 164
13.19.4. 設定Access Control List 165
13.19.5. 在VPC新增Private Gateway 167
13.19.6. 配置VM到層級 168
13.19.7. 為VPC取得一個新的IP 169
13.19.8. 釋出一個IP給VPC 169
13.19.9. 開啓/關閉Static NAT 170
13.19.10. 在VPC新增 Load Balancing Rules 171
13.19.11. 在VPC新增 Port Forwarding Rule 172
13.19.12. 移除Tiers 173
13.19.13. 編輯、重新啓動和移除Virtual Private Cloud 174
13.20. 持續網路 174
13.20.1. Persistent Network Considerations 174
13.20.2. Creating a Persistent Guest Network 175
A. 修訂記錄 177

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

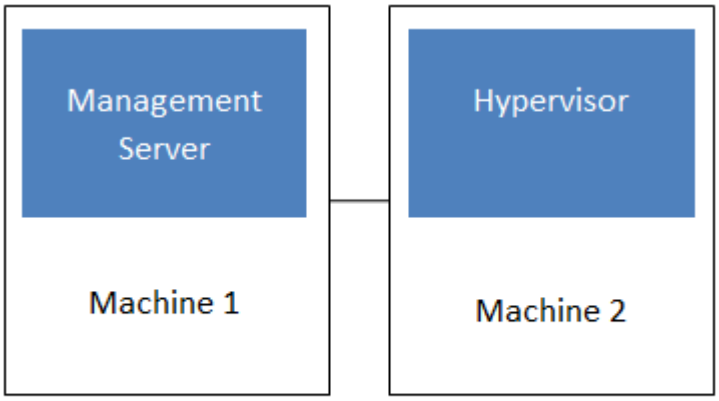
CloudStack has a number of features to increase the availability of the system. The Management Server itself may be deployed in a multi-node installation where the servers are load balanced. MySQL may be configured to use replication to provide for a manual failover in the event of database loss. For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

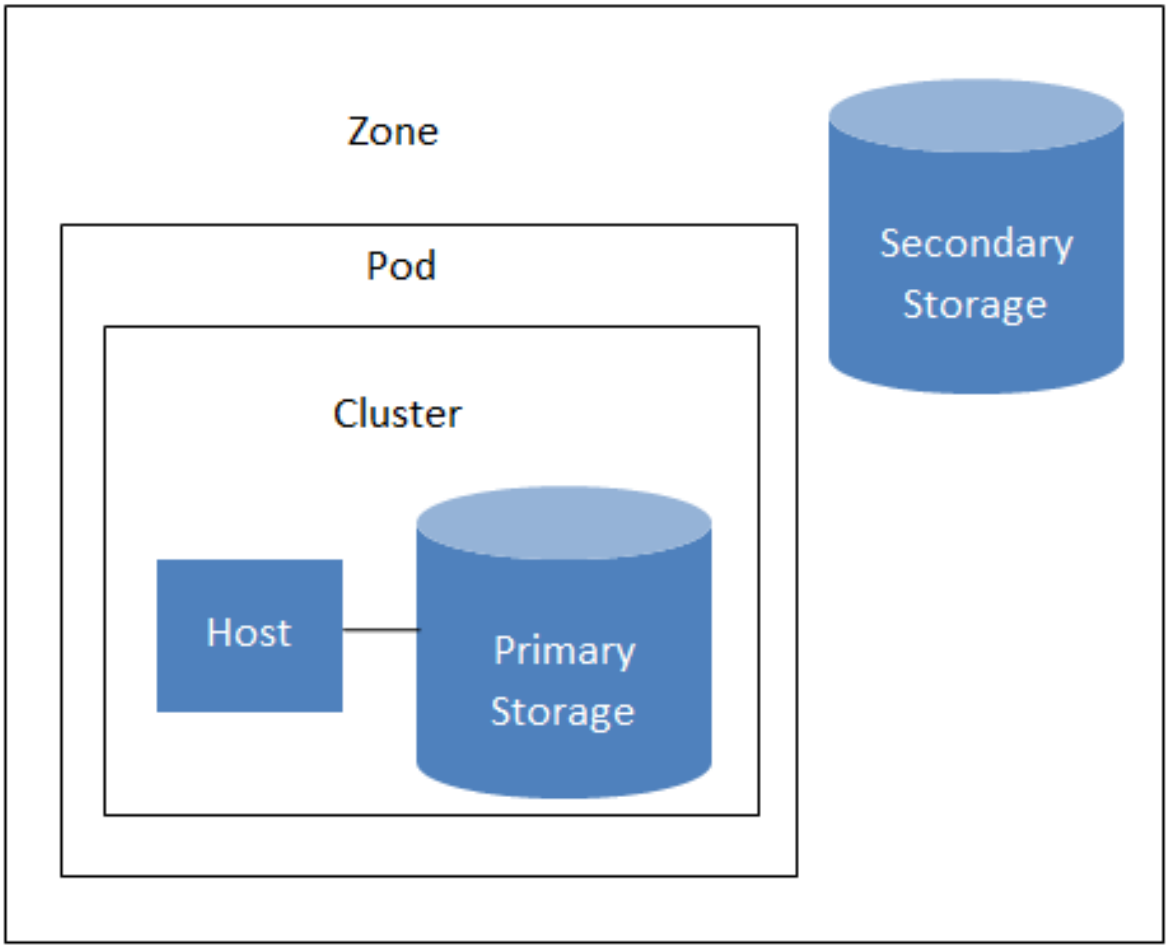
管理伺服器管理多個區域(通常為資料中心)，包含訪客虛擬機器的主機，雲端基礎架構可以組織為下:

- 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

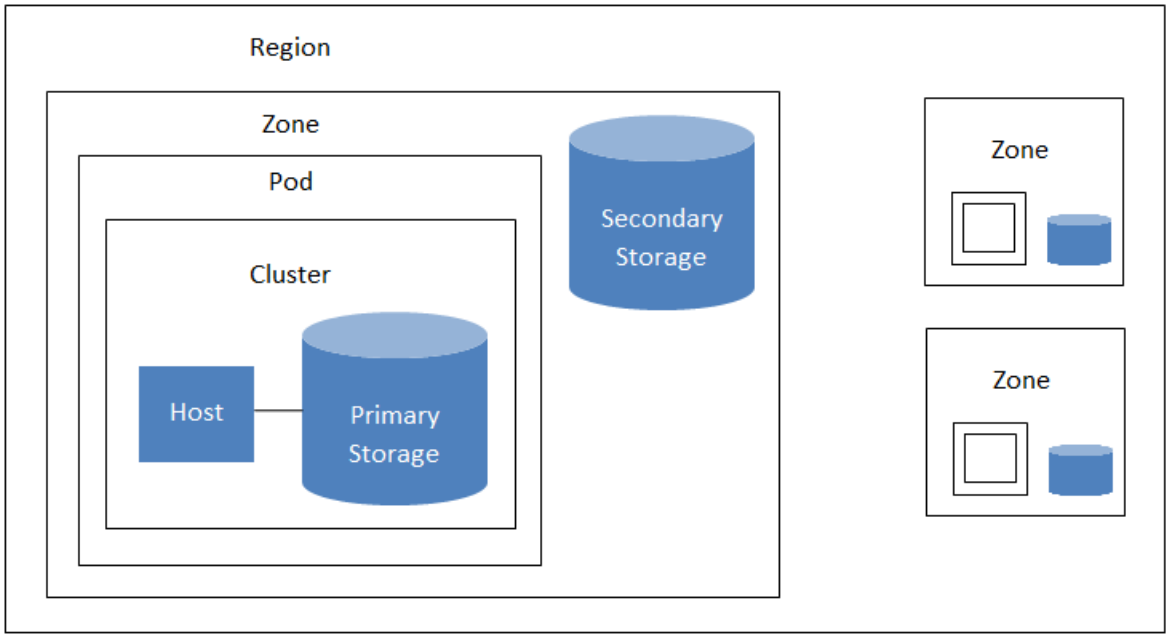
雲端基礎架構概念

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

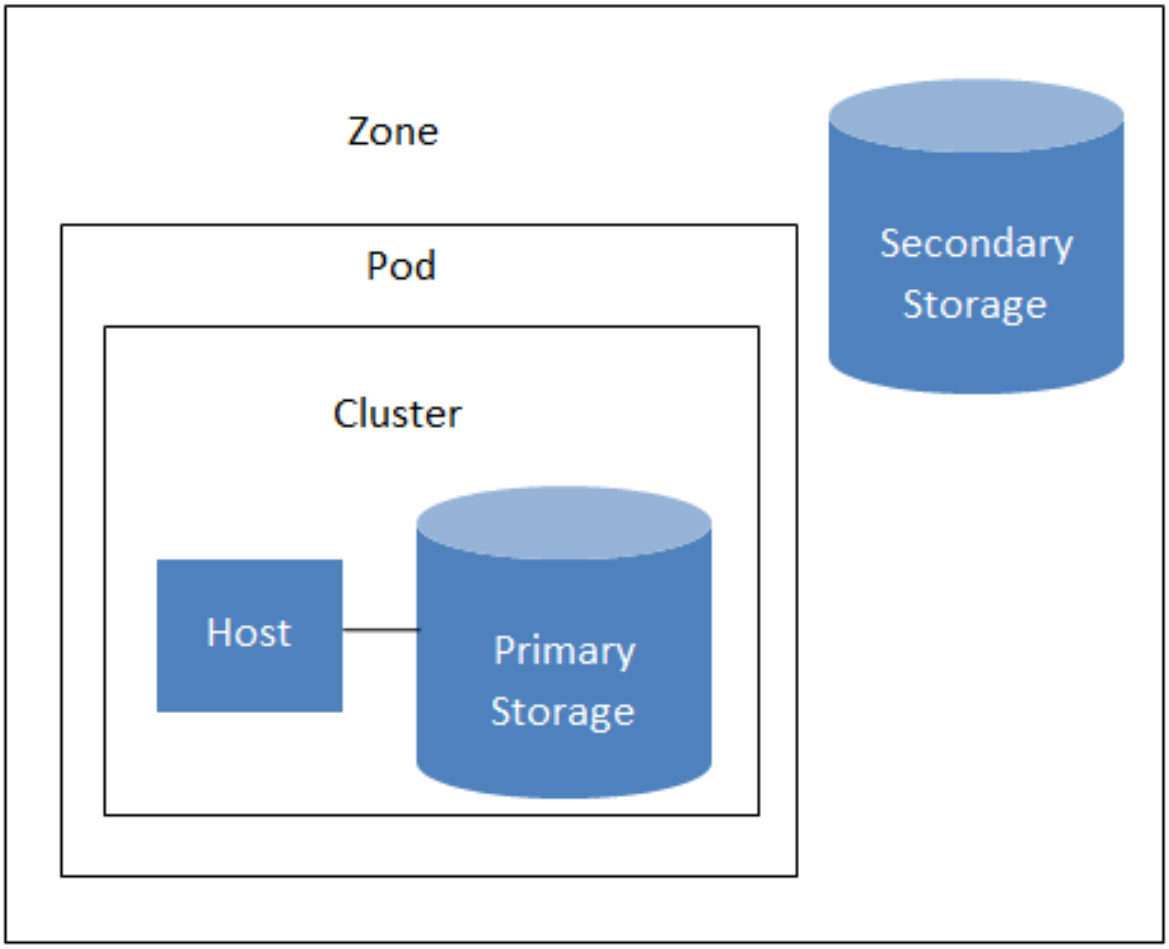
A zone is the second largest organizational unit within a CloudStack deployment. A zone typically corresponds to a single datacenter, although it is permissible to have multiple

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

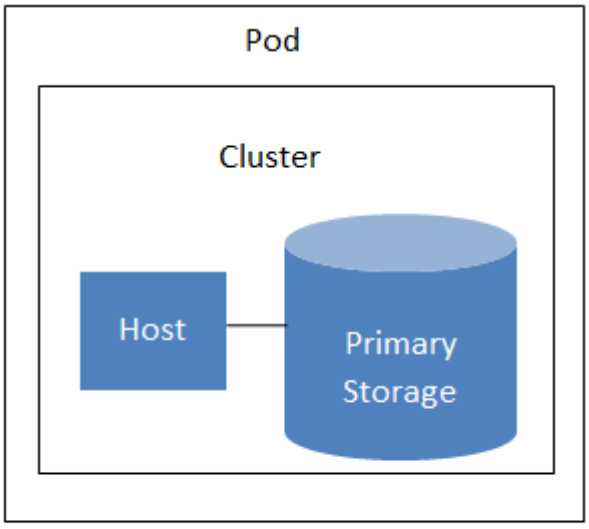
・多少主要儲存裝置及總容量

・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



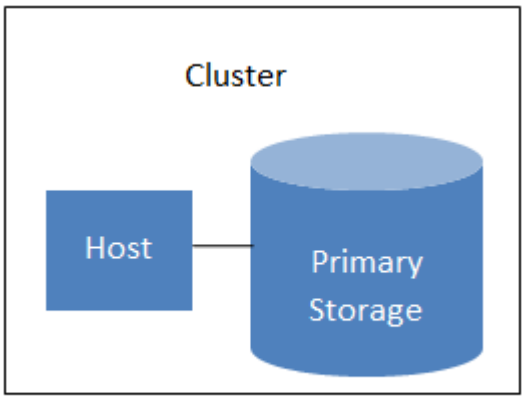
A simple pod

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

從來源建立

官方CloudStack 釋出始終為原始碼的形式，您可以找到"convenience binaries,"，此來源是標準的釋出。此章節會涵蓋取得原始釋出及建立它，如此您就可以使用Maven或建立Debian packages或RPM來部署

注意，直接使用原始碼建立及部署並不是部署IaaS最有效率的方法，但是，我們也會涵蓋建立RPM或是Debian packages的方法

此指示是版本限定的，也就是4.0.x 系列與4.1.x系列的原始碼是不同的

如果您是使用未釋出的CloudStack版本，請參閱INSTALL.md 檔案，它位於此釋出的最上層資料夾

3.1. 取得release

You can download the latest CloudStack release from the Apache CloudStack project download page[1].

Prior releases are available via archive.apache.org as well. See the downloads page for more information on archived releases.

您或許會注意到'Latest release'的幾個連結，檔案的結尾為tar.bz2或是PGP/GPG、MD5和 SHA512檔案

- tar.bz2檔案包含Bzip2-compressed tarball的原始碼
- .asc檔案是分離的加密簽證，可以用來認證release的真實性
- .md5是release的MD5散列，幫助確認下載的正當性
- .sha是release的SHA512散列，幫助確認下載的正當性

3.2. 辨認下載的 release

有很多種機制能檢查下載的release的正當性

3.2.1. 取得KEYS

您需要下載KEYS[2]檔案來啓用GPG簽證認證

您之後需要匯入這些keys:

```
# gpg --import KEYS
```

3.2.2. GPG

CloudStack產品提供分離的GPG簽證，利用以下指令來檢查簽證:

```
$ gpg --verify apache-cloudstack-4.0.0-incubating-src.tar.bz2.asc
```

如果您看到 'Good signature'，那麼這個簽證就是合格的

[1] http://cloudstack.apache.org/downloads.html
[2] http://www.apache.org/dist/incubator/cloudstack/KEYS

3.2.3. MD5

除了加密簽證，CloudStack還有 MD5 checksum可以檢查下載是否符合release，您可以執行以下指令來檢查:

```
$ gpg --print-md MD5 apache-cloudstack-4.0.0-incubating-src.tar.bz2 | diff - apache-cloudstack-4.0.0-incubating-src.tar.bz2.md5
```

成功的話就不會顯示任何東西，如果顯示了一些東西，那麼您產生的hash及從伺服器拿出來的hash就表示不一樣

3.2.4. SHA512

除了MD5 hash，CloudStack還提供了SHA512加密hash來加强認證，您可以使用以下指令來檢查:

```
$ gpg --print-md SHA512 apache-cloudstack-4.0.0-incubating-src.tar.bz2 | diff - apache-cloudstack-4.0.0-incubating-src.tar.bz2.sha
```

成功完成的話，您不會看到任何顯示。如果有東西出現的話，就表示hash不同

3.3. 建立Apache CloudStack的先決條件

建立 CloudStack有許多先決條件，此文件假設Linux系統的編譯器為使用RPM或DEB

您需要至少以下需求來編譯CloudStack

1. Maven (version 3)
2. Java (OpenJDK 1.6 或 Java 7/OpenJDK 1.7)
3. Apache Web Services Common Utilities (ws-commons-util)
4. MySQL
5. MySQLdb (提供 Python database API)
6. Tomcat 6 (非 6.0.35)
7. genisoimage
8. rpmbuild or dpkg-dev

3.4. 解壓縮原始碼

解壓縮 CloudStack釋出相對容易，且可以使用簡單的指令來達成:

```
$ tar -jxvf apache-cloudstack-4.1.0.src.tar.bz2
```

您現在可以移進資料夾:

```
$ cd ./apache-cloudstack-4.1.0-src
```

3.5. 建立DEB packages

除了bootstrap dependencies，您也需要安裝許多其他的dependencies，建議使用Maven 3，目前在12.04.1 LTS無法使用，因此您需要加一個包含Maven 3的PPA repository，執行指令add-apt-repository後，您會被提示繼續，並且會新增一個GPG key

```
        $ sudo apt-get update
        $ sudo apt-get install python-software-properties
        $ sudo add-apt-repository ppa:natecarlson/maven3
        $ sudo apt-get update
        $ sudo apt-get install ant debhelper openjdk-6-jdk tomcat6 libws-commons-util-java genisoimage python-
mysqldb libcommons-codec-java libcommons-httpclient-java liblog4jl.2-java maven3
```

Now that we have resolved the dependencies we can move on to building CloudStack and packaging them into DEBs.

```
        mvn clean install -P developer,systemvm
        $ dpkg-buildpackge -uc -us
```

This command will build seven Debian packages. You should have the following:

・cloudstack-agent_4.1.0_all.deb

・cloudstack-awsapi_4.1.0_all.deb

・cloudstack-cli_4.1.0_all.deb

・cloudstack-common_4.1.0_all.deb

・cloudstack-docs_4.1.0_all.deb

・cloudstack-management_4.1.0_all.deb

・cloudstack-usage_4.1.0_all.deb

3.5.1. 建立APT repo

建立後，您會想要使用HTTP複製它們到服務 packages的系統。您須建立資料夾給packages，然後使用 dpkg-scanpackages來建立Packages.gz，此package包含壓縮檔結構的資訊。最後將repository加到您的系統(s)，讓您可以使用APT安裝packages

第一步，確定您有安裝dpkg-dev package。當您pulled in debhelper時就應該安裝了。但是，如果正在不同系統產生Packages.gz，請確定此系統也有安裝

```
$ sudo apt-get install dpkg-dev
```

下一步，複製DEB到可以服務HTTP的資料夾，我們使用/var/www/cloudstack/repo作為範例，您可以改變

```
            sudo mkdir -p /var/www/cloudstack/repo/binary
            sudo cp *.deb /var/www/cloudstack/repo/binary
            sudo cd /var/www/cloudstack/repo/binary
            sudo dpkg-scanpackages . /dev/null | tee Packages | gzip -9 > Packages.gz
```

Note: Override Files

您可以放心忽略警示

現在您應該有所有的DEB packages 及Packages.gz，在binary資料夾中，並可以使用HTTP。(您或許會想用wget 或 curl來測試)

3.5.2. 使用APT repository設定您的機器

現在我們已經建立repository，您需要設定您的機器來使用APT repository，您可以在/etc/apt/sources.list.d下增加repository file來達到此目的，使用您偏好的編輯器來建立/etc/apt/sources.list.d/cloudstack.list ，並包含此行:

```
deb http://server.url/cloudstack/repo binary ./
```

現在您有repository info，您想要執行其他更新，APT會知道到哪找CloudStack packages

```
$ sudo apt-get update
```

您可以繼續Ubuntu的安裝指南

3.6. 從原始碼建立RPM

在之前提及節 3.3, “建立Apache CloudStack的先決條件”，您需要安裝多個安裝前要求的物件，在此假設您使用CentOS 64-bit或Red Hat Enterprise Linux

```
# yum groupinstall "Development Tools"
```

```
# yum install java-1.6.0-openjdk-devel.x86_64 genisoimage mysql mysql-server ws-commons-util MySQL-python
 tomcat6 createrepo
```

下一步，您需要使用Maven安裝build-time dependencies給CloudStack，我們使用Maven 3，所以您會想grab a Maven 3 tarball[3]並解壓縮到您的home資料夾(或任一位置):

```
$ tar zxvf apache-maven-3.0.4-bin.tar.gz
```

```
$ export PATH=/usr/local/apache-maven-3.0.4//bin:$PATH
```

Maven也需要Java安裝在哪，並預期JAVA_HOME環境變數已設定:

```
$ export JAVA_HOME=/usr/lib/jvm/jre-1.6.0-openjdk.x86_64/
```

確認Maven正確安裝:

```
$ mvn --version
```

[3] http://maven.apache.org/download.cgi

您或許想要確定您的環境變數在登出/重新開機後依舊存在，請確定使用PATH 更新~/.bashrc，及 JAVA_HOME變數

為$PRODUCT；建立RPM相對容易，假設您已經下載原始碼，並解壓縮 tarball 到本地資料夾，幾分鐘後，您將可以產生packages

Packaging已改變

如果您先前為$PRODUCT;建立packages ，您需要小心過程中可能會因為計畫已經改為使用Apache Maven而有相當大的變化，請一定要按照以下步驟執行

3.6.1. 產生RPM

現在，我們已經有要求的物件及原始碼，請您cd到packaging/centos63/資料夾

使用package.sh script產生RPM:

```
$./package.sh
```

此會執行一段時間，最後的packages會在dist/rpmbuild/RPMS/x86_64/

You should see six RPMs in that directory:

- cloudstack-agent-4.1.0.el6.x86_64.rpm
- cloudstack-awsapi-4.1.0.el6.x86_64.rpm
- cloudstack-cli-4.1.0.el6.x86_64.rpm
- cloudstack-common-4.1.0.el6.x86_64.rpm
- cloudstack-management-4.1.0.el6.x86_64.rpm
- cloudstack-usage-4.1.0.el6.x86_64.rpm

Filename Variations

The file names may vary slightly. For instance, if you were to build the RPMs on a Fedora 18 system, you'd see "fc18" instead of "el6" in the filename. (Fedora 18 isn't a supported platform at this time, just providing an example.)

3.6.1.1. 建立yum repo

由於RPM是個很有用的packaging 格式，它通常可以在網路上輕易被Yum repositories使用，下一步為使用最後的 packages建立Yum Repo:

```
$ mkdir -p ~/tmp/repo
```

```
$ cp dist/rpmbuild/RPMS/x86_64/*rpm ~/tmp/repo/
```

```
$ createrepo ~/tmp/repo
```

在~/tmp/repo 的檔案及資料夾現在可以被上傳到網頁伺服器，並作為 yum repository

3.6.1.2. 使用新的yum repository設定您的系統

現在您的 yum repository充滿RPM元資料，我們需要設定需要安裝$PRODUCT;的機器，建立檔案，命名為/etc/yum.repos.d/cloudstack.repo，並有這個資訊：

```
[apache-cloudstack]
name=Apache CloudStack
baseurl=http://webserver.tld/path/to/repo
enabled=1
gpgcheck=0
```

完成此步驟，您即可輕鬆安裝$PRODUCT;到任一機器上

3.7. Building Non-OSS

If you need support for the VMware, NetApp, F5, NetScaler, SRX, or any other non-Open Source Software (nonoss) plugins, you'll need to download a few components on your own and follow a slightly different procedure to build from source.

Why Non-OSS?

Some of the plugins supported by CloudStack cannot be distributed with CloudStack for licensing reasons. In some cases, some of the required libraries/JARs are under a proprietary license. In other cases, the required libraries may be under a license that's not compatible with Apache's licensing guidelines for third-party products[4].

1. To build the Non-OSS plugins, you'll need to have the requisite JARs installed under the deps directory.

   Because these modules require dependencies that can't be distributed with CloudStack you'll need to download them yourself. Links to the most recent dependencies are listed on the How to build on master branch[5] page on the wiki.

2. You may also need to download vhd-util[6], which was removed due to licensing issues. You'll copy vhd-util to the scripts/vm/hypervisor/xenserver/ directory.

3. Once you have all the dependencies copied over, you'll be able to build CloudStack with the nonoss option:

   ```
   $ mvn clean
   ```

[4] http://www.apache.org/legal/resolved.html#category-x
[5] https://cwiki.apache.org/CLOUDSTACK/how-to-build-on-master-branch.html
[6] http://download.cloud.com.s3.amazonaws.com/tools/vhd-util

```
$ mvn install -Dnonoss
```

4. Once you've built CloudStack with the nonoss profile, you can package it using the 節 3.6, “從原始碼建立RPM” or 節 3.5, “建立DEB packages” instructions.

安裝

4.1. 誰該閱讀本手冊

給那些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。

4.2. Overview of Installation Steps

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

・選擇部署架構

・Choosing a Hypervisor: Supported Features

・網路設定

・Storage Setup

・Best Practices

1. Make sure you have the required hardware ready. See 節 4.3, “最低系統需求”
2. Install the Management Server (choose single-node or multi-node). See 節 4.5, “管理伺服器安裝”
3. Log in to the UI. See 章 5, 使用者介面
4. Add a zone. Includes the first pod, cluster, and host. See 節 6.3, “新增Zone”
5. Add more pods (optional). See 節 6.4, “新增Pod”
6. Add more clusters (optional). See 節 6.5, “新增一個Cluster”
7. Add more hosts (optional). See 節 6.6, “增加主機”
8. Add more primary storage (optional). See 節 6.7, “新增Primary Storage”
9. Add more secondary storage (optional). See 節 6.8, “新增次要儲存裝置”
10. Try using the cloud. See 節 6.9, “初始化及測試”

4.3. 最低系統需求

4.3.1. 管理伺服器、資料庫及儲存系統需求

運行Management Server以及MySQL資料庫的實體機器必須滿足以下需求：此機器必須也能提供primary和secondary storage的服務，例如透過本機磁碟或是NFS服務。然而，Management Server也可以運行於虛擬機上。

・作業系統:

  - 推薦： CentOS/RHEL 6.3+ 或 Ubuntu 12.04(.1)
- 64-bit x86 CPU（多核提供更好的效能）
- 記憶體4GB
- 硬碟250 GB（建議500GB，越多容量越大）
- 至少1個NIC
- 固定IP
- hosname指令將會回傳您的主機名稱

4.3.2. 主機/超級監督者 系統需求

主機是雲端服務以訪客VM的形式執行的地方，每台主機須符合以下需求：

- 必須支援HVM（Intel-VT or AMD-V enabled）
- 64-bit x86 CPU（多核提供更好的效能）
- 支援Hardware virtualization
- 記憶體4GB
- 36GB硬碟
- 至少1個NIC
-

> **注意**
>
> 如果主機之前使用DHCP，請確保在原本的DHCP伺服器及CloudStack新增的DHCP路由器間沒有衝突

- 套用在高層管理者軟體的最新hotfix
- 當您配置CloudStack時，所有高層管理者主機的VM都不能是執行狀態
- All hosts within a cluster must be homogeneous. The CPUs must be of the same type, count, and feature flags.

主機還有其他需求，由高層管理者執行。詳見安裝章節最上層的需求表單：

> **警告**
>
> 確定您已執行所有要求以及安裝步驟，高層管理者主機必須已準備使用CloudStack，例如，XenServer的需求表列在 Citrix XenServer安裝之下

- 節 8.1.1，“KVM Hypervisor主機系統需求”

- 節 8.2.1, “XenServer主機系統需求”
- 節 8.3.1, “vSphere主機系統需求”

4.4. 設定package repository

CloudStack僅從官方鏡像原始碼分布，但是CloudStack論壇成員可以建立方便的二進位編碼，讓使用者可以直接安裝Apache CloudStack

If you didn't follow the steps to build your own packages from source in the sections for 節 3.6, “從原始碼建立RPM” or 節 3.5, “建立DEB packages” you may find pre-built DEB and RPM packages for your convenience linked from the downloads[1] page.

注意

這些repositories包含管理伺服器及KVM超級監督者

4.4.1. DEB package repository

您可以使用以下指令增加DEB package repository到您的apt sources。注意，僅Ubuntu 12.04 LTS (precise) packages會建立

使用您管用的編輯器開啓(或新增)/etc/apt/sources.list.d/cloudstack.list，增加論壇提供的repository到檔案中：

```
deb http://cloudstack.apt-get.eu/ubuntu precise 4.0
```

現在將public key加到trusted keys

```
$ wget -O - http://cloudstack.apt-get.eu/release.asc|apt-key add -
```

現在更新您的local apt cache

```
$ apt-get update
```

您的DEB package repository設定完成，可以使用

4.4.2. RPM package repository

有為CloudStack的 RPM package repository，您可以輕鬆安裝在RHEL的系統

如果您不是使用RPM系統，您需要增加Yum repository來安裝CloudStack

Yum repository資訊在/etc/yum.repos.d，您會看到多個.repo檔案，每個都是特別的repository

新增一個CloudStack套件庫，請建立/etc/yum.repos.d/cloudstack.repo檔案，並加入以下內容

```
[cloudstack]
name=cloudstack
baseurl=http://cloudstack.apt-get.eu/rhel/4.0/
```

[1] http://cloudstack.apache.org/downloads.html

```
enabled=1
gpgcheck=0
```

您現在應該能使用Yum安裝 CloudStack

4.5. 管理伺服器安裝

4.5.1. 管理伺服器安裝簡介

此章節教您如何安裝管理伺服器，有兩種安裝方法，取決於您要在雲端架設多少管理伺服器

- 單一管理伺服器節點，MySQL在同一節點
- 多管理伺服器節點，MySQL不同節點

不論何種方法，機器必須符合System Requirements中的需求

警告

為安全考量，請確定公開網路無法存取管理伺服器的port 8096 或 port 8250

安裝管理伺服器的步驟為:

1. 準備作業系統
2. (僅XenServer)下載及安裝vhd-util
3. 安裝第一個管理伺服器
4. 安裝及設定MySQL資料庫
5. 準備NFS Shares
6. 準備及啓動其他管理伺服器(選擇性)
7. 準備系統VM模組

4.5.2. 準備作業系統

使用以下步驟在每個Management Server節點，作業系統必須準備主導Management Server

1. 以root登入作業系統
2. 檢查正確的主機名稱

   ```
   hostname --fqdn
   ```

   This should return a fully qualified hostname such as "management1.lab.example.org". If it does not, edit /etc/hosts so that it does.

3. 請確定機器有連上網際網路

   ```
   ping www.cloudstack.org
   ```

4. 開啓NTP同步時間

注意

您需要NTP來同步雲端伺服器的時間

a. 安裝NTP

```
yum install ntp
```

```
apt-get install openntpd
```

5. 重複以上步驟到每個會安裝Management Server的主機

4.5.3. 在第一台主機安裝管理伺服器

安裝的第一步是將軟體安裝在一個節點上，不管您之後要安裝在幾個主機上

注意

如果您計畫安裝在多個節點上，或是更高的可用性，請先不要進行其他節點，我們會在後面步驟進行

CloudStack管理伺服器可以使用RPM 或 DEB 封包安裝，這些封包取決於您想要管理伺服器執行的所有東西

4.5.3.1. 安裝在CentOS/RHEL

首先，先安裝需要的封包:

```
yum install cloud-client
```

4.5.3.2. 安裝在Ubuntu

```
apt-get install cloud-client
```

4.5.3.3. 下載vhd-util

此步驟僅為安裝超級監督者主機的 XenServer安裝

建立管理伺服器前，請先從vhd-util[2]下載vhd-util

[2] http://download.cloud.com.s3.amazonaws.com/tools/vhd-util

如果管理伺服器為RHEL 或 CentOS，請複製vhd-util到/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver

如果管理伺服器是Ubuntu，複製vhd-util到/usr/lib/cloud/common/scripts/vm/hypervisor/xenserver

4.5.4. 安裝資料庫伺服器

CloudStack管理伺服器使用MySQL資料庫伺服器來儲存資料，當您安裝管理伺服器到一個節點，您可以在本地直接安裝MySQL伺服器，對於安裝多管理伺服器節點，我們假設MySQL資料庫也在不同節點執行

CloudStack已經測試過MySQL 5.1 及 5.5，這些版本皆包含在RHEL/CentOS 及Ubuntu中

4.5.4.1. 在管理伺服器節點安裝資料庫

這個章節描述如何在與Management Server相同的機器上安裝MySQL，這項技術是有意架設數個Management Server節點。如果您需要安裝多個Management Server，您將使用不同的MySQL節點，參見節 4.5.4.1，“在管理伺服器節點安裝資料庫”

1. 從package repository安裝MySQL：

```
yum install mysql-server
```

```
apt-get install mysql-server
```

2. 開啓MySQL設定檔，檔案為/etc/my.cnf或

3. 插入以下幾行到[mysqld]區域

   您可以將這些行數放在 datadir，最大連結欄位應該為350乘以管理伺服器的數量，這個範例假設為一個

注意

對Ubuntu，您可以建立/etc/mysql/conf.d/cloudstack.cnf檔案，並新增這些指令，不要忘了加入[mysqld]在第一行

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

4. 啓動或重新啓動MySQL來使設定生效

   對於RHEL/CentOS，MySQL不會自動啓動，請手動啓動

```
service mysqld start
```

   對於Ubuntu，請重新啓動 MySQL

```
service mysqld restart
```

5. (僅CentOS 及 RHEL, Ubuntu不需要)

警告

對於RHEL and CentOS, MySQL預設沒有 root 密碼, 强烈建議您設定root密碼

執行以下指令强化您的安裝, 您可以所有問題回答"Y"

```
mysql_secure_installation
```

6. CloudStack可以被安全機制阻擋, 像是SELinux, 停用SELinux以便Agent可以正常運作

設定SELinux (RHEL 及 CentOS):

a. 檢查您的機器是否有SELinux, 沒有的話請跳過這一章

對於RHEL 或 CentOS, SELinux是預設啓動的, 您可以用以下來驗證:

```
$ rpm -qa | grep selinux
```

b. 在/etc/selinux/configSELINUX變數設為"permissive", 此舉會使設定在重新開機後維持不變

於RHEL/CentOS

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

改變以下幾行

```
SELINUX=enforcing
```

為:

```
SELINUX=permissive
```

c. 將SELinux設為允許立即啓動, 不用重新開機

```
$ setenforce permissive
```

7. 設定資料庫。以下指令會建立"雲端"資料庫的使用者

- 在dbpassword, 指定雲端使用者的密碼, 您也可以不要設密碼
- 在 deploy-as, 指定使用者名稱及密碼。在以下指令, 假設有root使用者並創建雲端使用者
- (選擇性)對於encryption_type, 您可以使用文件或網路來指定通過資料庫密碼的技術, 預設為: 文件, 詳見 節 4.5.5, “關於密碼及金要加密”

- (選擇性)對於management_server_key，替換在CloudStackproperties file用來編譯機密參數的預設金鑰，預設：password。我們强烈建議您替換成更安全的數值，詳見節 4.5.5，“關於密碼及金要加密”
- (選擇性)對於database_key，替換在CloudStackproperties file用來編譯機密參數的預設金鑰，預設：password。我們强烈建議您替換成更安全的數值，詳見節 4.5.5，“關於密碼及金要加密”
- (選擇性)對於management_server_ip，您可以分開指定cluster管理伺服器節點IP。如果不指定，則為本地IP位址

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

當程式執行完成後，您將會看到類似訊息“Successfully initialized the database.”

8. 如果您在管理伺服器上的同一個機器執行KVM超級監督者，請編輯/etc/sudoers並加入以下行數：

```
Defaults:cloud !requiretty
```

9. 建立好資料庫，您可以結束設定。這個指令會建立iptables、sudoers及啓動管理伺服器

```
# cloudstack-setup-management
```

您會看到 “CloudStack Management Server setup is done.”

4.5.4.2. 在Separate Node安裝資料庫

這個章節描述如何在獨立、從Management Server分離的機器上安裝MySQL，這項技術是有意架設數個Management Server節點。如果您只要安裝一個Management Server，您將使用相同的MySQL節點，參見節 4.5.4.1，“在管理伺服器節點安裝資料庫”

注意

管理伺服器不需要為MySQL使用特定的產品，您可以使用任何作業系統。建議使用相同的產品，詳見節 4.3.1，“管理伺服器、資料庫及儲存系統需求”

1. 從package repository安裝MySQL：

```
yum install mysql-server
```

```
apt-get install mysql-server
```

2. 編輯MySQL系統設定(/etc/my.cnf or /etc/mysql/my.cnf，取決於您的作業系統)並在[mysqld]部分加入以下行列，您可以將這些行列放在datadir下方。max_connections欄位設為350乘以Management Servers的數量，這個例子假設有兩個：

注意

對Ubuntu，您可以建立/etc/mysql/conf.d/cloudstack.cnf檔案，並新增這些指令，不要忘了加入[mysqld]在第一行

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=700
log-bin=mysql-bin
binlog-format = 'ROW'
bind-address = 0.0.0.0
```

3. 啓動或重新啓動MySQL來使設定生效

   對於RHEL/CentOS，MySQL不會自動啓動，請手動啓動

   ```
   service mysqld start
   ```

   對於Ubuntu，請重新啓動 MySQL

   ```
   service mysqld restart
   ```

4. （僅CentOS 及 RHEL，Ubuntu不需要）

   警告

   對於RHEL and CentOS，MySQL預設沒有 root 密碼，强烈建議您設定root密碼

   執行以下指令强化您的安裝，您可以除了"Disallow root login remotely?"外，其他問題回答"Y"。建立資料庫需要遠端登入root

   ```
   mysql_secure_installation
   ```

5. 如果有防火牆，請打開 TCP port 3306。

   對於Ubuntu，有預設防火牆UFW，用這指令開啓埠：

   ```
   ufw allow mysql
   ```

   於RHEL/CentOS：

   a. 編輯 /etc/sysconfig/iptables文件並在 INPUT的一開始加入以下行列

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

b. 請重載iptables rules

```
service iptables restart
```

6. 回到您第一個管理使用者的root

7. 設定資料庫。以下指令會建立雲端資料庫的使用者

- 在dbpassword，指定雲端使用者的密碼，您也可以不要設密碼
- 在 deploy-as，指定使用者名稱及密碼。在以下指令，假設有root使用者並創建雲端使用者
- (選擇性)對於encryption_type，您可以使用文件或網路來指定通過資料庫密碼的技術，預設為:文件，詳見 節 4.5.5，“關於密碼及金要加密”
- (選擇性)對於management_server_key，替換在CloudStackproperties file用來編譯機密參數的預設金鑰，預設：password。我們强烈建議您替換成更安全的數值，詳見About Password and Key Encryption
- (選擇性)對於database_key，替換在CloudStackproperties file用來編譯機密參數的預設金鑰，預設：password。我們强烈建議您替換成更安全的數值，詳見節 4.5.5，“關於密碼及金要加密”
- (選擇性)對於management_server_ip，您可以分開指定cluster管理伺服器節點IP。如果不指定，則為本地IP位址

```
cloudstack-setup-databases cloud:<dbpassword>@<ip address mysql server> \
--deploy-as=root:<password> \
-e <encryption_type> \
-m <management_server_key> \
-k <database_key> \
-i <management_server_ip>
```

當程式執行完成後，您將會看到類似訊息“Successfully initialized the database.”

4.5.5. 關於密碼及金要加密

CloudStack儲存許多重要的密碼及秘密金鑰，這些數值都會自動加密:

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

CloudStack使用 Java Simplified Encryption (JASYPT)程式庫，資料會使用database secret key加密及解密，database secret key存放在 CloudStack的內部性質檔案中。其他加密數值列在上面，像是SSH keys，就放在CloudStack 內部資料庫

當然，database secret key本身不能公開，它必須加密，那麼，CloudStack要如何閱讀? 在管理伺服器啓動時，我們必須從外部提供次要秘密金鑰，此金鑰可以其中一種方法提供：讀檔或由CloudStack 管理者提供。CloudStack 資料庫有個新系統設定可以讓它知道要用哪種方法，如果加密形式為"file," ，則金鑰就存在檔案中；如果為"web," ，則管理者就需要執行工具com.cloud.utils.crypt.EncryptionSecretKeySender，透過已知的通訊埠，將金鑰送到管理伺服器

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

4.5.6. 準備NFS Shares

CloudStack 需要空間來存放主要及次要儲存裝置（見 Cloud Infrastructure Overview)。 這些都可以是NFS shares， 這個章節會教您在加入儲存裝置到CloudStack 前，如何設定NFS shares

替代儲存裝置

NFS並不是primary以及secondary storage的唯一選項。例如，您可以使用Ceph RBD、GlusterFS、iSCSI以及其他儲存技術。儲存技術的選擇將會跟您的Hypervisor選擇有關。

主要及次要儲存裝置的需求詳述於:

- 節 2.6, “About Primary Storage”
- 節 2.7, “About Secondary Storage”

產品常用分離式NFS伺服器來安裝，詳見節 4.5.6.1, “使用”

你也可以使用安裝Management Server的機器作為您的NFS伺服器，這是比較典型的安裝方式，理論上，在大型的佈署環境中也是可行的，請參閱： 節 4.5.6.2, “將管理伺服器用為NFS伺服器” .

4.5.6.1. 使用

這個章節教您如何為NFS伺服器上的次要及(選擇性)主教儲存裝置建立NFS shares，伺服器在不同於管理伺服器的節點執行。

以下指令會依您的作業系統版本不同，會有所不同

警告

(僅KVM)確保您的NFS沒有任何容量掛載

1. 在儲存裝置伺服器，為次要儲存裝置建立NFS share，如果您也建立在主要儲存裝置上，那也請建立次要NFS share。例如:

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

2. 編輯/etc/exports來設定新的資料夾為NFS exports，使用rw,async,no_root_squash來匯出NFS share(s)

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

插入以下幾行

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

3. 輸出 /export資料夾

```
# exportfs -a
```

4. 在管理伺服器為次要儲存裝置建立掛載點，例如:

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

5. 掛載次要儲存裝置，並取代範例NFS伺服器名稱及路徑。

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

4.5.6.2. 將管理伺服器用為NFS伺服器

這個章節會教您如何使用管理伺服器來為同意節點的主要及次要儲存裝置設定NFS分享。這是個基本的安裝，但是技術上能夠有更大的擴充空間。在此假設您指少有16TB的空間

以下指令會依您的作業系統版本不同，會有所不同

1. 在RHEL/CentOS系統，您需要安裝 nfs-utils ：

```
$ sudo yum install nfs-utils
```

2. 在管理伺服器的主機上建立兩個資料夾，這兩個資料夾之後會給主要及次要儲存裝置使用，例如:

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

3. 編輯/etc/exports來設定新的資料夾為NFS exports，使用rw,async,no_root_squash來匯出NFS share(s)

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

插入以下幾行

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

4. 輸出 /export資料夾

```
# exportfs -a
```

5. 編輯/etc/sysconfig/nfs檔案

```
# vi /etc/sysconfig/nfs
```

取消下列程式碼註解:

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

6. 編輯/etc/sysconfig/iptables檔案

```
# vi /etc/sysconfig/iptables
```

加入以下行數到INPUT chain的開頭, <NETWORK>是您之後會使用的網路:

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

7. 執行以下指令:

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

8. 如果客戶及伺服器間是使用NFS v4 communication, 請加入您的domain到 /etc/idmapd.conf, 超級監督者主機及管理伺服器都需要

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

移除 idmapd.conf中Domain那一行一開始的所有"#", 並換成您的domain, 以下範例為company.com

```
Domain = company.com
```

9. 重新開啓管理伺服器主機

兩個稱為/export/primary and /export/secondary的NFS shares就建立好了

10. 我們推薦您先測試, 確定前幾步有做對

a. 登入超級監督者主機

b. 確定NFS 及 rpcbind有執行，指令會依您的作業系統不同而不同，例如：

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

c. 回到超級監督者主機，嘗試掛載/export資料夾，例如(換成您的管理伺服器名稱)：

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

4.5.7. 準備及啓動其他管理伺服器

對於次要及後續的管理伺服器，您需要安裝管理伺服器軟體。連結到資料庫，然後為伺服器建立作業系統

1. 執行節 4.5.2, “準備作業系統”及節 3.6, “從原始碼建立RPM”或節 3.5, “建立DEB packages”步驟
2. 此步驟僅為安裝超級監督者主機的 XenServer安裝

   從vhd-util[3]下載vhd-util

   如果管理伺服器為RHEL 或 CentOS，請複製vhd-util到/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver

   如果管理伺服器是Ubuntu，複製vhd-util到/usr/lib/cloud/common/scripts/vm/hypervisor/xenserver/vhd-util
3. 確定必要的服務已經啓動

   ```
   # service rpcbind start
   # service nfs start
   # chkconfig nfs on
   # chkconfig rpcbind on
   ```
4. 設定資料庫客戶，注意，請忽略--deploy-as變數(更多細節，詳見節 4.5.4.2, “在Separate Node安裝資料庫”)

   ```
   # cloudstack-setup-databases cloud:dbpassword@dbhost -e encryption_type -m management_server_key -
   k database_key -i management_server_ip
   ```
5. 設定作業系統及啓動管理伺服器:

[3] http://download.cloud.com.s3.amazonaws.com/tools/vhd-util

```
# cloudstack-setup-management
```

此節點的管理伺服器應該會開始執行

6. 重複以上步驟到其他管理伺服器

7. Be sure to configure a load balancer for the Management Servers. See 節 12.6, “Management Server Load Balancing”.

4.5.8. 準備系統VM模組

次要儲存裝置必須種植使用CloudStack系統VM的模組

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

1. 在管理伺服器執行一至多個以下cloud-install-sys-tmplt指令來取得系統VM模組，為每種超級監督者類型執行一遍

   如果次要儲存裝置掛載不適命名為/mnt/secondary，替換成您自己的名稱

   如果您設定 CloudStack 資料庫加密為"web"，您需要增加欄位-s <management-server-secret-key>，詳見節 4.5.5, “關於密碼及金要加密”

   此過程需要5GB的空間，及30分鐘的時間

   - 對於 XenServer:

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

   - 對於 vSphere:

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

   - 對於KVM:

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

   在Ubuntu，使用以下路徑:

   ```
   # /usr/lib/cloud/common/scripts/storage/secondary/cloud-install-sys-tmplt
   ```

2. 如果您是使用分離NFS伺服器，執行此步驟；如果您是使用管理伺服器為NFS伺服器，請注意，您"不能"執行此步驟

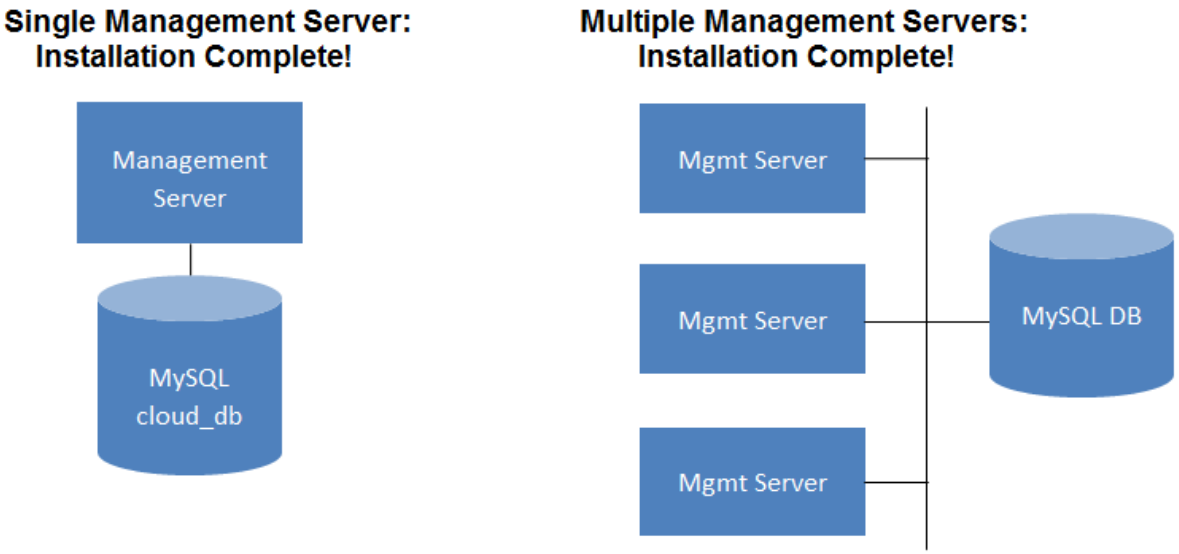
   當程式執行完畢，卸載次要儲存裝置，必移除建立的資料夾

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

3. 重複以上步驟到每個次要儲存伺服器

4.5.9. 安裝完成！下一步

恭喜！您已完成安裝CloudStack管理伺服器及用來保存系統資料的資料庫



您接下來要做甚麼?

- 即使沒有增加任何雲端基礎架構，您依舊可以執行使用者介面來體驗雲端，讓您了解如何與CloudStack互動，詳見Log In to the UI
- 當您準備好了，加入雲端基礎架構並嘗試執行一些虛擬機器，如此您可以知道CloudStack 如何管理，詳見Provision Your Cloud Infrastructure

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

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.

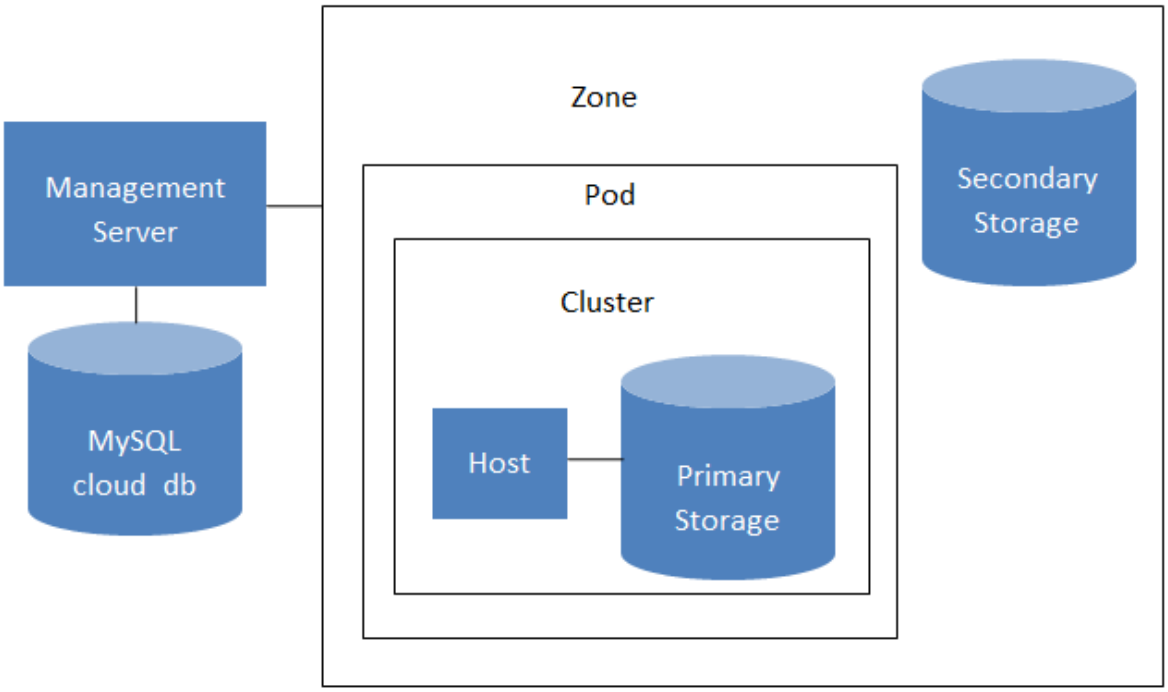
6.1. Overview of Provisioning Steps

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 6.2, “Adding Regions (optional)”.
2. Add a zone to the region. See 節 6.3, “新增Zone”.
3. Add more pods to the zone (optional). See 節 6.4, “新增Pod”.
4. Add more clusters to the pod (optional). See 節 6.5, “新增一個Cluster”.
5. Add more hosts to the cluster (optional). See 節 6.6, “增加主機”.
6. Add primary storage to the cluster. See 節 6.7, “新增Primary Storage”.
7. Add secondary storage to the zone. See 節 6.8, “新增次要儲存裝置”.
8. Initialize and test the new cloud. See 節 6.9, “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

6.2. 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” .

6.2.1. 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
```

6.2.2. 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.

6.2.3. 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.

6.2.4. 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
```

6.3. 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 6.3.1，“基礎區域設定”

   - 節 6.3.2，“進階Zone設定”

6.3.1. 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

6.3.2. 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.

6.4. 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

6.5. 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

6.5.1. 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

6.5.2. 加入叢集: vSphere

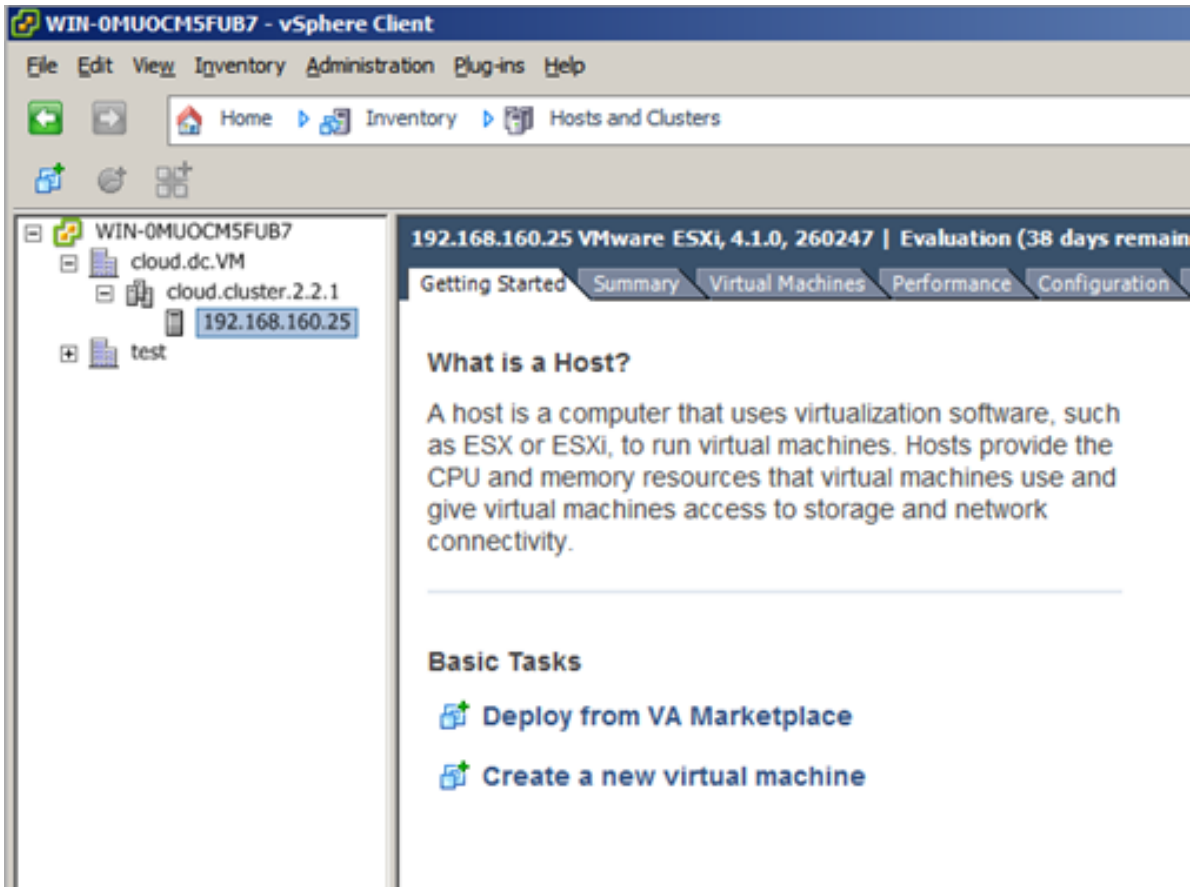
藉由結合vCenter及CloudStack管理介面, 可以完成vSphere主機管理, CloudStack需要所有主機都必須在 CloudStack叢集中, 但是叢集有可能只包含一個主機。身為管理者, 您必須決定叢集是使用一個還多個主機, 多主機叢集可以操作live migration等功能, 叢集要求像 NFS or iSCSI的分享儲存

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

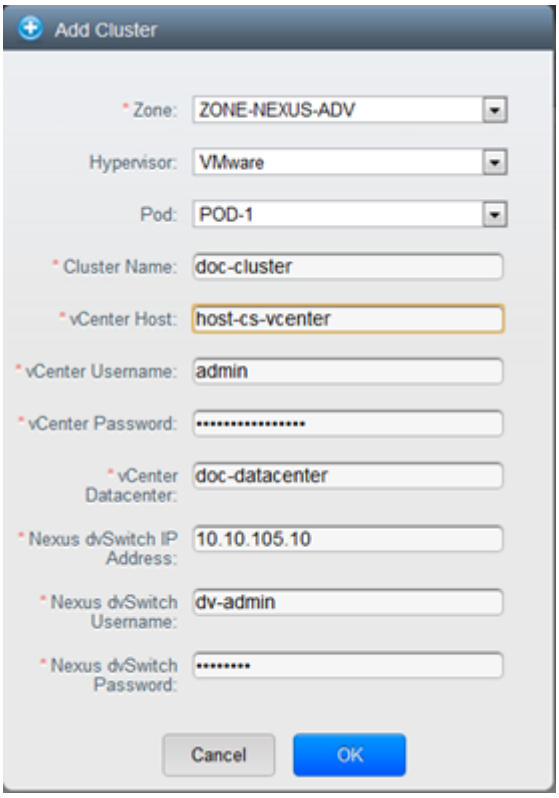
5. 按 View Clusters

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

6.6. 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 6.6.1, “(XenServer 或 KVM)增加主機”
   - 節 6.6.2, “Adding a Host (vSphere)”

6.6.1. (XenServer 或 KVM)增加主機

XenServer 及 KVM主機可以隨時加到叢集

6.6.1.1. 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

6.6.1.1.1. 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
```

6.6.1.1.2. 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

6.6.1.2. 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

6.6.2. 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.

6.7. 新增Primary Storage

6.7.1. 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

6.7.2. 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

6.8. 新增次要儲存裝置

6.8.1. 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

6.8.2. 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 6.3，“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 節 4.5.6，“準備NFS Shares”.
3. 確定您已在管理伺服器安裝時，準備了系統VM模組See 節 4.5.8，“準備系統VM模組”.
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 6.3，“新增Zone”

6.9. 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

Global Configuration Parameters

7.1. 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

7.2. 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.

超級監督者安裝流程

8.1. KVM超級監督者主機安裝

8.1.1. KVM Hypervisor主機系統需求

KVM包含很多種Linux作業系統，雖然您並不需要執行這些產品，但建議以下：

・CentOS / RHEL: 6.3

・Ubuntu: 12.04(.1)

KVM hypervisors最主要的要求是libvirt 和 Qemu的版本，不論是哪種Linux系統，請確保有達到以下要求：

・libvirt: 0.9.4或更高

・Qemu/KVM: 1.0 或更高

在CloudStack的預設橋接器是Linux原生的橋接器(bridge module)，CloudStack 包含了能運作 OpenVswitch的選項，需求表列於下

・libvirt: 0.9.11 或更高

・openvswitch: 1.7.1 或更高

除此之外，以下硬體需求：

・在單一個cluster中，所有主機必須是同一產品版本

・同一cluster內的主機都必須是同質的，CPU的形式、數量及特色旗標都必須一樣

・必須支援HVM (Intel-VT or AMD-V enabled)

・64-bit x86 CPU (多核提供更好的效能)

・記憶體4GB

・至少1個NIC

・當您配置CloudStack時，所有高層管理者主機的VM都不能是執行狀態

8.1.2. KVM 安裝簡介

如果您想要用 Linux Kernel Virtual Machine (KVM) hypervisor 來執行來賓VM，在主機(一至多個)上安裝KVM。這章節的資料並不是複製KVM安裝文件，而是提供CloudStack需要的特定步驟來準備一個以CloudStack作業的KVM主機

警告

在繼續前，請先確認您的版本是最新版

警告

如果您的主機不是由CloudStack所控制，不建議執行服務

安裝KVM Hypervisor Host的步驟為:

1. 準備作業系統
2. 安裝及設定libvirt
3. 設定Security Policies (AppArmor and SELinux)
4. 安裝及設定 Agent

8.1.3. 準備作業系統

作業系統必須準備接管CloudStack Agent並執行 KVM instances

1. 以root登入作業系統
2. 檢查正確的主機名稱

```
$ hostname --fqdn
```

   應該會回復正確的主機名稱如 "kvm1.lab.example.org"，如果沒有，編輯/etc/hosts

3. 請確定機器有連上網際網路

```
$ ping www.cloudstack.org
```

4. 開啓NTP同步時間

注意

您需要NTP來同步雲端伺服器的時間，不同步的時間會導致不可預期的問題

   a. 安裝NTP

```
$ yum install ntp
```

```
$ apt-get install openntpd
```

5. 為每個超級監督者主機重複以上步驟

8.1.4. 安裝及設定 Agent

使用Agent來管理CloudStack主機上的KVM instances。Agent 與管理伺服器及控制所有instances的主機溝通

首先，我們開始安裝

於RHEL/CentOS

```
$ yum install cloudstack-agent
```

於Ubuntu

```
$ apt-get install cloudstack-agent
```

現在，主機已經可以被加到cluster，在後面章節會提及，詳見節 6.6，“增加主機”。建議您！在加入主機之前，先繼續閱讀文件。

8.1.5. 安裝及設定libvirt

CloudStack uses libvirt for managing virtual machines. Therefore it is vital that libvirt is configured correctly. Libvirt is a dependency of cloudstack-agent and should already be installed.

1. 為了具備live migration的能力 ,libviry必須傾聽不安全的TCP連線，我們也必須關閉libvirt的多重DNS廣播，這些設定均在/etc/libvirt/libvirtd.conf檔案中可以找到

   Set the following parameters:

   ```
   listen_tls = 0
   ```

   ```
   listen_tcp = 1
   ```

   ```
   tcp_port = "16509"
   ```

   ```
   auth_tcp = "none"
   ```

   ```
   mdns_adv = 0
   ```

2. 於libvirtd.conf中開啓"listen_tcp"是不夠的，我們仍必須修改以下參數

   於RHEL/CentOS 請修改 /etc/sysconfig/libvirtd:

   取消下列程式碼註解

   ```
   #LIBVIRTD_ARGS="--listen"
   ```

   於Ubuntu請修改 /etc/init/libvirt-bin.conf

   修改以下數行(檔案尾端)

   ```
   exec /usr/sbin/libvirtd -d
   ```

為(添加-l參數)

```
exec /usr/sbin/libvirtd -d -l
```

3. 重新啓動libvirt

於RHEL/CentOS

```
$ service libvirtd restart
```

於Ubuntu

```
$ service libvirt-bin restart
```

8.1.6. 設定 Security Policies

CloudStack可以被安全機制阻擋，像是AppArmor及 SELinux，停用安全機制以便Agent可以正常運作

1. 設定SELinux (RHEL 及 CentOS)：

   a. 檢查您的機器是否有SELinux，沒有的話請跳過這一章

   對於RHEL 或 CentOS，SELinux是預設啓動的，您可以用以下來驗證：

   ```
   $ rpm -qa | grep selinux
   ```

   b. 在/etc/selinux/configSELINUX變數設為"permissive"，此舉會使設定在重新開機後維持不變

   於RHEL/CentOS

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

   改變以下幾行

   ```
   SELINUX=enforcing
   ```

   為

   ```
   SELINUX=permissive
   ```

   c. 將SELinux設為允許立即啓動，不用重新開機

   ```
   $ setenforce permissive
   ```

2. 設定 Apparmor (Ubuntu)

   a. 檢查您的機器是否有AppArmor，沒有的話請跳過這一章

   對於Ubuntu，AppArmor是預設啓動的，您可以用以下來驗證：

   ```
   $ dpkg --list 'apparmor'
   ```

b. 為 libvirt停用AppArmor profiles

```
$ ln -s /etc/apparmor.d/usr.sbin.libvirtd /etc/apparmor.d/disable/
```

```
$ ln -s /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper /etc/apparmor.d/disable/
```

```
$ apparmor_parser -R /etc/apparmor.d/usr.sbin.libvirtd
```

```
$ apparmor_parser -R /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper
```

8.1.7. 設定網路橋接器

警告

此章節非常重要，請完整閱讀

注意

此章節詳細描述如何使用Linux本基設定橋接器，如果您想使用 OpenVswitch來設定，請看下一章節

為了轉送流量到您的instances，您需要只少兩個橋接器：public 及 private

預設橋接器稱為 cloudbr0及cloudbr1，您需要確定每個超級監督者都能使用

最重要的因素為，您需要在所有超級監督者都是相同的設定

8.1.7.1. 網路範例

有很多種方法可以設定網路，在 Basic networking mode，您需要兩個(V)LAN，一個給私人網路，另一個給公開網路

假設超級監督者有一個網路卡（eth0），附有三條VLAN:

1. VLAN 100給超級監督者管理用
2. VLAN 200給instances的公開網路（cloudbr0）
3. VLAN 300給instances的私人網路(cloudbr1)

在VLAN 100，我們給予超級監督者IP位址192.168.42.11/24，閘道為192.168.42.1

注意

超級監督者及管理伺服器不需要再同一個子網路!

8.1.7.2. 設定網路橋接器

取決於您的產品，設定會不同，以下為RHEL/CentOS 及Ubuntu的範例

注意

目標為建立兩個橋接器，稱為 'cloudbr0' 及 'cloudbr1'，但這些應只用為指引，確切的設定取決於您的網路設計

8.1.7.2.1. 設定於RHEL/CentOS

在 libvirt 安裝時，需要的封包都已安裝，我們可以進行到設定網路

先設定eth0

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Make sure it looks similar to:

```
DEVICE=eth0
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=Ethernet
```

現在，設定三條VLAN介面:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0.100
```

```
DEVICE=eth0.100
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=Ethernet
VLAN=yes
IPADDR=192.168.42.11
GATEWAY=192.168.42.1
NETMASK=255.255.255.0
```

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0.200
```

```
DEVICE=eth0.200
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
```

```
BOOTPROTO=none
TYPE=Ethernet
VLAN=yes
BRIDGE=cloudbr0
```

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0.300
```

```
DEVICE=eth0.300
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=Ethernet
VLAN=yes
BRIDGE=cloudbr1
```

現在將橋接器加到VLAN上

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr0
```

Now we just configure it is a plain bridge without an IP-Address

```
DEVICE=cloudbr0
TYPE=Bridge
ONBOOT=yes
BOOTPROTO=none
IPV6INIT=no
IPV6_AUTOCONF=no
DELAY=5
STP=yes
```

在cloudbr1做相同的設定

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr1
```

```
DEVICE=cloudbr1
TYPE=Bridge
ONBOOT=yes
BOOTPROTO=none
IPV6INIT=no
IPV6_AUTOCONF=no
DELAY=5
STP=yes
```

建議您在看到所有東西都正常運作後再開機

警告

請確定替代方案，像是IPMI 或 ILO，可以達到您的機器，以免您設定錯誤而導致網路停止運作

8.1.7.2.2. 設定於Ubuntu

在 libvirt 安裝時，需要的封包都已安裝，我們可以直接進行設定網路

```
vi /etc/network/interfaces
```

修改介面檔案為:

```
auto lo
iface lo inet loopback

# The primary network interface
auto eth0.100
iface eth0.100 inet static
    address 192.168.42.11
    netmask 255.255.255.240
    gateway 192.168.42.1
    dns-nameservers 8.8.8.8 8.8.4.4
    dns-domain lab.example.org

# Public network
auto cloudbr0
iface cloudbr0 inet manual
    bridge_ports eth0.200
    bridge_fd 5
    bridge_stp off
    bridge_maxwait 1

# Private network
auto cloudbr1
iface cloudbr1 inet manual
    bridge_ports eth0.300
    bridge_fd 5
    bridge_stp off
    bridge_maxwait 1
```

建議您在看到所有東西都正常運作後再開機

警告

請確定替代方案，像是IPMI 或 ILO，可以達到您的機器，以免您設定錯誤而導致網路停止運作

8.1.8. Configure the network using OpenVswitch

警告

此章節非常重要，請完整閱讀

為了轉送流量到您的instances，您需要只少兩個橋接器：public 及 private

預設橋接器稱為 cloudbr0及cloudbr1，您需要確定每個超級監督者都能使用

最重要的因素為，您需要在所有超級監督者都是相同的設定

8.1.8.1. Preparing

To make sure that the native bridge module will not interfere with openvswitch the bridge module should be added to the blacklist. See the modprobe documentation for your

distribution on where to find the blacklist. Make sure the module is not loaded either by rebooting or executing rmmod bridge before executing next steps.

The network configurations below depend on the ifup-ovs and ifdown-ovs scripts which are part of the openvswitch installation. They should be installed in /etc/sysconfig/network-scripts/

8.1.8.2. 網路範例

有很多種方法可以設定網路，在 Basic networking mode，您需要兩個(V)LAN，一個給私人網路，另一個給公開網路

假設超級監督者有一個網路卡（eth0），附有三條VLAN:

1. VLAN 100給超級監督者管理用

2. VLAN 200給instances的公開網路（cloudbr0）

3. VLAN 300給instances的私人網路(cloudbr1)

在VLAN 100，我們給予超級監督者IP位址192.168.42.11/24，閘道為192.168.42.1

注意

超級監督者及管理伺服器不需要再同一個子網路！

8.1.8.3. 設定網路橋接器

It depends on the distribution you are using how to configure these, below you'll find examples for RHEL/CentOS.

注意

The goal is to have three bridges called 'mgmt0', 'cloudbr0' and 'cloudbr1' after this section. This should be used as a guideline only. The exact configuration will depend on your network layout.

8.1.8.3.1. Configure OpenVswitch

The network interfaces using OpenVswitch are created using the ovs-vsctl command. This command will configure the interfaces and persist them to the OpenVswitch database.

First we create a main bridge connected to the eth0 interface. Next we create three fake bridges, each connected to a specific vlan tag.

```
# ovs-vsctl add-br cloudbr
# ovs-vsctl add-port cloudbr eth0
# ovs-vsctl set port cloudbr trunks=100,200,300
# ovs-vsctl add-br mgmt0 cloudbr 100
# ovs-vsctl add-br cloudbr0 cloudbr 200
# ovs-vsctl add-br cloudbr1 cloudbr 300
```

8.1.8.3.2. 設定於RHEL/CentOS

The required packages were installed when openvswitch and libvirt were installed, we can proceed to configuring the network.

先設定eth0

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Make sure it looks similar to:

```
DEVICE=eth0
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=Ethernet
```

We have to configure the base bridge with the trunk.

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr
```

```
DEVICE=cloudbr
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
DEVICETYPE=ovs
TYPE=OVSBridge
```

We now have to configure the three VLAN bridges:

```
vi /etc/sysconfig/network-scripts/ifcfg-mgmt0
```

```
DEVICE=mgmt0
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=static
DEVICETYPE=ovs
TYPE=OVSBridge
IPADDR=192.168.42.11
GATEWAY=192.168.42.1
NETMASK=255.255.255.0
```

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr0
```

```
DEVICE=cloudbr0
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
DEVICETYPE=ovs
TYPE=OVSBridge
```

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr1
```

```
DEVICE=cloudbr1
ONBOOT=yes
```

```
HOTPLUG=no
BOOTPROTO=none
TYPE=OVSBridge
DEVICETYPE=ovs
```

建議您在看到所有東西都正常運作後再開機

警告

請確定替代方案，像是IPMI 或 ILO，可以達到您的機器，以免您設定錯誤而導致網路停止運作

8.1.9. 設定防火牆

超級監督者需要能與其他監督者通信，以及管理伺服器必須能接觸超級監督者

請開啓TCP通訊埠(如果您使用防火牆)：

1. 22 (SSH)
2. 1798
3. 16509 (libvirt)
4. 5900 - 6100 (VNC consoles)
5. 49152 - 49216 (libvirt live migration)

取決於您的防火牆，開啓通訊埠的方法會不同，以下為RHEL/CentOS 及Ubuntu的範例

8.1.9.1. 於RHEL/CentOS:

RHEL 及 CentOS使用IP對照表，您可以執行以下IP對照表指令來開啓額外的通訊埠：

```
$ iptables -I INPUT -p tcp -m tcp --dport 22 -j ACCEPT
```

```
$ iptables -I INPUT -p tcp -m tcp --dport 1798 -j ACCEPT
```

```
$ iptables -I INPUT -p tcp -m tcp --dport 16509 -j ACCEPT
```

```
$ iptables -I INPUT -p tcp -m tcp --dport 5900:6100 -j ACCEPT
```

```
$ iptables -I INPUT -p tcp -m tcp --dport 49152:49216 -j ACCEPT
```

這些IP對照表設定再重新開機後會消失，所以必須先儲存

```
$ iptables-save > /etc/sysconfig/iptables
```

8.1.9.2. 於Ubuntu

預設防火牆為UFW(Uncomplicated FireWall)，是個Python環繞在IP對照表四周

執行以下指令來開啓通訊埠：

```
$ ufw allow proto tcp from any to any port 22
```

```
$ ufw allow proto tcp from any to any port 1798
```

```
$ ufw allow proto tcp from any to any port 16509
```

```
$ ufw allow proto tcp from any to any port 5900:6100
```

```
$ ufw allow proto tcp from any to any port 49152:49216
```

注意

預設UFW是停用的，執行這些指令並不會啓用防火牆

8.1.10. 將主機加到CloudStack

現在，主機已經可以被加到cluster，在後面章節會提及，詳見節 6.6，“增加主機”。建議您！在加入主機之前，先繼續閱讀文件。

8.2. CloudStack的Citrix XenServer安裝

如果您使用 Citrix XenServer hypervisor執行訪客虛擬機器，請安裝XenServer 6.0 或 XenServer 6.0.2在雲端主機(s)上。執行以下步驟來初始化安裝，如果您想更新 XenServer，請參照 節 8.2.11，“更新XenServer版本”

8.2.1. XenServer主機系統需求

- 主機必須相容以下其中一個，詳見Citrix Hardware Compatibility Guide: http://hcl.xensource.com
  - XenServer 5.6 SP2
  - XenServer 6.0
  - XenServer 6.0.2
- 如果您是使用舊主機，您需要重安裝Citrix XenServer
- 必須支援HVM（Intel-VT or AMD-V enabled）
- 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
- All hosts within a cluster must be homogeneous. The CPUs must be of the same type, count, and feature flags.
- 必須支援HVM（Intel-VT or AMD-V enabled）
- 64-bit x86 CPU（多核提供更好的效能）

- 支援Hardware virtualization
- 記憶體4GB
- 36GB硬碟
- 至少1個NIC
- 固定IP
- 當您配置CloudStack時，所有高層管理者主機的VM都不能是執行狀態

警告

缺少最新的hotfixes會導致資料毀損及VM錯誤

8.2.2. XenServer安裝步驟

1. 從https://www.citrix.com/English/ss/downloads/，為您的CloudStack 下載適當的XenServer版本(詳見節 8.2.1, “XenServer主機系統需求”)，請使用 Citrix XenServer Installation Guide 安裝
2. 安裝後，將執行以下設定，這些設定在接下來的章節做描述:

必要的	非必要的
節 8.2.3, “設定XenServer dom0記憶體”	節 8.2.7, “安裝CloudStack XenServer Support Package (CSP)”
節 8.2.4, “使用者名稱與密碼”	若不是使用NFS、iSCSI或本地硬碟，請建立SR。詳見節 8.2.8, “XenServer主要儲存裝置設定”
節 8.2.5, “時間同步”	節 8.2.9, “XenServer iSCSI 多通道設定(選擇性)”
節 8.2.6.1, “取得及安裝授權”	節 8.2.10, “XenServer實體網路設定”

8.2.3. 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http://support.citrix.com/article/CTX126531，此文章為 XenServer 5.6版本，但適用6.0版

8.2.4. 使用者名稱與密碼

所有叢集電腦中的XenServers必須與CloudStack設定的使用者名稱及密碼一致

8.2.5. 時間同步

主機必須使用NTP，所有同槽的主機都必須是同一時間

1. 安裝NTP

```
# yum install ntp
```

2. 編輯NTP設定檔，將檔案指向 NTP伺服器

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

在此檔案用您想要使用的NTP伺服器來新增一至多個伺服器，例如：

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

3. 重新啓動NTP客戶端

```
# service ntpd restart
```

4. 確定NTP有重新啓動

```
# chkconfig ntpd on
```

8.2.6. 授權

Citrix XenServer免費版本提供30天的試用期，您可以選擇安裝免費授權或是跳過這一步，如果您跳過這一步，您之後啓動時仍會需要安裝此授權

8.2.6.1. 取得及安裝授權

如果您選擇立即安裝授權，您會需要使用 XenCenter取得及啓動授權

1. 在XenCenter，選擇Tools > License manager
2. 選擇您的 XenServer，點選Activate Free XenServer
3. 取得授權

您可以使用XenCenter或xe 指令工具來安裝授權

8.2.7. 安裝CloudStack XenServer Support Package (CSP)

(選擇性)

想要在XenServer啓用security groups、彈性負載平衡及彈性IP，請下載及安裝 CloudStack XenServer Support Package (CSP)。安裝後執行以下額外步驟到每一台XenServer主機

1. 從以下其中一個連結下載CSP軟體到XenServer 主機：

   對於 XenServer 6.0.2：

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

   對於XenServer 5.6 SP2：

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

   對於XenServer 6.0：

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

2. 解壓縮檔案:

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

3. 執行以下程式碼:

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

4. 如果 XenServer 主機是使用基礎網路的zone的一部分，關閉Open vSwitch (OVS):

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

   如果有提示，請重新啓動

XenServer主機現在可以加進CloudStack

8.2.8. XenServer主要儲存裝置設定

CloudStack本身支援 NFS、 iSCSI及本地儲存裝置，如果您使用其中一種的儲存類型，則不需要新增 XenServer Storage Repository ("SR")

如果您想要使用像FiberChannel等來連結儲存裝置，您需要自行建立SR。執行以下步驟來完成建立。如果您使用XenServer群的主機，請在主節點操作；如果您是使用非叢集電腦的XenServer，則在XenServer操作

1. 接上FiberChannel電纜到每台叢集電腦的主機及FiberChannel儲存裝置主機

2. 重新掃描SCSI匯流排，請選其中一種方法來執行HBA掃描，使用指令或 XenCenter

```
# scsi-rescan
```

3. 重複2步驟到每台主機

4. 請確定您有看到新的SCSi硬碟

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

   結果應該會像 (scsi-<scsiID>)，但檔案的名稱會不同:

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

5. 重複4步驟到每台主機

6. 在儲存裝置伺服器執行此指令來取得新SR的ID

```
# uuidgen
```

   結果應該會像這樣，但ID會不同:

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

7. 建立 FiberChannel SR，在name-label輸入剛得到的ID

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

此指令會回復SR一組唯一的ID，像是以下範例(您的ID會不同)：

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

8. 使用以下指令來建立人類可讀的描述，在 uuid使用剛剛取得的SR ID，在name-description寫下描述

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

記下這些數值，您在增加此儲存裝置到 CloudStack時會用到（詳見 節 6.7，“新增Primary Storage”），在Add Primary Storage對話框中的 Protocol，選擇PreSetup。在SR Name-Label，輸入之前設定的name-label（此範例為e6849e96-86c3-4f2c-8fcc-350cc711be3d）

9. (選擇性)如果您想在 FiberChannel SAN啓用多通道I/O，請參閱SAN vendor提供的文件

8.2.9. XenServer iSCSI 多通道設定(選擇性)

設定Citrix XenServer的儲存裝置庫時，您可以啓用多通道I/O，透過減少硬體來提供更高的可靠性。使用支援 Citrix伺服器的SAN solution來啓用，並按照Citrix文件步驟來設定，連結如下：

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

您也可以詢問SAN vendor建議

記下這些數值，您在增加此儲存裝置到 CloudStack時會用到（詳見 節 6.7，“新增Primary Storage”），在Add Primary Storage對話框中的 Protocol，選擇PreSetup。在SR Name-Label，輸入之前建立SR的name-label

如果您遇到問題，請向SAN的客服反應，如果他們無法解決，請參閱 Contacting Support

8.2.10. XenServer實體網路設定

安裝好 XenServer後，您還需要一些網路設定。在此安裝步驟，您應該已經有計畫了，像是主機應該有甚麼NICs，及每種NIC使用那些流量。NIC對您的計畫是必須考慮的

如果您計畫使用NIC連結，所有叢集電腦主機的NIC都必須相同，例如，如果eth0為其中一台主機的私人連結，則eth0就必須是叢集電腦所有主機的私人連結

指定給管理網路介面的IP位址必須固定，您可以設定在主機上或使用固定DHCP取得

CloudStack設定多種類型的網路流量可以在 XenServer主機上使用不同的NIC或連結。您可以控制及使用 XenServer網路名稱標題來提供管理伺服器的輸入端，名稱標題位於實體介面或連結上，可以在CloudStack設定。在簡單的例子不用使用名稱標題

8.2.10.1. 使用Dedicated NIC設定公開網路(選擇性)

CloudStack支援使用次要NIC(或是NIC鍵結對，節 8.2.10.4，“NIC 連結 (選擇性)”)，對於公開網路，如果連結未使用，公開網路可以在任一NIC，或是在叢集電腦主機的不同NIC。例如，公開網路可以

在節點A的eth0及節點B的eth1。但是XenServer name-label 必須是一樣的，以下範例為設定網路標題為 "cloud-public"，安裝及執行管理伺服器後，您必須將其名稱設定為選定的網路標題(e.g. "cloud-public")，會在 節 4.5，“管理伺服器安裝”討論

如果您使用兩個NICs互相連結來建立公開網路，詳見節 8.2.10.4，“NIC 連結 (選擇性)”

如果您使用一個NIC提供公開網路存取點，在每個新增到CloudStack的主機執行以下步驟

1. 執行xe network-list，並找到公開網路，通常會連結到公開的NIC，找到後，請記下它的UUID，呼叫<UUID-Public>

2. 執行以下指令:

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

8.2.10.2. 設定多訪客網路(選擇性)

CloudStack支援使用多訪客網路，每個網路都會分配一個名稱標題，例如，您或許會有兩個網路標題為 "cloud-guest" 及 "cloud-guest2"，管理伺服器安裝及執行後，您需要增加網路並使用這些標題，如此CloudStack才會注意到這些網路

，新增主機到CloudStack前，執行以下步驟到每台新主機:

1. 執行xe network-list，並找到訪客網路，找到後記下UUID，呼叫 <UUID-Guest>

2. 執行以下指令，替換名稱標籤及UUID

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

3. 重複以上步驟到每台額外的訪客網路，並使用不同的名稱標籤及UUID

8.2.10.3. 分離儲存裝置網路(選擇性)

您可以選擇建立分離的儲存裝置網路，這必須在連結步驟前，先在主機上執行。可以使用一或兩個NIC來達成。此步驟須由管理者來執行

給予儲存裝置網路不同的名稱標籤

為了使分離儲存網路能正常運作，必須是唯一可以判斷主要儲存裝置的IP的介面，例如，如果eth0是管理網路的NIC，ping -I eth0 <primary storage device IP>會失敗。次要儲存裝置必須是管理網路NIC或鍵結可判斷的，如果被放在儲存網路上，它也必須能經由儲存網路NIC或鍵結判斷

您也可以建立兩個分離儲存網路，例如，如果您想要實現多通道iSCSI，或致力於將非鍵結NIC設為多通道。這兩個網路需要不同的名稱標題

如果去鍵結完成了，管理者必須在所有主機(主要及附屬)建立及命名分離儲存網路

以下為建立eth5來存取在172.16.0.0/24儲存網路的範例

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

8.2.10.4. NIC 連結 (選擇性)

XenServer支援 Source Level Balancing (SLB) NIC連結，兩個NIC可以鍵結在一起，可以傳送公用、私人及訪客流量，或是任意組合。分離儲存網路也可以達成，以下是一些支援的設定範例:

- 2 NICs分別給私人、公開及儲存裝置
- 2 NICs給私人、1 NIC給公開，儲存裝置使用管理網路
- 2 NICs給私人、2 NIC給公開，儲存裝置使用管理網路
- 1 NIC分別給私人、公開及儲存裝置

所有NIC鍵結皆為選擇性

XenServer預期所有叢集的節點都是相同的網路配線及鍵結。按照安裝，主要主機會先加到叢集電腦，再來才是附屬主機。鍵結會在其他主機加入時連接主要主機。建立主要主機的鍵結和建立附屬主機的步驟是不一樣的，在以下會說明。這裡有些重要的提示:

- 您必須在第一部部署到叢集的主機先設立鍵結。然後，您必須使用xe指令來建立其他附屬主機的鍵結
- 附屬主機必須和主要主機的配線相同，例如，如果eth0是主要主機的私人鍵結，那麼主機必定是位於管理網路中，為了增加附屬主機

8.2.10.4.1. 管理網路連結

管理者必須先連接管理網路NICs，然後才增加主機到 CloudStack

8.2.10.4.2. 在第一台主機建立私人鍵結

使用以下步驟在XenServer建立連結。這些步驟僅需要在第一台主機執行，此範例為建立雲端私人網路，使用兩組實體NICs (eth0 及 eth1)

1. 找您想要連結的實體NIC

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

   這些指令顯示eth0 及 eth1 NICs 及它們的 UUIDs。依您選擇替換ethX裝置，使用指令slave1-UUID 和 slave2-UUID呼叫UUID

2. 為鍵結建立新網路，例如，一個新網路，名稱為 "cloud-private"

   這標籤很重要， CloudStack會依照名稱尋找網路，您必須在所有管理網路的主機皆使用相同的名稱標籤

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

現在您有能被CloudStack的鍵結對，如同管理網路

8.2.10.4.3. 公開網路鍵結

鍵結可以被用在分離、公開的網路。如果網路會被鍵結及分離管理網路，管理者需要為公開網路設立鍵結。

8.2.10.4.4. 在第一台主機建立公開鍵結

這些步驟僅在第一台主機執行，例如，利用兩個實體NICs（eth2 和 eth3）建立雲端公開網路鍵結

1. 找您想要連結的實體NIC

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

   以下指令顯示eth2 及eth3 NICs和它們的UUIDs，依您的選擇替換ethX裝置，用以上指令slave1-UUID 和 slave2-UUID呼叫UUID

2. 為鍵結建立新的網路，例如，一個新的網路，名稱為"cloud-public"

   這標籤很重要， CloudStack會依照名稱尋找網路，您必須在所有管理網路的主機皆使用相同的名稱標籤

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

現在您有能被CloudStack的鍵結對，如同公開網路

8.2.10.4.5. 增加更多主機道從集

隨著鍵結(如果有)建立在主要主機上您需要新增附屬主機。在所有即將被新增的主機執行以下指令，此舉會將主機加入單一XenServer群

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

8.2.10.4.6. 完成跨叢集電腦鍵結設定

當所有主機都加入群集後，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
```

現在鍵結已經建立及設定完成

8.2.11. 更新XenServer版本

此章節教您如何更新CloudStack主機上的 XenServer，實際上的更新寫在 XenServer 文件中，但有些額外步驟需要在更新前/後執行

注意

請確定硬體相容新版的XenServer

更新XenServer:

1. 更新資料庫，在管理伺服器上:

   a. 備份資料庫

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

   b. 您或許會因VM在更新的主機執行而變更作業系統形式

   - 如果您從 XenServer 5.6 GA更新到XenServer 5.6 SP2，請更換任何有CentOS 5.5 (32-bit)，Oracle Enterprise Linux 5.5 (32-bit)，或 Red Hat Enterprise Linux 5.5 (32-bit)作業系統的VM，將其邊更為Other Linux (32-bit)，請更換任何有64位元版本的VM為Other Linux (64-bit)
   - 如果您從 XenServer 5.6 SP2 更新為 XenServer 6.0.2，請更換任何有CentOS 5.6 (32-bit)，CentOS 5.7 (32-bit)，Oracle Enterprise Linux 5.6 (32-bit)，Oracle Enterprise Linux 5.7 (32-bit)，Red Hat Enterprise Linux 5.6 (32-bit)，或 Red Hat Enterprise Linux 5.7 (32-bit)作業系統的VM，將其邊更為Other Linux (32-bit)，請更換任何有64位元版本的VM為Other Linux (64-bit)
   - 如果您是從XenServer 5.6更新為XenServer 6.0.2，請執行以上所有動作

   c. 重新啓動管理伺服器及使用伺服器，您需要在所有叢集都重新開機一次

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

2. 從CloudStack切斷XenServer cluster的連線

   a. 以root登入 CloudStack使用者介面

   b. 移動到 XenServer cluster，點選Actions，然後選擇Unmanage

   c. 檢查 cluster直到顯示Unmanaged

3. 登入其中一台主機，並執行此指令來清理VLAN:

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

4. 然後執行更新準備程式碼:

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

   疑難雜症: 如果您看見"can't eject CD,"錯誤，請登入VM並卸載CD，再重新執行一遍

5. 更新所有主機的XenServer，注意，先更新主要主機

   a. 移動所有VM到另一台主機，詳見Administrator's Guide的移動指南

   疑難雜症: 如果您在移動VM時看到此錯誤:

   ```
   [root@xenserver-qa-2-49-4 ~]# xe vm-migrate live=true host=xenserver-qa-2-49-5 vm=i-2-8-VM
   You attempted an operation on a VM which requires PV drivers to be installed but the drivers were not
    detected.
   ```

```
vm: b6cf79c8-02ee-050b-922f-49583d9f1a14 (i-2-8-VM)
```

執行以下來解決問題:

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

b. 重新啓動主機

c. 更新較新的XenServer版本，使用XenServer文件裡的步驟

d. 更新完成後，從管理伺服器複製以下檔案到主機中，在以下顯示的資料夾位置:

複製此管理伺服器文件...	...到此位置
/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver/xenserver60/NFSSR.py	/opt/xensource/sm/NFSSR.py
/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver/setupxenserver.sh	/opt/xensource/bin/setupxenserver.sh
/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver/make_migratable.sh	/opt/xensource/bin/make_migratable.sh
/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver/cloud-clean-vlan.sh	/opt/xensource/bin/cloud-clean-vlan.sh

e. 執行以下程式碼:

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

疑難雜症: 如果您看到以下錯誤，您可以放心放心忽略

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

f. 插入儲存裝置庫(實體方格裝置)到XenServer主機:

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

注意: 如果您增加一台主機到XenServer群，您需要移動所有此主機的VM到其他主機，然後才從XenServer群移除主機

6. 重複這些步驟來更新所有主機

7. 在其中一台主機執行以下指令來清理主機tag:

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

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

8. XenServer叢集電腦與CloudStack重新連線

   a. 以root登入 CloudStack使用者介面

   b. 移動到 XenServer cluster，點選Actions，然後選擇manage

   c. 等待所有主機出現

9. 所有主機出現後，在一台主機執行以下步驟:

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

8.3. VMware vSphere安裝與設定

如果您想使用 VMware vSphere hypervisor 來執行訪客的VM，請安裝vSphere在您的雲端主機(一至多個)

8.3.1. vSphere主機系統需求

8.3.1.1. 軟體需求:

- vSphere 及 vCenter，皆為 version 4.1 或 5.0

  推薦vSphere Standard。但客戶需要考慮vSphere licensing下的CPU限制，詳見 http://www.vmware.com/files/pdf/vsphere_pricing.pdf，並與您的 VMware銷售員討論

  推薦vCenter Server Standard

- 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

套用到所有必要的Hotfixes

缺少最新的hotfixes會導致資料毀損及VM錯誤

8.3.1.2. 硬體需求:

- 主機必須相容vSphere，詳見VMware Hardware Compatibility Guide http://www.vmware.com/resources/compatibility/search.php

- 所有主機必須是64位元及支援HVM（Intel-VT 或 AMD-V）

- 同一cluster內的主機都必須是同質的，CPU的形式、數量及特色旗標都必須一樣
- 64-bit x86 CPU（多核提供更好的效能）
- 支援Hardware virtualization
- 記憶體4GB
- 36GB硬碟
- 至少1個NIC
- 固定IP

8.3.1.3. vCenter 伺服器需求:

- Processor - 2 CPUs 2.0GHz or higher Intel or AMD x86 processors。處理器需求可能因資料庫在同一台機器上運行而需要更高
- Memory - 3GB RAM。記憶體需求可能因資料庫在同一台機器上運行而需要更高
- Disk storage - 2GB。硬碟需求可能因資料庫在同一台機器上運行而需要更高
- Microsoft SQL Server 2005 Express disk requirements。一大組資料庫需要至少2GB硬碟空間來解壓縮安裝壓縮檔
- Networking - 1Gbit or 10Gbit.

更多資訊，詳見 "vCenter Server and the vSphere Client Hardware Requirements" http://pubs.vmware.com/vsp40/wwhelp/wwhimpl/js/html/wwhelp.htm#href=install/c_vc_hw.html

8.3.1.4. 其他需求:

- VMware vCenter Standard Edition 4.1 或 5.0必須安裝及能夠管理vSphere 主機
- vCenter必須設定為使用標準port 443，讓它可以與CloudStack管理伺服器溝通
- 如果您是使用舊主機，您需要重安裝VMware ESXi
- CloudStack僅支援VMware vSphere 4.1 或 5.0，不支援4.0
- All hosts must be 64-bit and must support HVM (Intel-VT or AMD-V enabled). All hosts within a cluster must be homogeneous. That means the CPUs must be of the same type, count, and feature flags.
- CloudStack管理網路不能被設為分離虛擬網路，CloudStack管理網路與 vCenter管理網路相同，並會繼承它的設定，詳見節 8.3.5.2, “設定”
- CloudStack 僅支援ESXi，不支援ESX
- 所有之前使用CloudStack的資源必須只使用在CloudStack，CloudStack無法分享ESXi的instance或其他管理控制台的儲存裝置。不要分享會被不同組ESXi的CloudStack使用的儲存裝置容量
- 將所有目標ESXi超級監督者放到cluster，cluster屬於 vCenter中的分離資料庫
- 會被CloudStack管理的cluster不能包含任何VM，不要執行管理伺服器、vCenter或是其他指定給CloudStack使用的VM，可以建立分離cluster來給CloudStack使用，但請確定cluster中沒有任何VM

- 所有需要的VLAN會被集中到所有連結ESXi 超級監督者主機的網路切換器，其中會包含管理、儲存裝置、vMotion及訪客的VLAN。訪客VLAN(使用在Advanced Networking，詳見Network Setup)是CloudStack管理的連續VLAN範圍

8.3.2. VMware的準備清單

為了順利安裝，請先準備以下資訊:

- 列在 節 8.3.2.1, “vCenter Checklist”的資訊
- 列在節 8.3.2.2, “VMware的網路清單”的資訊

8.3.2.1. vCenter Checklist

您會需要以下關於vCenter的資訊:

vCenter 需求	數值	備註
vCenter 使用者		使用者必須有管理優先權
vCenter使用者密碼		以上使用者的密碼
vCenter資料庫名稱		資料庫名稱
vCenter Cluster名稱		Cluster名稱

8.3.2.2. VMware的網路清單

您會需要以下關於VLAN的資訊:

VLAN 資訊	數值	備註
ESXi VLAN		您所有ESXi hypervisors位於的VLAN
ESXI VLAN IP位址		ESXi VLAN中的IP Address Range，每個虛擬路由器由此範圍使用IP
ESXi VLAN IP閘道		
ESXi VLAN遮罩		
VLAN管理伺服器		CloudStack 管理伺服器安裝的VLAN
公開VLAN		公開網路的VLAN
公開VLAN閘道		
公開VLAN遮罩		
公開		Range of Public IP Addresses 提供CloudStack使用，這些位址將被使用在CloudStack 上的虛擬路由器，將私人流量導向外部網路
客戶使用的		一段連續範圍VLAN，一個使用者會被配發一個VLAN。

8.3.3. vSphere安裝步驟

1. 您需要從VMware網頁下載及購買vSphere如果您還沒有（https://www.vmware.com/tryvmware/index.php?p=vmware-vsphere&lp=1），然後跟著VMware vSphere 安裝指南安裝

2. 以下安裝將執行以下設定，這些設定在接下來的章節做描述：

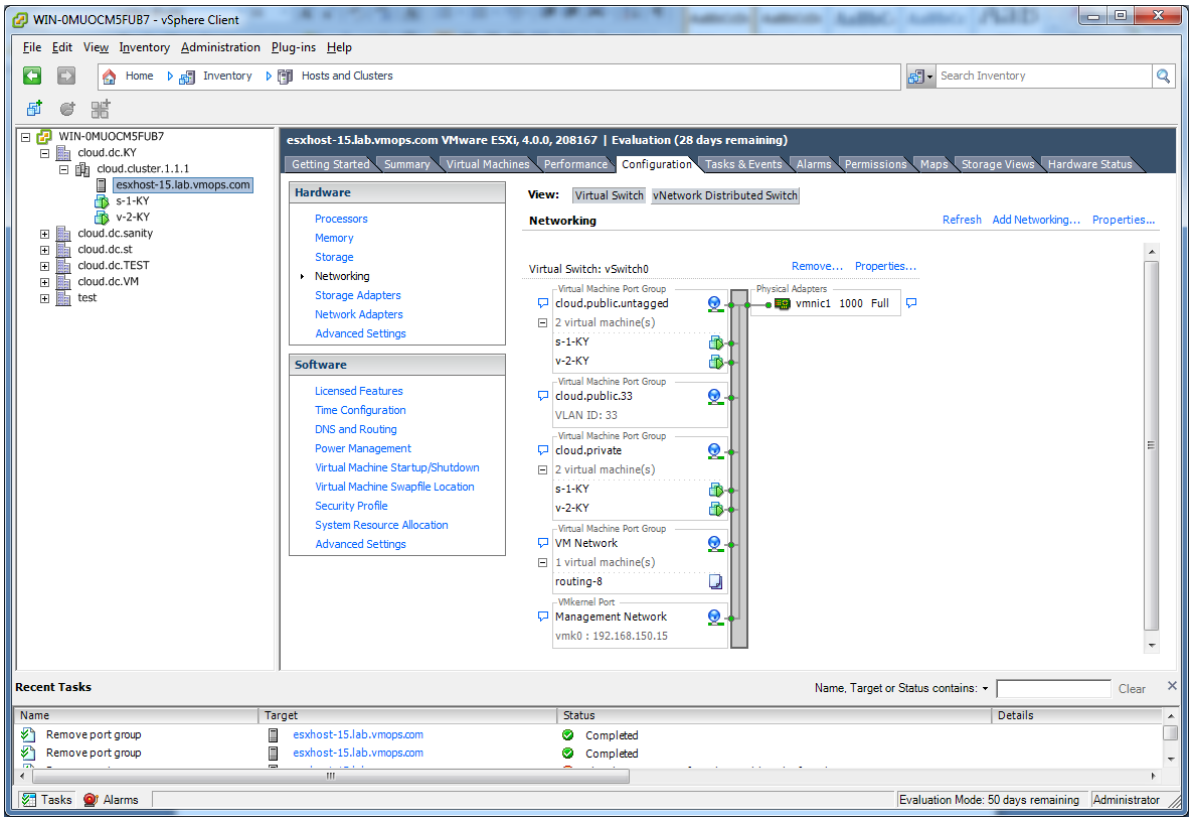
必要的	非必要的
ESXi 主機設定	NIC 結合
設定主機的實體網路、虛擬開關、vCenter管理網路及擴充埠的範圍	多途徑儲存
準備 iSCSI 儲存裝置	
設定 vCenter 的 cluster 並增加主機到 cluster，或是增加沒有cluster的主機到	

8.3.4. ESXi主機設定

所有ESXi 主機都應該在BIOS允許CPU硬體虛擬化支援。請注意，硬體虛擬化支援預設都是關閉的

8.3.5. 實體主機網路

您需要為 vSphere主機的牽線做規劃，適當的網路設定是在您新增 vSphere主機到CloudStack前所需要的。關於設定ESXi主機，您可以先使用vClient，並以獨立主機的形式新增到vCenter，一旦您看見主機出現在vCenter的清單中，您就可以點選清單中主機的 Configuration標籤



在host configuration標籤中，點選"Hardware/Networking"進入網路設定葉面

8.3.5.1. 設定

有一個預設的virtual switch vSwitch0會被新增，CloudStack需要所有ESXi 雲端主機都使用同一組virtual switch名稱。如果您改變預設的名稱，您也會需要設定一至多個CloudStack 變數

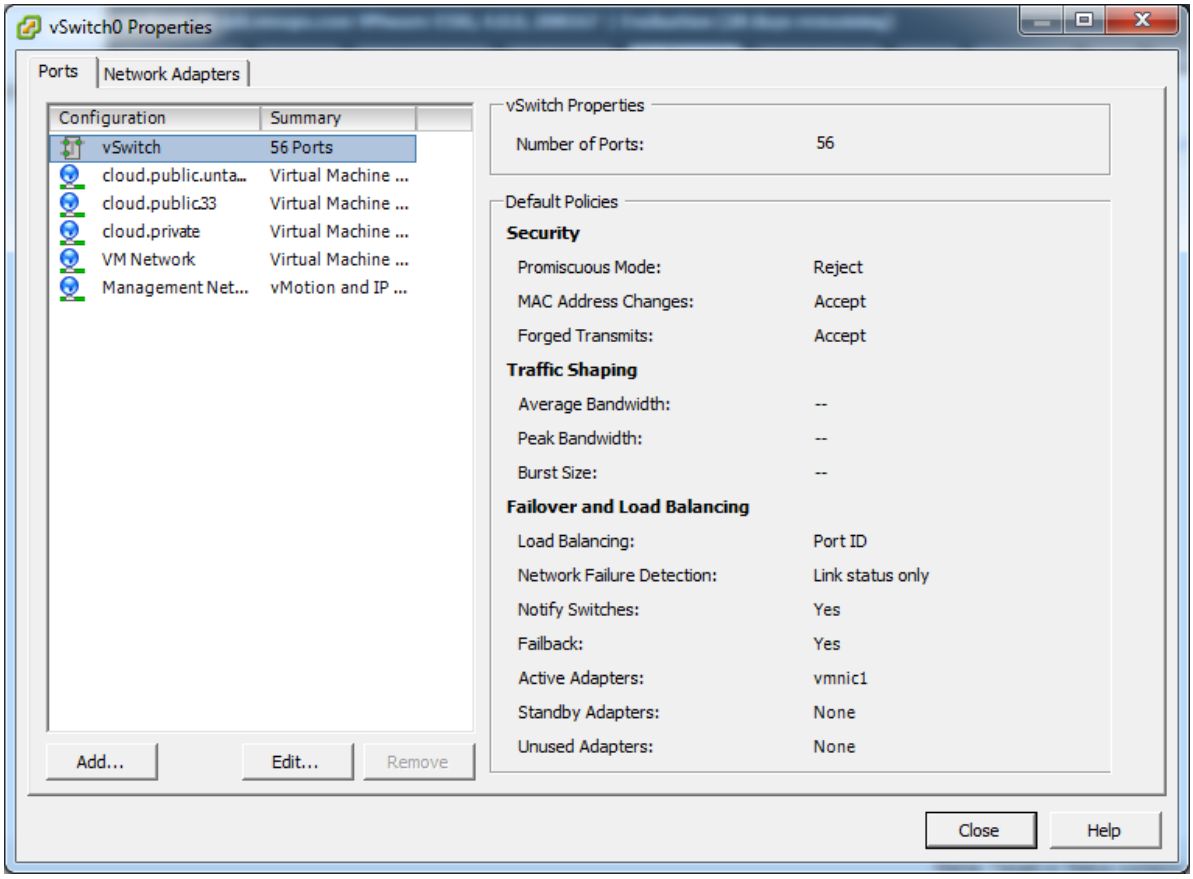
8.3.5.1.1. Separating Traffic

CloudStack允許您使用vCenter在每個ESXi 主機設定三個獨立的網路，這些網路由它們連結到的vSwitch名稱來區分。可被設定的網路分別為公用(流量從/到公用網路)、訪客(訪客網路間的流量)和私人(管理及儲存流量)。您可以套用預設的virtual switch到這三個網路，或是創建一、二個

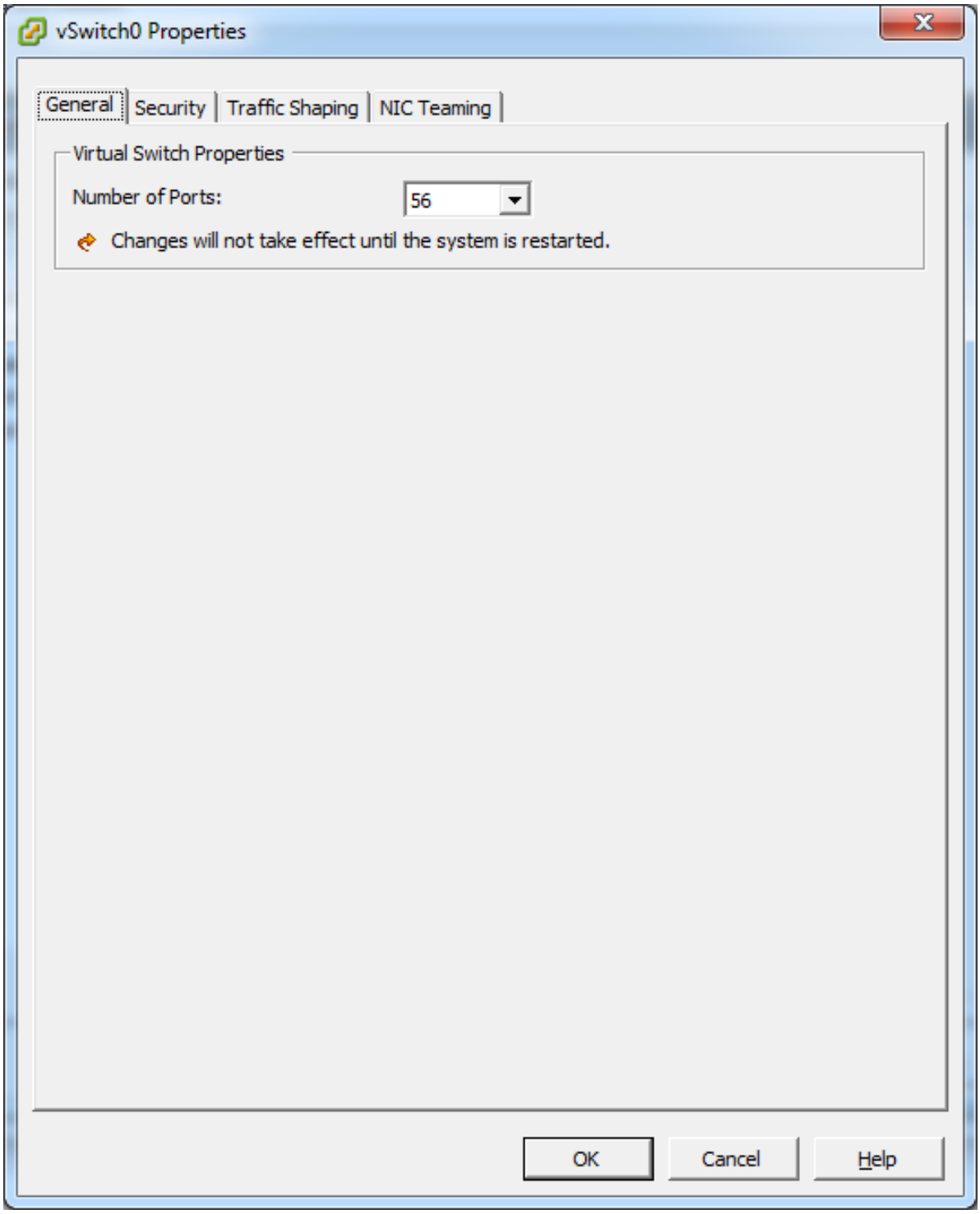
如果您想要這樣分離流量，您需要先根據 vCenter指示建立及設定vSwitches，記錄下每個流量型態的vSwitch名稱，您會需要用這些設定CloudStack

8.3.5.1.2. Increasing Ports

ESXi主機上的virtual switch預設上有56個埠，我們建議您設定到4088個，最大的允許量。選擇virtual switch的"Properties..."(注意，這不是Networking的Properties連結)



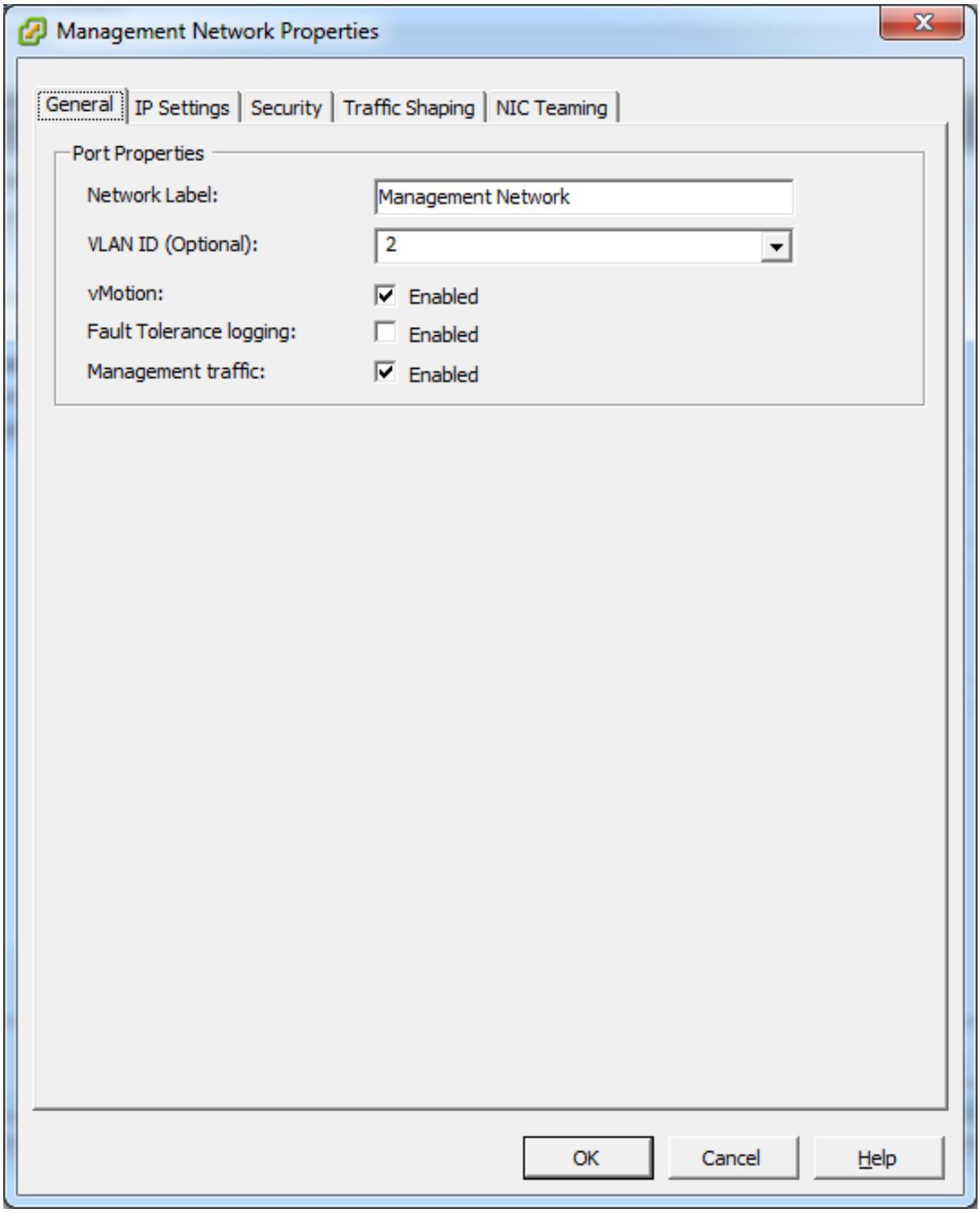
在vSwitch properties對話框，選擇vSwitch然後按 Edit，您應該會看到以下對話框:



在這個對話框，您可以改變switch埠的數量。當您完成改變後，ESXi主機會重新開機

8.3.5.2. 設定

在vSwitch properties對話框，您會看到vCenter management network，這個一樣的 network也會用在 CloudStack management network。CloudStack要求vCenter management network必須要適當地設定。選擇對話框中的management network item然後按下



請先確定以下數值已經設定:

・VLAN ID 已設定為想要的ID

・啓用vMotion

・啓用Management traffic

如果ESXi主機有多個VMKernelports, 以及不是使用預設的"Management Network"為management network名稱, 您必須按照指南來設定management network port group, CloudStack才能找到:

・使用一個 management network port標籤橫跨所有ESXi主機

・在CloudStack UI中，到Configuration - Global Settings設定vmware.management.portgroup到ESXi主機的management network標籤

8.3.5.3. 為CloudStack Console Proxy擴展部的範圍

(只能套用到 VMware vSphere version 4.x)

您需要擴展防火牆的埠範圍，讓主機上的console proxy能夠在VMware-based VMs能夠工作。預設的額外埠範圍是59000-60000。登入到每個主機的 VMware ESX service console，然後執行以下指令:

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

8.3.5.4. 設定vSphere的

vSphere主機上的NIC bonding可以依照 vSphere安裝指南來完成

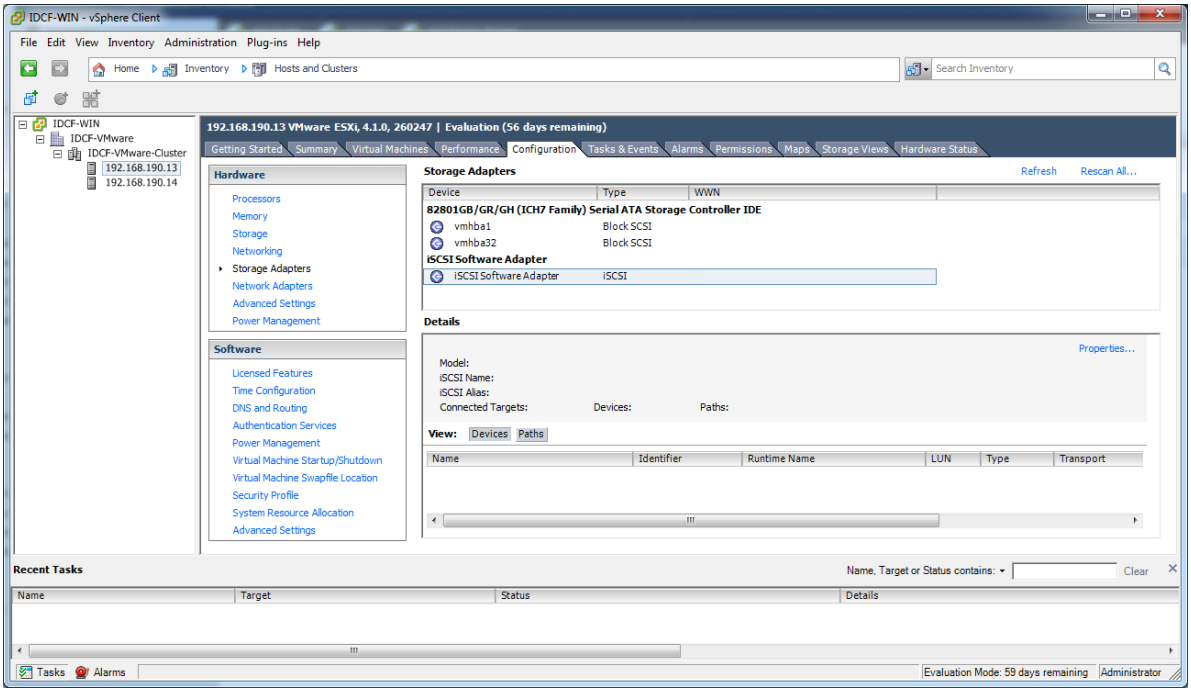
8.3.6. vSphere的儲存裝置準備工作(限)

使用 iSCSI，在vCenter會有準備工作。您必須要新增一個 iSCSI 目標以及新增一個 iSCSI datastore

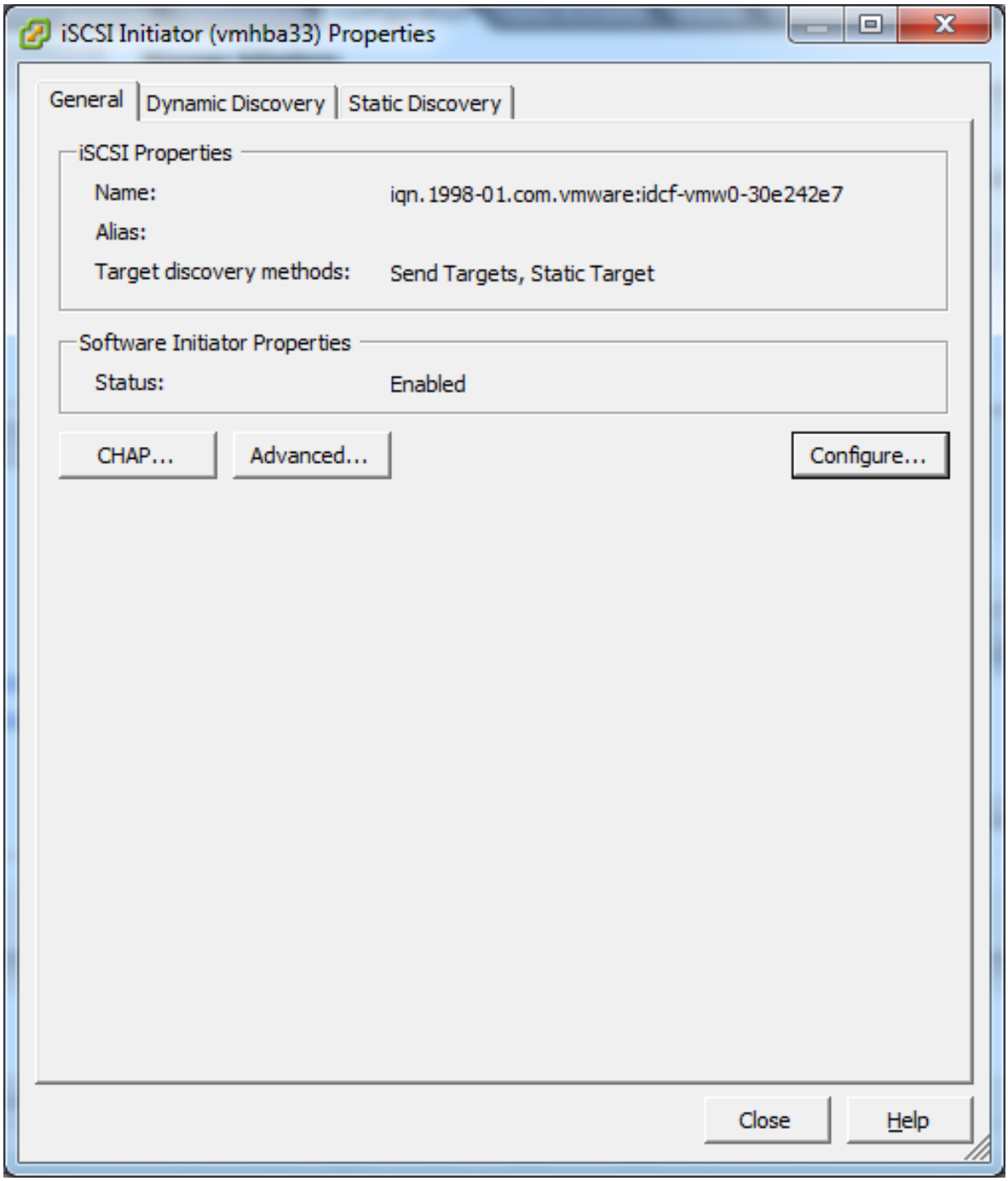
如果您是使用NFS，請跳過這個章節

8.3.6.1. 啓用 ESXi 主機的

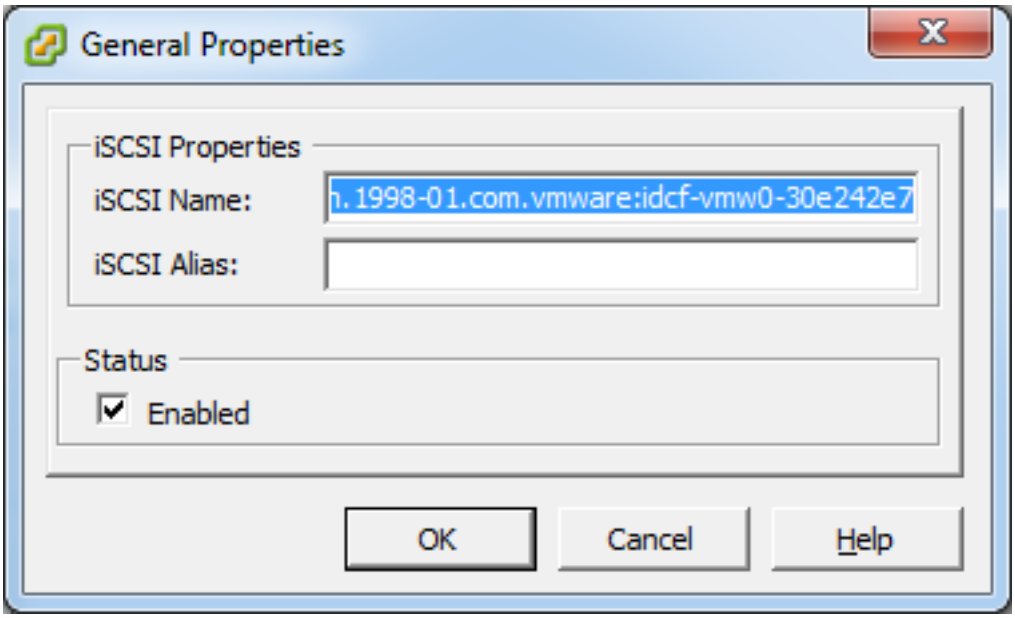
1. 在vCenter，到hosts and Clusters/Configuration，然後按下 Storage Adapters連結，您會看到:



2. 選擇 iSCSI software adapter ，然後選擇Properties



3. 選擇Configure...

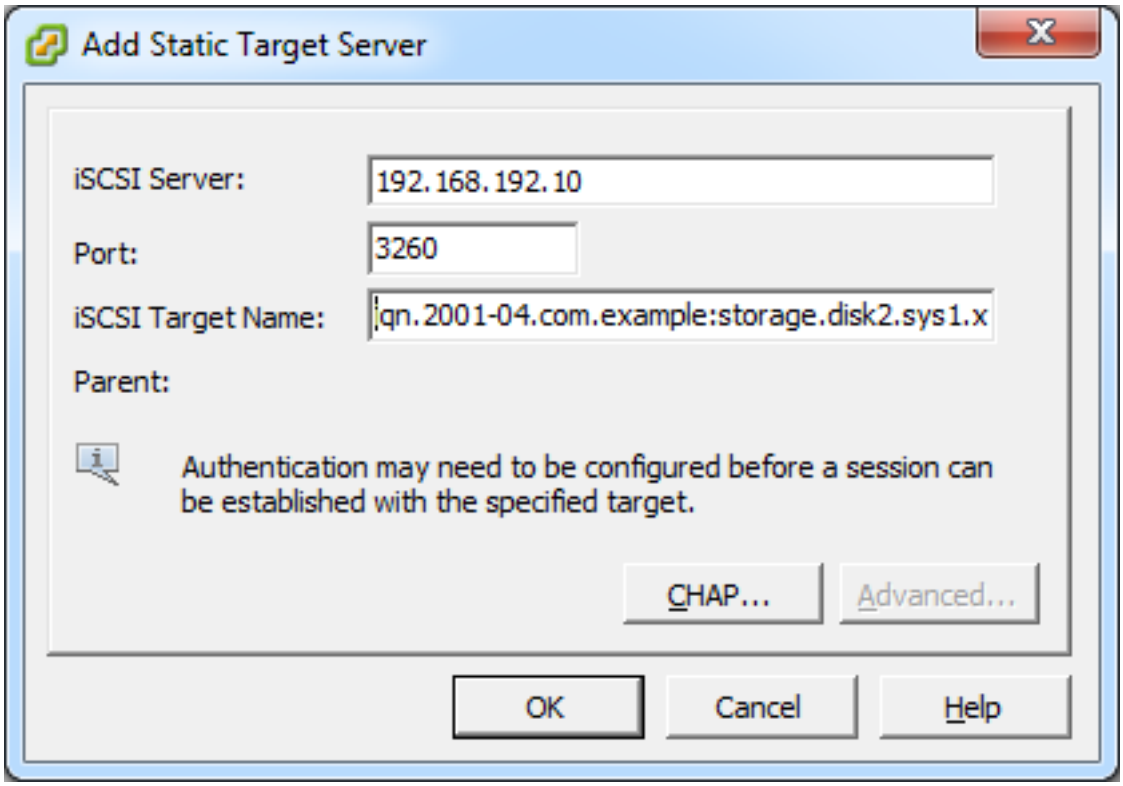


4. 勾選 Enabled來啓用 initiator

5. 按下OK並儲存

8.3.6.2. 新增iSCSI target

在properties對話框, 新增 iSCSI target資訊



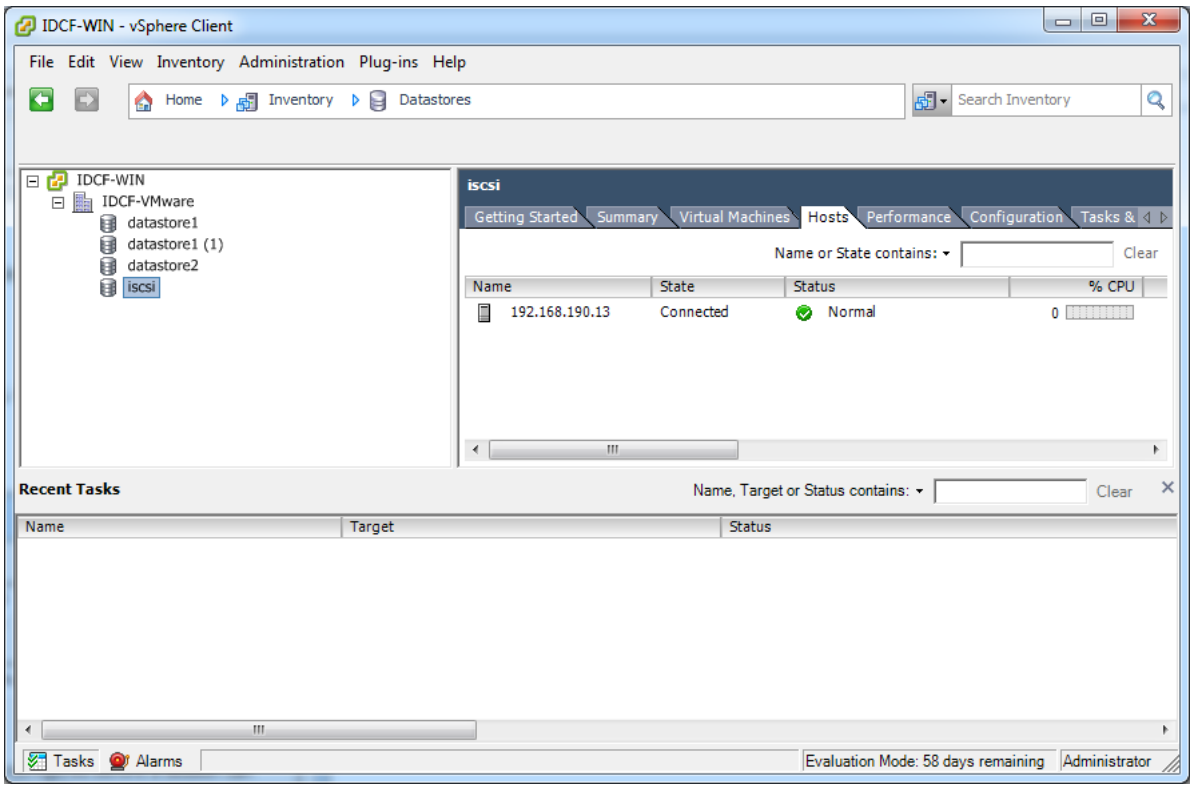
在所有 ESXi 主機重複這些步驟

8.3.6.3. 新增一個 iSCSI datastore

按照以下步驟來新增 VMFS datastore

1. 選擇Home/Inventory/Datastores.
2. 在datacenter node按右鍵
3. 選擇Add Datastore...
4. 使用安裝精靈來新增iSCSI datastore

這個步驟只需要在一台主機上執行即可



8.3.6.4. Multipathing for vSphere(選擇性)

vSphere node上的Storage multipathing可以依照vSphere安裝指南來完成

8.3.7. 新增主機 或 設定 Clusters (vSphere)

使用vCenter來建立vCenter cluster以及新增主機到cluster。您之後會新增整個cluster到CloudStack (詳見 節 6.5.2, “加入叢集: vSphere ”).

8.3.8. 套用Hotfixes到 VMware vSphere主機

1. 從CloudStack切斷VMware vSphere cluster連結, 時間足夠我們套用hotfix到主機上
   a. 以root登入

      詳見

   b. 移動到 VMware cluster, 點選Actions, 然後選擇Unmanage
   c. 檢查 cluster直到顯示Unmanaged

2. 執行以下到每個cluster上的 ESXi主機:

   a. 移動每個主機到maintenance mode

   b. 確保所有VM都已經移到其他cluster 的主機了

   c. 如果只有一台主機，關閉所有VM，然後將主機移至maintenance mode

   d. 將補釘套用到ESXi主機

   e. 如果有提示，請重新啓動

   f. 取消maintenance mode

3. 重新連線到CloudStack

   a. 以root登入

   b. 移動到VMware cluster，點選Actions，然後選擇

   c. 等待所有主機出現，這可能會等待數分鐘

      確認主機的狀態是否適當地同步以及更新到CloudStack資料庫

額外安裝選項

接下來的幾個章節敘述CloudStack 的進階功能

9.1. 安裝使用伺服器(選擇性)

當管理伺服器設定完成，您可以選擇安裝使用伺服器，此伺服器從系統事件擷取資料，及啓用使用收費的帳戶

當多管理伺服器出現時，使用伺服器可以安裝在任意數量上。使用伺服器可以協調使用進程。有可用性疑慮的站點應該要在至少兩個管理伺服器上安裝管理伺服器

9.1.1. 安裝需求

・管理伺服器必須是執行狀態

・使用伺服器必須安裝在與管理伺服器相同的伺服器上

9.1.2. 安裝步驟

1. 執行 ./install.sh.

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

安裝準備好時，您會在一串選項下看到一些訊息

2. 選擇"S"來安裝使用伺服器

```
> S
```

3. 安裝好後，使用以下指令啓動使用伺服器

```
# service cloudstack-usage start
```

管理指南有更詳細的設定

9.2. SSL(選擇性)

CloudStack在預設安裝中提供HTTP存取，有很多技術及站點可以選擇來實現SSL，因此，在站點可以實現基本功能的情況下，我們將HTTP留給CloudStack實現

CloudStack使用Tomcat作為servlet 容器，對於想要CloudStack終止SSL工作的站點，Tomcat’s SSL或許可以存取，Tomcat SSL設定在http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html 詳加描述

9.3. 複製資料庫(選擇性)

CloudStack 支援複製資料庫到另一個MySQL節點，使用standard MySQL replicatio來複製，您或許會想備份MySQL伺服器或避免儲存資料遺失，MySQL replication使用master/slave model。master是使用管理伺服器的節點；slave是待機節點負責接收master的寫入指令及應用到本地、其餘的資料庫備份，以下為複製的步驟

注意

建立複製品不等於備份，您需要發展一套與複製不同的備份步驟

1. 確保master沒有任何資料
2. 編輯master的my.cnf，加入以下行數在datadir下方的[mysqld]區域

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

server_id必須是獨一無二的，建議是給master ID為1，其他slave則是大於1的連續數字，如此伺服器就會依照1,2,3...排列

3. 重新啓動 MySQL

```
# service mysqld restart
```

4. 在master新增複製帳戶，並給予優先權。使用"cloud-repl"為使用者名稱，"password"為密碼，在此假設master及slave是在172.16.1.0/24網路中

```
# mysql -u root
mysql> create user 'cloud-repl'@'172.16.1.%' identified by 'password';
mysql> grant replication slave on *.* TO 'cloud-repl'@'172.16.1.%';
mysql> flush privileges;
mysql> flush tables with read lock;
```

5. 離開現在的MySQL工作
6. 在另一個shell開啓第二個MySQL 工作
7. 取得目前資料庫的位置

```
# mysql -u root
mysql> show master status;
+------------------+----------+--------------+------------------+
| File             | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+------------------+----------+--------------+------------------+
| mysql-bin.000001 |      412 |              |                  |
+------------------+----------+--------------+------------------+
```

8. 記下檔案及位置
9. 離開此工作
10. 完成master設定，回到第一個工作，解鎖並離開MySQL

```
```

```
mysql> unlock tables;
```

11. 安裝及設定slave。在slave伺服器，執行以下指令

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

12. 編輯my.cnf，加入以下行數在datadir下方的[mysqld]區域

```
server_id=2
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
```

13. 重新啓動 MySQL

```
# service mysqld restart
```

14. 將slave連結到master，並從master複製，用之前步驟取得的數值取代IP位址、密碼、登入紀錄檔及位置

```
mysql> change master to
    -> master_host='172.16.1.217',
    -> master_user='cloud-repl',
    -> master_password='password',
    -> master_log_file='mysql-bin.000001',
    -> master_log_pos=412;
```

15. 在slave啓動此複製

```
mysql> start slave;
```

16. 選擇性，開啓slave的3306通訊埠，如同之前在master開啓的

    此步驟非必要，如果您現在不設定，當複製品出現錯誤時，您就需要設定

9.3.1. Failover

此會提供複製資料庫，用來實施管理伺服器手動故障轉移，CloudStack使用管理者轉移故障，當資料庫故障轉移時，您需要：

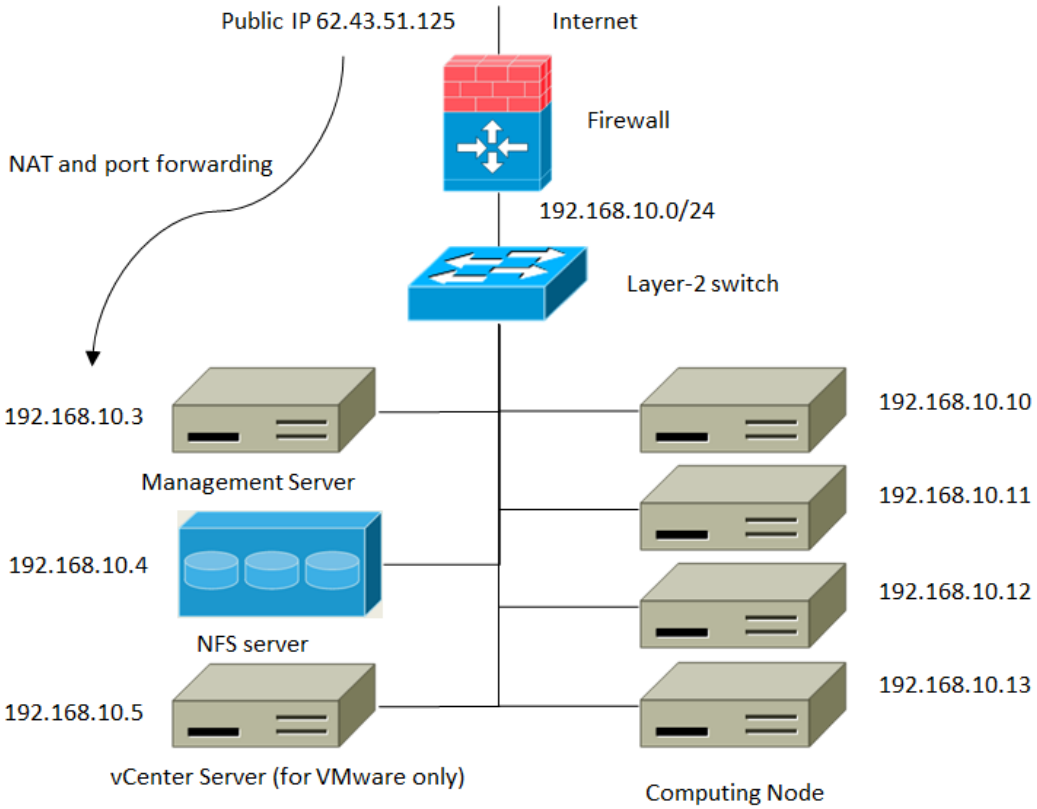
1. Stop the Management Servers (via service cloudstack-management stop).
2. 改變複製品的設定為master，然後重新啓動
3. 確保3306通訊埠有開啓
4. 做些改變讓管理伺服器使用新的資料庫，最簡單的方法是將新伺服器的IP位址放到每個管理伺服器的/etc/cloud/management/db.properties
5. 重新啓動管理伺服器：

```
# service cloudstack-management start
```

選擇部署架構

部署架構會依大小及用途而不同。此章節有範例，包含小型的部署，可用來測試；包含完整元件庫、大型的部署

10.1. Small-Scale Deployment

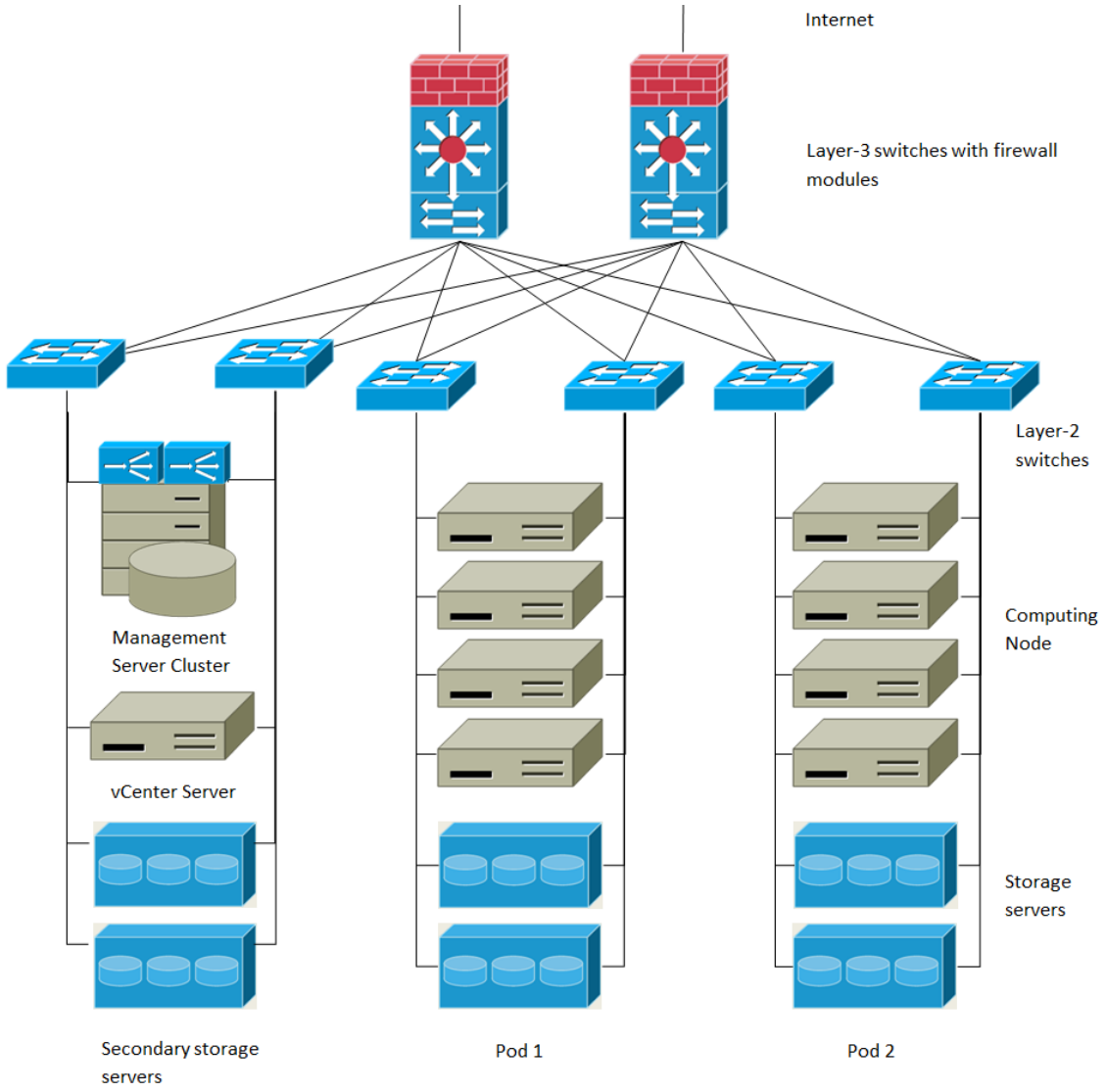


Small-Scale Deployment

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

- A firewall provides a connection to the Internet. The firewall is configured in NAT mode. The firewall forwards HTTP requests and API calls from the Internet to the Management Server. The Management Server resides on the management network.
- A layer-2 switch connects all physical servers and storage.
- A single NFS server functions as both the primary and secondary storage.
- The Management Server is connected to the management network.

10.2. 大尺度的Redundant設定



Large-Scale Redundant Deployment

此圖描述大尺度CloudStack 部署的網路架構

- layer-3 switching layer為資料中心的核心，應設置router redundancy protocol如VRRP。通常也高等級的核心交換器也包含防火牆，如果layer-3 switch沒有內建的防火牆，分離的防火牆也可使用。防火牆設為NAT模式，並提供以下功能:
  - 從網際網路轉送HTTP要求及API呼叫到管理伺服器，管理伺服器位於管理網路
  - 當雲端擴展多個區域，防火牆應要開啓站對站VPN，像是不同區域的伺服器，能互相溝通
- 建立layer-2 access switch layer在每個pod，多交換器可以堆積，來增加通訊埠。不論是哪一種，都應部署redundant pairs of layer-2 switches
- 管理伺服器叢集(包含前端負載平衡器、管理伺服器節點及MySQL資料庫)藉由一對負載平衡器連結到管理網路
- 次要儲存伺服器連結到管理網路

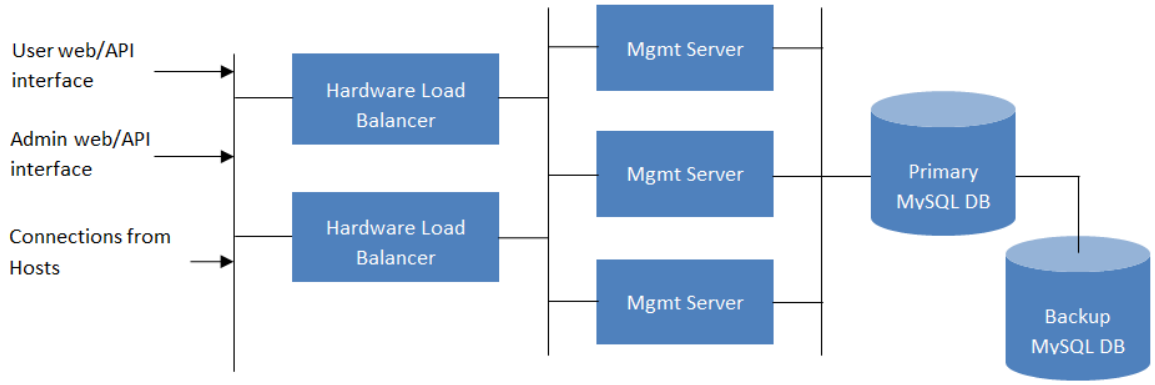
- 每個pod包含儲存及運算伺服器。每個儲存及運算伺服器都應有redundant NICs連接到separate layer-2 access switches

10.3. Separate Storage Network

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

10.4. Multi-Node Management Server

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



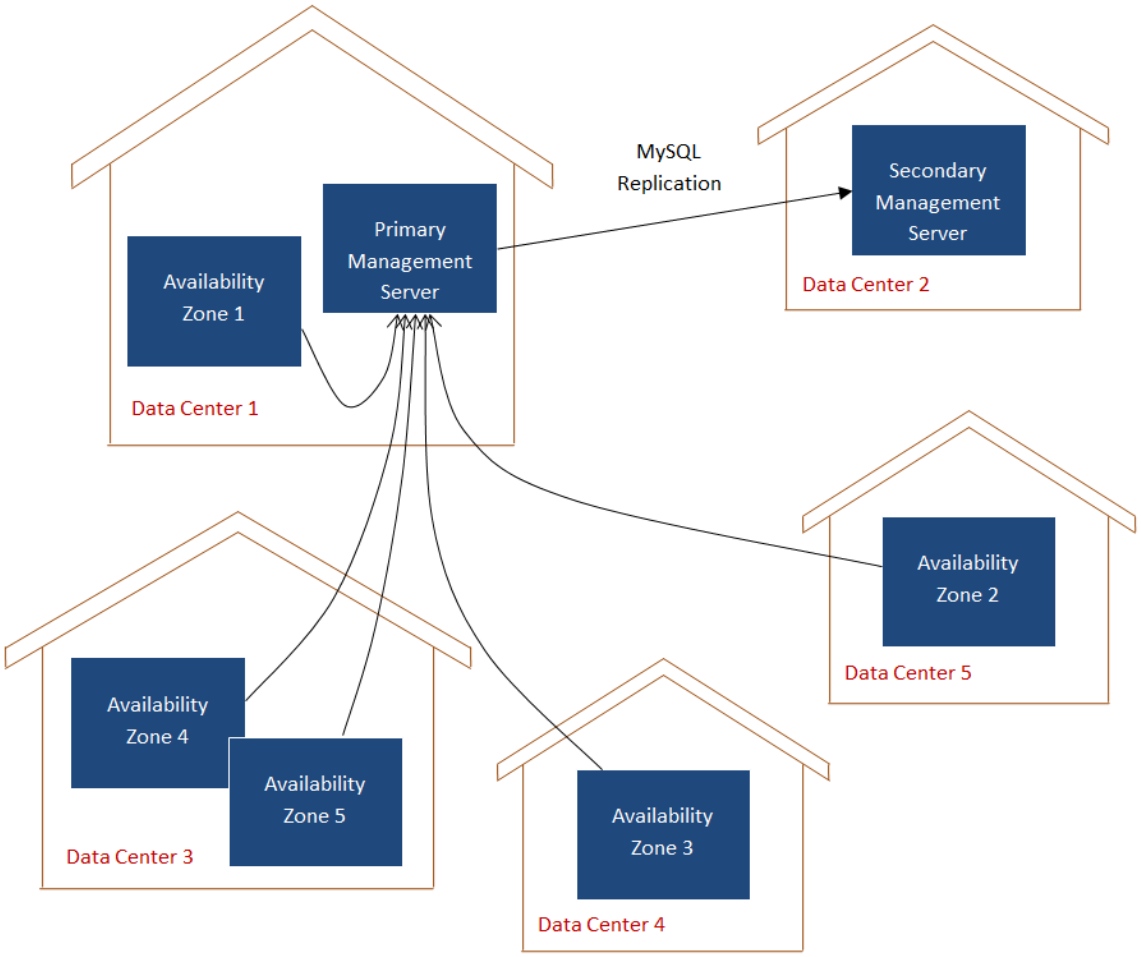
Multi-Node Management Server Deployment

The administrator must decide the following.

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

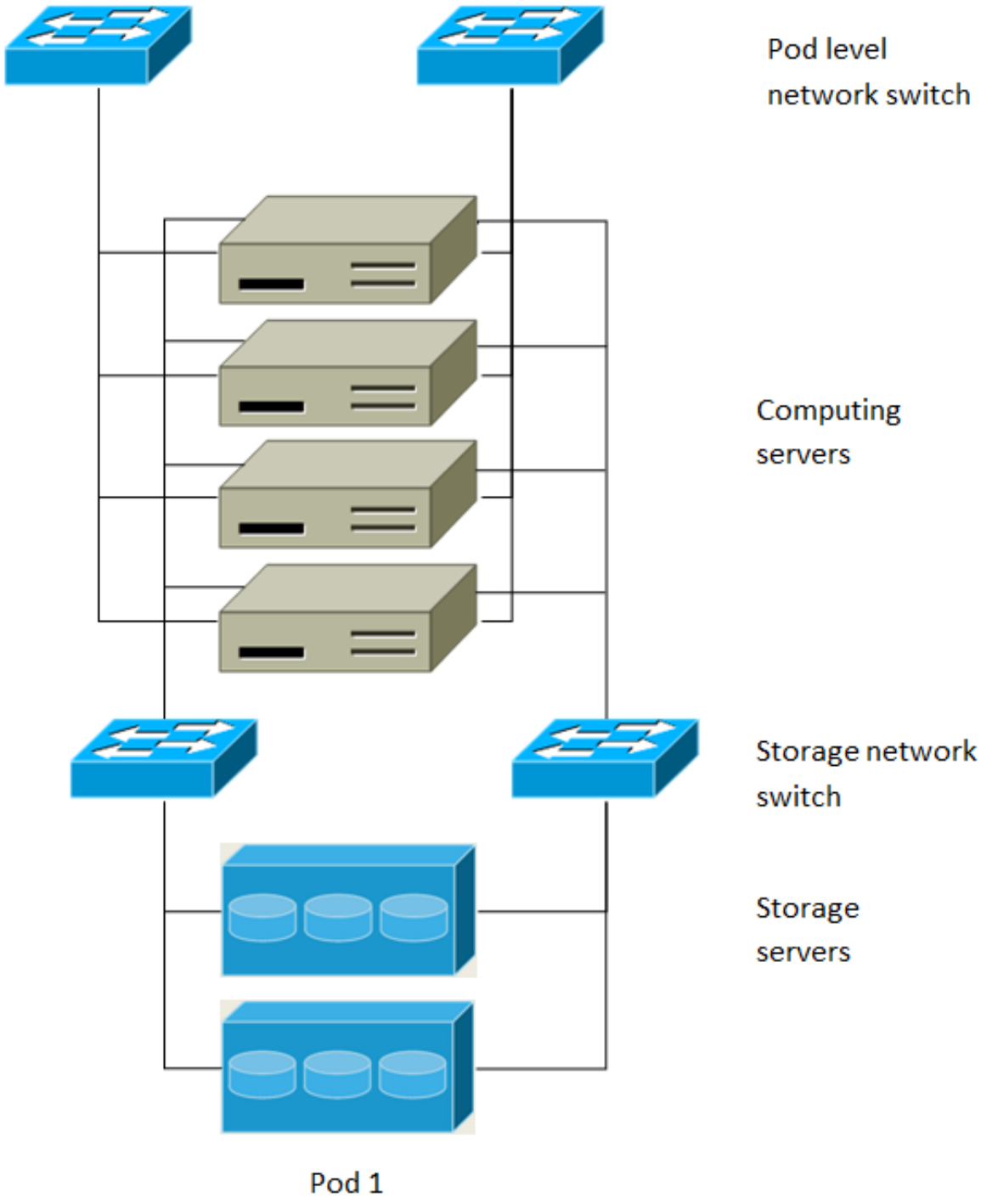
10.5. 多站點部署

CloudStack平台藉由使用區域，得以使多站點可以擴充，以下圖形為多站點部署的例子



Example of a Multi-Site Deployment

Data Center 1進駐主要管理伺服器，是為區域1，MySQL資料庫在資料中心2複製到次要管理伺服器安裝程序



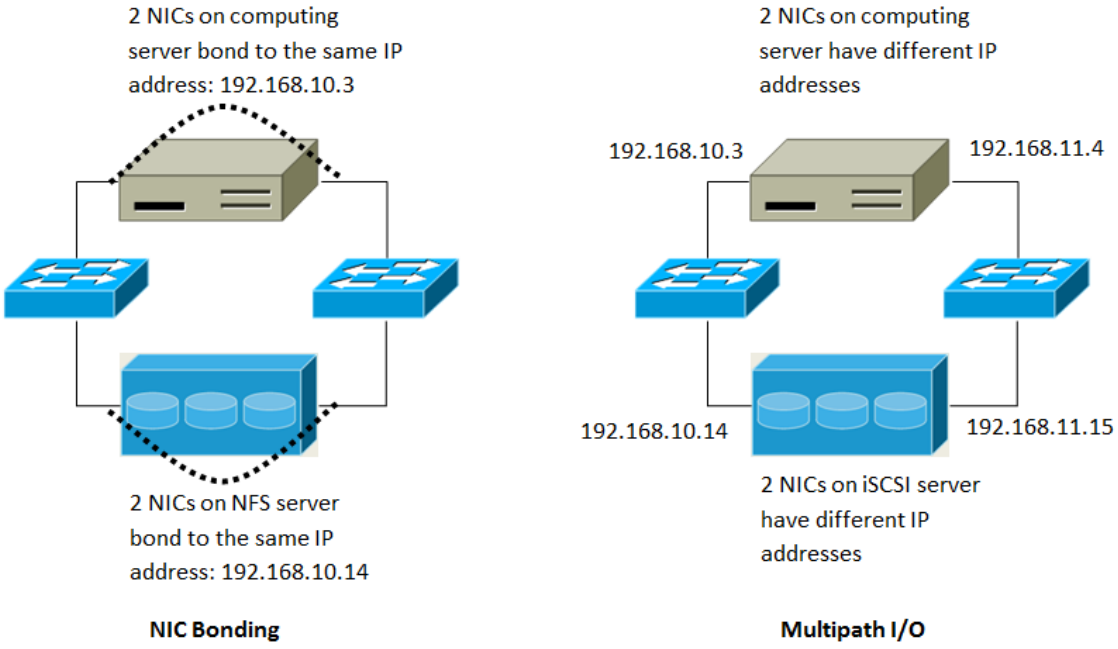
Separate Storage Network

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

There are two ways to configure the storage network:

- Bonded NIC and redundant switches can be deployed for NFS. In NFS deployments, redundant switches and bonded NICs still result in one network (one CIDR block+ default gateway address).

- iSCSI can take advantage of two separate storage networks (two CIDR blocks each with its own default gateway). Multipath iSCSI client can failover and load balance between separate storage networks.



NIC Bonding and Multipath I/O

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

Amazon Web Services相容的界面

11.1. Amazon Web Services相容的界面

CloudStack 可以將Amazon Web Services(AWS)的API指令轉譯成為CloudStack的API指令，所以使用者可以運用現有的AWS相關工具操作CloudStack。此轉譯的服務是利用CloudStackmanagement server的tomcat，但是不同連接埠，Amazon Web Services (AWS) 界面提供了 EC2 SOAP以及Query APIs和S3 REST API。

注意

此服務的前身為CloudBridge，目前已經完全併入CloudStack的management server。

警告

相對應於EC2的查詢API以及S3的API目前正在開發階段， 相容於S3的API提供了將資料儲存於management server檔案系統的方法。

限制條件

- 僅支援基礎網路設定的zones。
- 新安裝的 CloudStack 才具有此功能，而以舊版本升級方式安裝的是沒有本功能的。
- Features such as Elastic IP (EIP) and Elastic Load Balancing (ELB) are only available in an infrastructure with a Citrix NetScaler device. Users accessing a Zone with a NetScaler device will need to use a NetScaler-enabled network offering (DefaultSharedNetscalerEIP and ELBNetworkOffering).

11.2. 支援的API版本

- EC2介面使用Amazon's WDSL編譯，版本時間 11月15日，2010年，在http://ec2.amazonaws.com/doc/2010-11-15/可取得
- 介面相容EC2 command-line tools EC2 tools v. 1.3.6230，可於http://s3.amazonaws.com/ec2-downloads/ec2-api-tools-1.3-62308.zip下載

注意

支援更多較新版本的EC2 API的工作正在進行

11.3. 啓用 EC2 及 S3相容介面

提供 AWS API compatibility的軟體已經隨CloudStack安裝了，您必須使用前啓用服務及執行一些設定

1. 設定每個服務的廣域設定參數為ture，詳見章 7, Global Configuration Parameters

2. 建立一組CloudStack服務，使用與Amazon service offerings相同的名稱，您可以藉由CloudStack使用者介面完成，詳細描述在Administration Guide

警告

確定您有包含Amazon預設服務m1.small，及任何您想使用的EC2 instance types

3. 如果您還沒有在1步驟設定參數，請重新啓動管理伺服器

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

以下章節提供步驟細節

11.3.1. 啓用服務

您需要設定參數enable.ec2.api及enable.s3.api為true，您不需要同時啓用，僅啓用您需要的即可。可透過到Global Settings 使用CloudStack 圖形介面或是使用API都可以完成

以下快取物件告訴您如何使用圖形介面啓用這些服務

使用CloudStack API，最簡單的是使用所謂非認證呼叫的累積埠。在Global Settings將通訊埠設為8096，並呼叫updateConfiguration ，以下URL教您如何做

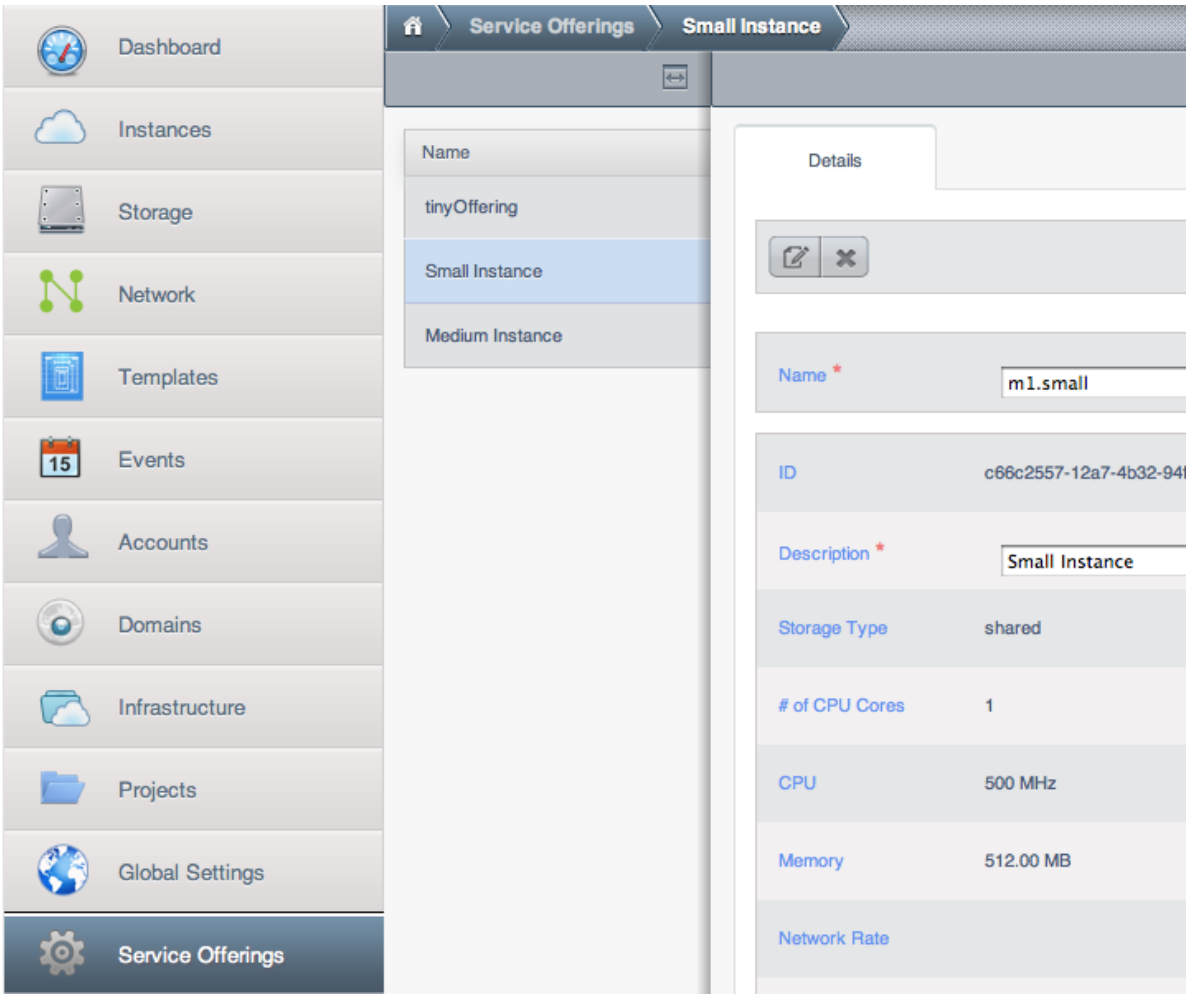
```
http://localhost:8096/client/api?command=updateConfiguration&name=enable.ec2.api&value=true
http://localhost:8096/client/api?command=updateConfiguration&name=enable.ec2.api&value=true
```

啓用後，請重新啓動伺服器

11.3.2. 建立EC2相容服務

您也需要定義計算服務，名稱需與 Amazon EC2 instance types[1] API 名稱（例如 m1.small,m1.large）相同，可以藉由CloudStack圖形介面完成，到 Service Offerings下選擇Compute offering，並建立新的計算服務或修改已有的，確保名稱與EC2 instance type API名稱相同，以下快取物件教您如何做:

[1] http://aws.amazon.com/ec2/instance-types/



11.3.3. 修改AWS API 通訊埠

注意

(選擇性)WS API等候7080通訊埠的要求，如果您較喜歡AWS API等候其他通訊埠，您可以用以下方法改變:

a. 編輯檔案/etc/cloud/management/server.xml、 /etc/cloud/management/server-nonssl.xml及/etc/cloud/management/server-ssl.xml

b. 在每個檔案，找到tag <Service name="Catalina7080">，在此tag，找尋<Connector executor="tomcatThreadPool-internal" port= ....<

c. 將通訊埠改成您想要的，然後儲存

d. 重新啓動 Management Server

如果您重新安裝CloudStack，您需要重新啓用服務及更新通訊埠

11.4. AWS API User Setup

通常，使用者不用擔心使用CloudStack提供的翻譯版本，他們僅需要送出AWS API 到 CloudStack終端即可，並且終端會翻譯呼叫到本地CloudStack API。Amazon EC2 compatible interface使用者可以保留EC2 tools、scripts及CloudStack deployment，只要指定管理伺服器及使用適當的使用者證明即可。每個使用者必須執行下設定:

・產生使用者證明

・註冊

・方便起見，建立環境變數給EC2 SOAP command-line tools

11.4.1. AWS API User Registration

每個使用者執行一次性的註冊，請依照以下步驟:

1. 使用CloudStack使用者介面取得資訊，使用API或詢問雲端管理者皆可:

   ・CloudStack 伺服器的publicly允許DNS名稱或IP位址

   ・使用者帳戶的Access key 及 Secret key

2. 產生一個private key及一個self-signed X.509 certificate。使用者可以替換自己喜歡的儲存位置 /path/to/…

   ```
   $ openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /path/to/private_key.pem -out /path/to/
   cert.pem
   ```

3. 使用AWS相容服務註冊user X.509 certificate及Access/Secret keys，如果您有CloudStack原始碼，請到awsapi-setup/setup 資料夾並使用Python script cloudstack-aws-api-register。如果您沒有原始碼，請使用以下指令下載:

   ```
   wget -O cloudstack-aws-api-register "https://git-wip-us.apache.org/repos/asf?
   p=cloudstack.git;a=blob_plain;f=awsapi-setup/setup/cloudstack-aws-api-register;hb=4.1"[2]
   ```

   然後執行，使用在步驟1取得的access and secret keys。範例如下

   ```
   $ cloudstack-aws-api-register --apikey=User's CloudStack API key --secretkey=User's CloudStack Secret key
    --cert=/path/to/cert.pem --url=http://CloudStack.server:7080/awsapi
   ```

注意

已有AWS certificate的使用者可以選擇使用相同的證明，但是請注意，證明會上傳到CloudStack管理伺服器資料庫

[2] https://git-wip-us.apache.org/repos/asf?p=cloudstack.git;a=blob_plain;f=awsapi-setup/setup/cloudstack-aws-api-register;hb=4.1

11.4.2. AWS API Command-Line Tools Setup

使用者必須執行以下步驟，才能使用EC2 command-line tools:

1. 確定您有正確的EC2 Tools版本，支援版本http://s3.amazonaws.com/ec2-downloads/ec2-api-tools-1.3-62308.zip

2. 建立EC2環境變數，可在您使用服務時設定，或是在shell profile建立，取代終端(也就是EC2_URL)為適當的 CloudStack 管理伺服器及通訊埠位置，在bash shell輸入以下:

```
$ export EC2_CERT=/path/to/cert.pem
$ export EC2_PRIVATE_KEY=/path/to/private_key.pem
$ export EC2_URL=http://localhost:7080/awsapi
$ export EC2_HOME=/path/to/EC2_tools_directory
```

11.5. 使用Timeouts來確保AWS API Command Completion

Amazon EC2 command-line tools有預設的連結超時時間，使用CloudStack時，有些指令會需要較長的時間，如果您發現這些指令因超時而未完成，您需要額外指定超時時間，您可加入以下選擇性 command-line欄位到任一 CloudStack-supported EC2 command:

`--connection-timeout TIMEOUT`	指定一個連結超時時間(秒)，例如: `--connection-timeout 30`
`--request-timeout TIMEOUT`	指定一個需要的超時時間(秒)，例如: `--request-timeout 45`

例如:

```
ec2-run-instances 2 —z us-testl —n 1-3 --connection-timeout 120 --request-timeout 120
```

注意

超時選擇性變數並不會指定到 CloudStack

11.6. 支援AWS API的呼叫

以下為Amazon EC2指令，當AWS API相容介面啓用時，由CloudStack支援。有一些指令，CloudStack及Amazon EC2會不同，不同的部份會註記。基本的SOAP呼叫都會給，想建立工具的開發者不用擔心

表格 11.1. Elastic IP API對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-allocate-address	AllocateAddress	associateIpAddress
ec2-associate-address	AssociateAddress	enableStaticNat
ec2-describe-addresses	DescribeAddresses	listPublicIpAddresses
ec2-diassociate-address	DisassociateAddress	disableStaticNat

EC2指令	SOAP call	CloudStack API呼叫
ec2-release-address	ReleaseAddress	disassociateIpAddress

表格 11.2. Availability Zone API 對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-describe-availability-zones	DescribeAvailabilityZones	listZones

表格 11.3. Images API 對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-create-image	CreateImage	createTemplate
ec2-deregister	DeregisterImage	DeleteTemplate
ec2-describe-images	DescribeImages	listTemplates
ec2-register	RegisterImage	registerTemplate

表格 11.4. Image Attributes API 對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-describe-image-attribute	DescribeImageAttribute	listTemplatePermissions
ec2-modify-image-attribute	ModifyImageAttribute	updateTemplatePermissions
ec2-reset-image-attribute	ResetImageAttribute	updateTemplatePermissions

表格 11.5. Instances API 對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-describe-instances	DescribeInstances	listVirtualMachines
ec2-run-instances	RunInstances	deployVirtualMachine
ec2-reboot-instances	RebootInstances	rebootVirtualMachine
ec2-start-instances	StartInstances	startVirtualMachine
ec2-stop-instances	StopInstances	stopVirtualMachine
ec2-terminate-instances	TerminateInstances	destroyVirtualMachine

表格 11.6. Instance 分配對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-describe-instance-attribute	DescribeInstanceAttribute	listVirtualMachines

表格 11.7. Keys Pairs 對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-add-keypair	CreateKeyPair	createSSHKeyPair
ec2-delete-keypair	DeleteKeyPair	deleteSSHKeyPair
ec2-describe-keypairs	DescribeKeyPairs	listSSHKeyPairs
ec2-import-keypair	ImportKeyPair	registerSSHKeyPair

表格 11.8. Passwords API 對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-get-password	GetPasswordData	getVMPassword

表格 11.9. Security Groups API 對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-authorize	AuthorizeSecurityGroupIngress	authorizeSecurityGroupIngress
ec2-add-group	CreateSecurityGroup	createSecurityGroup
ec2-delete-group	DeleteSecurityGroup	deleteSecurityGroup
ec2-describe-group	DescribeSecurityGroups	listSecurityGroups
ec2-revoke	RevokeSecurityGroupIngress	revokeSecurityGroupIngress

表格 11.10. Snapshots API 對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-create-snapshot	CreateSnapshot	createSnapshot
ec2-delete-snapshot	DeleteSnapshot	deleteSnapshot
ec2-describe-snapshots	DescribeSnapshots	listSnapshots

表格 11.11. Volumes API 對照

EC2指令	SOAP call	CloudStack API呼叫
ec2-attach-volume	AttachVolume	attachVolume
ec2-create-volume	CreateVolume	createVolume
ec2-delete-volume	DeleteVolume	deleteVolume
ec2-describe-volume	DescribeVolume	listVolumes
ec2-detach-volume	DetachVolume	detachVolume

11.7. 範例

有很多tool支援使用AWS compatible API，此章節提供一些建構的範例

11.7.1. Boto 範例

Boto是一種Python package，可在https://github.com/boto/boto 取得。此章節提供兩個使用Boto的例子，已在CloudStack AWS API Interface測試過

第一個為EC2範例，取代 Access and Secret Keys為您自己的，並更新終端

範例 11.1. EC2 Boto範例

```
#!/usr/bin/env python

import sys
import os
import boto
import boto.ec2

region = boto.ec2.regioninfo.RegionInfo(name="ROOT",endpoint="localhost")
apikey='GwNnpUPrO6KgIdZu01z_ZhhZnKjtSdRwuYd4DvpzvFpyxGMvrzno2q05MB0ViBoFYtdqKd'
secretkey='t4eXLEYWw7chBhDlaKf38adCMSHx_w1ds6JfSx3z9fSpSOm0AbP9MoJ0oGIzy2LSC8iw'

def main():
 '''Establish connection to EC2 cloud'''
        conn =boto.connect_ec2(aws_access_key_id=apikey,
                        aws_secret_access_key=secretkey,
                        is_secure=False,
                        region=region,
```

```
                        port=7080,
                        path="/awsapi",
                        api_version="2010-11-15")

        '''Get list of images that I own'''
 images = conn.get_all_images()
 print images
 myimage = images[0]
 '''Pick an instance type'''
 vm_type='m1.small'
 reservation = myimage.run(instance_type=vm_type,security_groups=['default'])

if __name__ == '__main__':
 main()
```

第二個為S3範例，取代Access and Secret keys為您自己的，也取代終端的。確定更新檔案路徑到您機器上

範例 11.2. S3 Boto範例

```
#!/usr/bin/env python

import sys
import os
from boto.s3.key import Key
from boto.s3.connection import S3Connection
from boto.s3.connection import OrdinaryCallingFormat

apikey='ChOw-pwdcCFy6fpeyv6kUaR0NnhzmG3tE7HLN2z30B_s-ogF5H,jZtN4rnzKnq2U,jtnHeg_yLA5gOw'
secretkey='IMY8R7CJQiSGFk4cHwfXXN3DUFXzO7cCiU80eM3MCmfLs7kusgyOfm0g9qzXRXhoAPCH-IRxXc3w'

cf=OrdinaryCallingFormat()

def main():
 '''Establish connection to S3 service'''
        conn =S3Connection(aws_access_key_id=apikey,aws_secret_access_key=secretkey, \
                           is_secure=False, \
                           host='localhost', \
                           port=7080, \
                           calling_format=cf, \
                           path="/awsapi/rest/AmazonS3")

        try:
            bucket=conn.create_bucket('cloudstack')
            k = Key(bucket)
            k.key = 'test'
            try:
               k.set_contents_from_filename('/Users/runseb/Desktop/s3cs.py')
            except:
               print 'could not write file'
               pass
        except:
            bucket = conn.get_bucket('cloudstack')
            k = Key(bucket)
            k.key = 'test'
            try:
               k.get_contents_to_filename('/Users/runseb/Desktop/foobar')
            except:
               print 'Could not get file'
               pass

        try:
           bucket1=conn.create_bucket('teststring')
           k=Key(bucket1)
```

```
            k.key('foobar')
            k.set_contents_from_string('This is my silly test')
        except:
            bucket1=conn.get_bucket('teststring')
            k = Key(bucket1)
            k.key='foobar'
            k.get_contents_as_string()

if __name__ == '__main__':
 main()
```

11.7.2. JClouds範例

網路設定

完成正確的網路設定對成功安裝CloudStack是很重要的，這個章節教您如何做決定及正確設定網路

12.1. 基本與進階網路

CloudStack提供兩種網路範本:

基本

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，但需要比基本網路更多的設定步驟

每個區域都有基本或進階其中一種網路，選擇及在CloudStack設定後，就不能變更了

以下為比較網路功能的表格

網路功能	基本網路	進階網路
網路數量	單一網路	多網路
防火牆型態	實體	實體及虛擬
負載平衡氣	實體	實體及虛擬
隔離類型	Layer 3	Layer 2 及 Layer 3
支援VPN	No	Yes
通訊埠轉送	實體	實體及虛擬
1:1 NAT	實體	實體及虛擬
Source NAT	No	實體及虛擬
使用者資料	Yes	Yes
網路使用監控	sFlow / netFlow，位於實體路由器	超級監督者及虛擬路由器
DNS 及 DHCP	Yes	Yes

這兩種類型可能會用在同一個雲端，但一個區域只能是基本或進階網路

不同網路流量可以在相同的實體網路分段，訪客流量可以用帳戶分段。您可以使用分離VLAN來隔離流量。如果您在單一實體網路使用分離VLAN，請確定VLAN tag 在分離的數個範圍

12.2. VLAN Allocation Example

VLANs are required for public and guest traffic. The following is an example of a VLAN allocation scheme:

VLAN IDs	Traffic type	Scope
less than 500	Management traffic. Reserved for administrative purposes.	CloudStack software can access this, hypervisors, system VMs.

VLAN IDs	Traffic type	Scope
500-599	VLAN carrying public traffic.	CloudStack accounts.
600-799	VLANs carrying guest traffic.	CloudStack accounts. Account-specific VLAN is chosen from this pool.
800-899	VLANs carrying guest traffic.	CloudStack accounts. Account-specific VLAN chosen by CloudStack admin to assign to that account.
900-999	VLAN carrying guest traffic	CloudStack accounts. Can be scoped by project, domain, or all accounts.
greater than 1000	Reserved for future use	

12.3. 硬體設定範例

此章節包含特定交換器模組r zone-level layer-3的交換範例設定，此假設VLAN管理協定，像是VTP或GVRP，是停用的。如果您選擇使用VTP或GVRP，程式碼就需要修改

12.3.1. Dell 62xx

The following steps show how a Dell 62xx is configured for zone-level layer-3 switching. These steps assume VLAN 201 is used to route untagged private IPs for pod 1, and pod 1's layer-2 switch is connected to Ethernet port 1/g1.

The Dell 62xx Series switch supports up to 1024 VLANs.

1. 設定資料庫所有VLAN

```
vlan database
vlan 200-999
exit
```

2. Configure Ethernet port 1/g1.

```
interface ethernet 1/g1
switchport mode general
switchport general pvid 201
switchport general allowed vlan add 201 untagged
switchport general allowed vlan add 300-999 tagged
exit
```

The statements configure Ethernet port 1/g1 as follows:

- VLAN 201 is the native untagged VLAN for port 1/g1.
- All VLANs (300-999) are passed to all the pod-level layer-2 switches.

12.3.2. Cisco 3750

The following steps show how a Cisco 3750 is configured for zone-level layer-3 switching. These steps assume VLAN 201 is used to route untagged private IPs for pod 1, and pod 1's layer-2 switch is connected to GigabitEthernet1/0/1.

1. 設定VTP模式為透明，此允許我們使用超過1000個 VLAN ID。由於我們最多只能用999個，並不强制使用vtp transparent mode

```
vtp mode transparent
vlan 200-999
exit
```

2. Configure GigabitEthernet1/0/1.

```
interface GigabitEthernet1/0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 201
exit
```

The statements configure GigabitEthernet1/0/1 as follows:

- VLAN 201 is the native untagged VLAN for port GigabitEthernet1/0/1.
- Cisco passes all VLANs by default. As a result, all VLANs (300-999) are passed to all the pod-level layer-2 switches.

12.4. Layer-2交換器

layer-2 交換器是在pod中，交換器層級的入口

- 它須集結所有VLAN到每個主機
- 它會交換包含運算及儲存主機的管理網路流量，layer-3交換器會作為管理網路的閘道

範例設定

此章節包含特定交換器模組pod-level layer-2的交換範例設定，此假設VLAN管理協定，像是VTP或GVRP，是停用的。如果您選擇使用VTP或GVRP，程式碼就需要修改

12.4.1. Dell 62xx

以下步驟為如何在pod-level layer-2 switching設定 Dell 62xx

1. 設定資料庫所有VLAN

```
vlan database
vlan 300-999
exit
```

2. VLAN 201用作建立pod 1 untagged私人IP路線，pod 1與 layer-2交換器連結

```
interface range ethernet all
switchport mode general
switchport general allowed vlan add 300-999 tagged
exit
```

設定所有Ethernet通訊埠如下:

- 所有通訊埠都使用同意種設定
- 所有VLAN(300-999)皆通過layer-2交換器的所有通訊埠

12.4.2. Cisco 3750

以下步驟為如何在pod-level layer-2 switching設定 Cisco 3750

1. 設定VTP模式為透明，此允許我們使用超過1000個 VLAN ID。由於我們最多只能用999個，並不强制使用vtp transparent mode

```
vtp mode transparent
vlan 300-999
exit
```

2. 設定所有通訊埠到dotlq ，並設201為本地VLAN

```
interface range GigabitEthernet 1/0/1-24
switchport trunk encapsulation dotlq
switchport mode trunk
switchport trunk native vlan 201
exit
```

預設，Cisco可以讓所有VLAN通過，Cisco交換器在兩個通訊埠相通時，如果本地VLAN ID不同時會抱怨，這就是為什麼要您在 layer-2 switch設為201的原因

12.5. 硬體防火牆

所有部署應該要有防火牆來保護管理伺服器；詳見Generic Firewall Provisions，有些部署可能會有 Juniper SRX防火牆，作為訪客網路的預設閘道；詳見節 12.5.2，“Juniper SRX的外部訪客防火牆累積(選擇性)”

12.5.1. 通用防火牆規則

硬體防火牆是為以下兩個原因：

- 保護管理伺服器，NAT及通訊埠轉送應設定為從公開網路直接送流量到管理伺服器
- 在管理網路及多區域間建立流量路線，站對站VPN應設在多區域間

您可以建立固定防火牆設定來達到以上目的，防火牆規則及政策不用再改變，任何支援NAT及站對站VPN的硬體防火牆品牌都可以使用

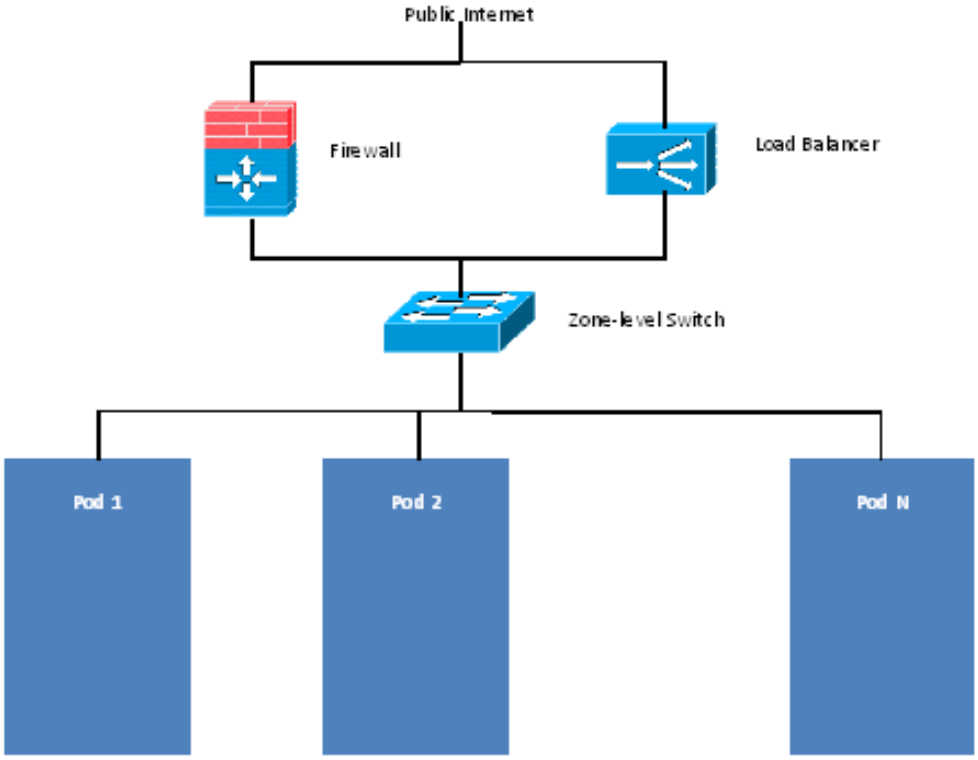
12.5.2. Juniper SRX的外部訪客防火牆累積(選擇性)

注意

僅適用使用進階網路的訪客

CloudStack提供Juniper SRX series直接管理防火牆的功能，此允許 CloudStack 建立static NAT的公開IP及訪客VM對照，並使用Juniper裝置作為虛擬路由器的防火牆，您可以在每個區域內有多個 Juniper SRX，此功能為選擇性，如果沒有配置，CloudStack會使用虛擬路由器

Juniper SRX可以選擇性地與外部負載平衡器連結，外部網路元素可以設為side-by-side或inline 連結



CloudStack需要Junipe設定為下:

注意

支援SRX的版本為10.3或更高

1. 根據供應商指示安裝您的SRX工具
2. 連結一個介面到管理網路，及一個介面到公開網路。您可以連結相同的介面到兩個網路，使用一個VLAN連到公衆網路
3. 確定"vlan-tagging"在私人介面是啓用的
4. 記錄公開及私人介面名稱，如果您使用VLAN連結公開介面，請加一個".[VLAN TAG]"在介面名稱後面，例如，您使用ge-0/0/3連到公開網路，VLAN tag 301，您的公開網路介面名稱應該為"ge-0/0/3.301"。您的私人介面名稱應維持相同，因為 CloudStack會自動建立邏輯介面
5. 建立公開安全區及私人安全區，預設上，這些都已經存在，並稱為"untrust" 及 "trust"，將公開介面加到公開區；私人介面加到私人區，記下安全區的名稱
6. 確定私人區到公開區的安全政策允許所有流量
7. 記下帳戶的使用者名稱及密碼，此帳戶為CloudStack 編譯規則時的登入口
8. 確定"ssh" 及 "xnm-clear-text"系統服務啓用

9. 如果想要流量計量:

   a. a.建立輸入防火牆過濾器及輸出防火牆過濾器，這些過濾器必須在公開及私人安全區內悶別是相同的名稱，過濾器應設為"interface-specific"，例如，以下為公開區是 "untrust"；私人區是"trust"的設定

```
root@cloud-srx# show firewall
filter trust {
    interface-specific;
}
filter untrust {
    interface-specific;
}
```

   b. 加入防火牆過濾器到您的公開介面，例如，範例設定結果(對於公開介面：ge-0/0/3.0，公開安全區： untrust，及私人安全區：trust)為:

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

10. 確定所有VLAN都已經在SRX的私人介面

11. 安裝CloudStack管理伺服器後，以管理者登入CloudStack使用者介面

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

13. 於Zones的方框中點選View More

14. 選擇想要套用的區域

15. 選擇Network標籤

16. 在圖中的 Network Service Providers節點，點選Configure(您可能會需要滾動畫面)

17. 點選SRX

18. 選擇Add New SRX (+) 並提供以下:

    - IP Address：SRX的IP位址
    - Username：SRX的使用者名稱，CloudStack會使用
    - Password：帳戶密碼
    - Public Interface：公開介面的名稱，例如ge-0/0/2，".x" 結尾表示使用VLAN
    - Private Interface：私人介面的名稱，例如，ge-0/0/1
    - Usage Interface：(選擇性)通常，公開介面用來計量流量，如果您想要用不同的介面，請指定
    - Number of retries：嘗試指令的次數，不包含失敗，預設為2

- Timeout (seconds): 在判斷失敗前, 等待指令的時間, 預設為300秒
- Public Network: 公衆網路名稱, 例如: trust
- Private Network: 私人網路名稱, 例如: untrust
- Capacity: 裝置可以處理的網路數量
- 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

19. 按OK
20. 點選Global Settings, 設定欄位external.network.stats.interval來指定您想要CloudStack多常從 Juniper SRX抓取一次網路使用統計, 如果您不是使用SRX, 請社為0

12.5.3. 外部訪客負載平衡器累積(選擇性)

CloudStack可以使用 Citrix NetScaler或BigIP F5負載平衡器來提供負載平衡服務, 如果沒有啓用, CloudStack會使用虛擬路由器中的負載平衡軟體

想要安裝及啓用:

1. 根據廠商指示設定產品
2. 連接到搭載公開流量及管理流量的網路(可能為同一網路)
3. 記錄IP位址、使用者名稱、密碼、公開介面名稱及私人介面名稱, 介面名稱會像是"1.1" 或"1.2"
4. 確定VLAN已經塞進管理網路介面
5. 安裝CloudStack管理伺服器後, 以管理者登入CloudStack使用者介面
6. 於左側的navigation按鈕中, 點選Infrastructure。
7. 於Zones的方框中點選View More
8. 選擇想要套用的區域
9. 選擇Network標籤
10. 在圖中的 Network Service Providers節點, 點選Configure(您可能會需要滾動畫面)
11. 選擇NetScaler 或 F5
12. 選擇Add button (+) 並提供以下:

    對於NetScaler:

    - IP Address: SRX的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: 已被加入的裝置類型, 可能為F5 Big Ip Load Balancer、NetScaler VPX、NetScaler MPX, 或 NetScaler SDX。關於類型的比較, 詳見CloudStack Administration Guide
    - Public interface: 裝置介面, 設定為公開網路的一部份
    - Private interface: 裝置介面, 設定為私人網路的一部份

- Number of retries: 嘗試指令的次數，不包含失敗，預設為2
- Capacity: 裝置可以處理的網路數量
- 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

13. 按OK

安裝及配置完成，您可以進行新增VMs 及NAT或負載平衡規則

12.6. 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.

12.7. 拓樸需

12.7.1. 安全性需求

公開網路不能存取管理伺服器的8096及8250通訊埠

12.7.2. 執行期間的內部通訊需求

- 管理伺服器會互相協調任務，此通信使用TCP的8250及9090通訊埠
- 控制台代理VM連結所有區域內主機，因此區域內任一pod的管理流量網路必須能與其他區域內的pod連線
- 次要儲存VM及控制台代理VM使用8250通訊埠與管理伺服器通信，如果您是使用多管理伺服器，在8250通訊埠地管理伺服器的負載平衡IP位址必需可到達

12.7.3. 儲存網路拓樸需求

次要儲存NFS匯出由次要儲存VM掛載，即使有分離儲存網路，次要儲存流量仍會經過管理流量網路。主要儲存流量如果可用的話，會經過儲存網路。如果您選擇將次要儲存NFS伺服器置於儲存網路，您必須確定在管理流量網路及儲存網路間存在路徑

12.7.4. External Firewall Topology Requirements

When external firewall integration is in place, the public IP VLAN must still be trunked to the Hosts. This is required to support the Secondary Storage VM and Console Proxy VM.

12.7.5. 進階區域拓樸需求

在Advanced Networking，分離子網路必須使用為私人或公開網路

12.7.6. XenServer拓樸需求

管理伺服器與XenServer主機溝通的埠為22(ssh)，80(HTTP)，443(HTTPs)

12.7.7. VMware拓樸需求

- 管理伺服器及次要儲存裝置VM必須能夠存取 vCenter及所有ESXi主機，為了能夠通過防火牆，請開啓 port 443
- 管理伺服器與 VMware vCenter伺服器使用port 443(HTTPs)溝通
- 管理伺服器在管理流量網路中，使用port 3922(ssh)與System VMs溝通

12.7.8. KVM拓樸需求

管理伺服器與KVM主機使用22通訊埠(ssh)溝通

12.8. Traffic Sentinel的訪客網路使用累計

CloudStack需要從外部網路的統計收集器來收集訪客網路使用資料，計量訪客網路統計可以藉由使用 inMon Traffic Sentinel的CloudStack累計取得

Traffic Sentinel是一種網路流量的資料收集封包，CloudStack可以從Traffic Sentinel送出統計到自己的使用紀錄，提供計費使用者的基礎。Traffic Sentinel使用流量監控協定sFlow#。路由器及交換器產生sFlow紀錄，並提供Traffic Sentinel收集，然後CloudStack可以詢問Traffic Sentinel 資料庫來取得資訊

CloudStack 決定哪個訪客IP在現在的詢問階段正在使用，此包含新指定的IP及之前指定的IP。 CloudStack 詢問Traffic Sentinel這些IP分配到 CloudStack這段時間的網路統計，回復資料與擁有IP 及 timestamps 的客戶帳戶相關， timestamps 在IP指定及釋出時，建立 CloudStack收費計量紀錄。 當使用伺服器執行時，timestamps會收集此資料

想要建立CloudStack 及 Traffic Sentinel間的累計:

1. 在您的網路架構，安裝Traffic Sentinel 並將其設定為收集流量資料。關於安裝及設定步驟，詳見 Traffic Sentinel Documentation[1]的 inMon文件
2. 在Traffic Sentinel使用者介面設定Traffic Sentinel ，設定為允許從訪客使用者使用程式詢問。 CloudStack會做為訪客使用者遠端詢問收集資料

   點選 File > Users > Access Control > Reports Query，然後從下拉式列表點選Guest from
3. On CloudStack, add the Traffic Sentinel host by calling the CloudStack API command addTrafficMonitor. Pass in the URL of the Traffic Sentinel as protocol + host + port

[1] http://inmon.com.

(optional); for example, http://10.147.28.100:8080. For the addTrafficMonitor command syntax, see the API Reference at API Documentation[2].

For information about how to call the CloudStack API, see the Developer's Guide at CloudStack API Developer's Guide[3].

4. 以administrator身分登入CloudStack UI

5. 在Global Settings頁面選擇Configuration, 然後設定以下:

direct.network.stats.interval: CloudStack 詢問Traffic Sentinel的頻率

12.9. 設定Zone VLAN與執行VM最大值

In the external networking case, every VM in a zone must have a unique guest IP address. There are two variables that you need to consider in determining how to configure CloudStack to support this: how many Zone VLANs do you expect to have and how many VMs do you expect to have running in the Zone at any one time.

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

guest.vlan.bits	Maximum Running VMs per Zone	Maximum Zone VLANs
12	4096	4094
11	8192	2048
10	16384	1024
10	32768	512

Based on your deployment's needs, choose the appropriate value of guest.vlan.bits. Set it as described in Edit the Global Configuration Settings (Optional) section and restart the Management Server.

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

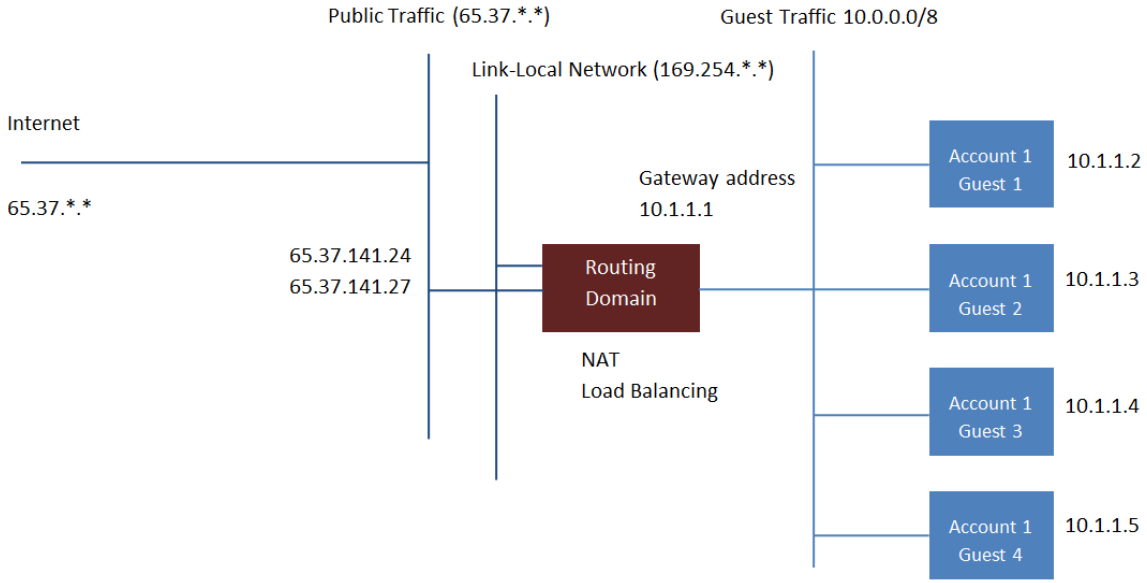
管理網路及流量

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

13.1. 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

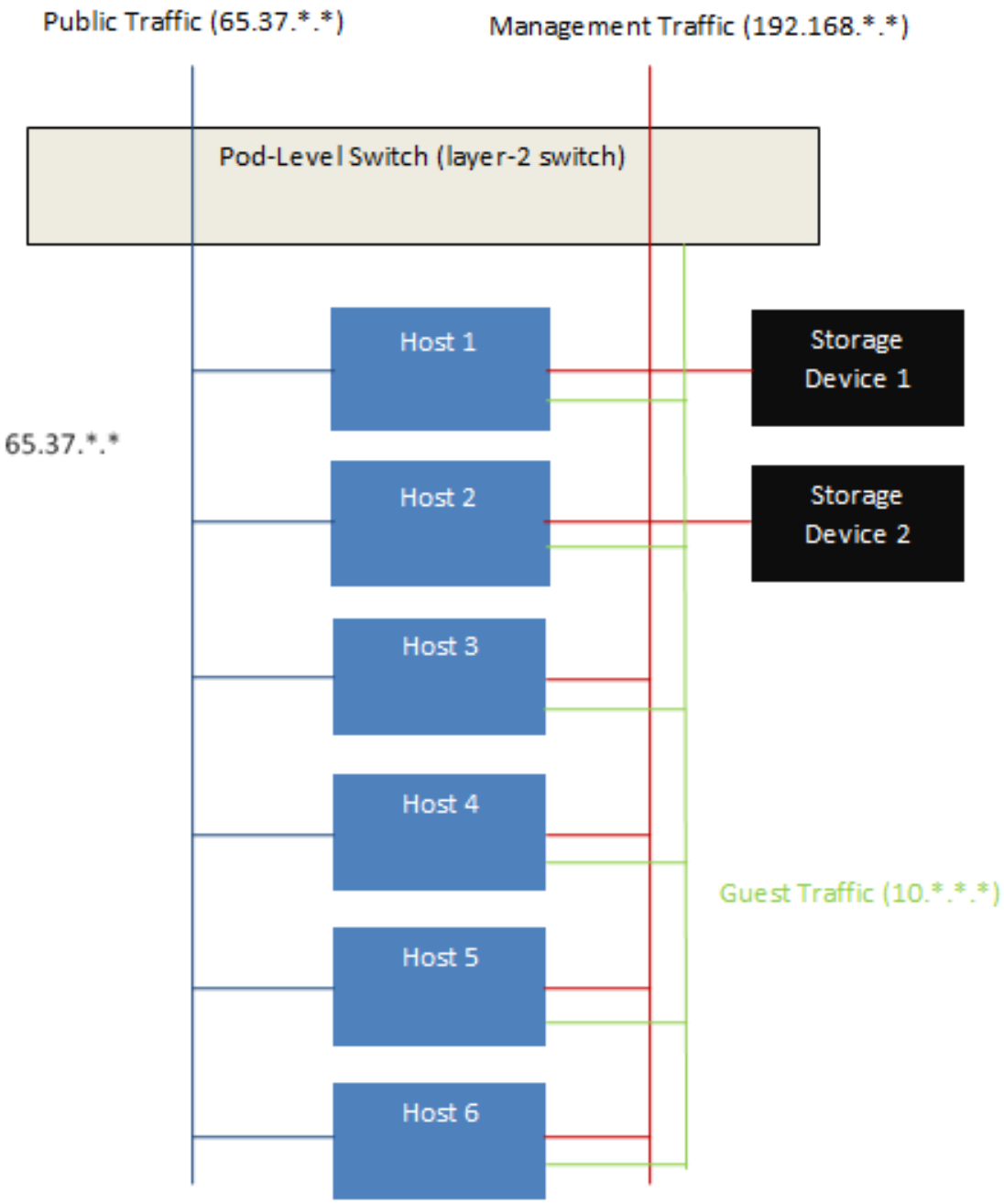
管理伺服器會自動建立虛擬路由器。虛擬路由器是一種在主機上執行的特殊虛擬機器，每個虛擬路由器有三個網路介面。eth0用作訪客流量的閘道，IP位址為10.1.1.1；eth1用作系統設定虛擬路由器的介面；eth2指定為公開流量的IP位址

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

13.2. 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

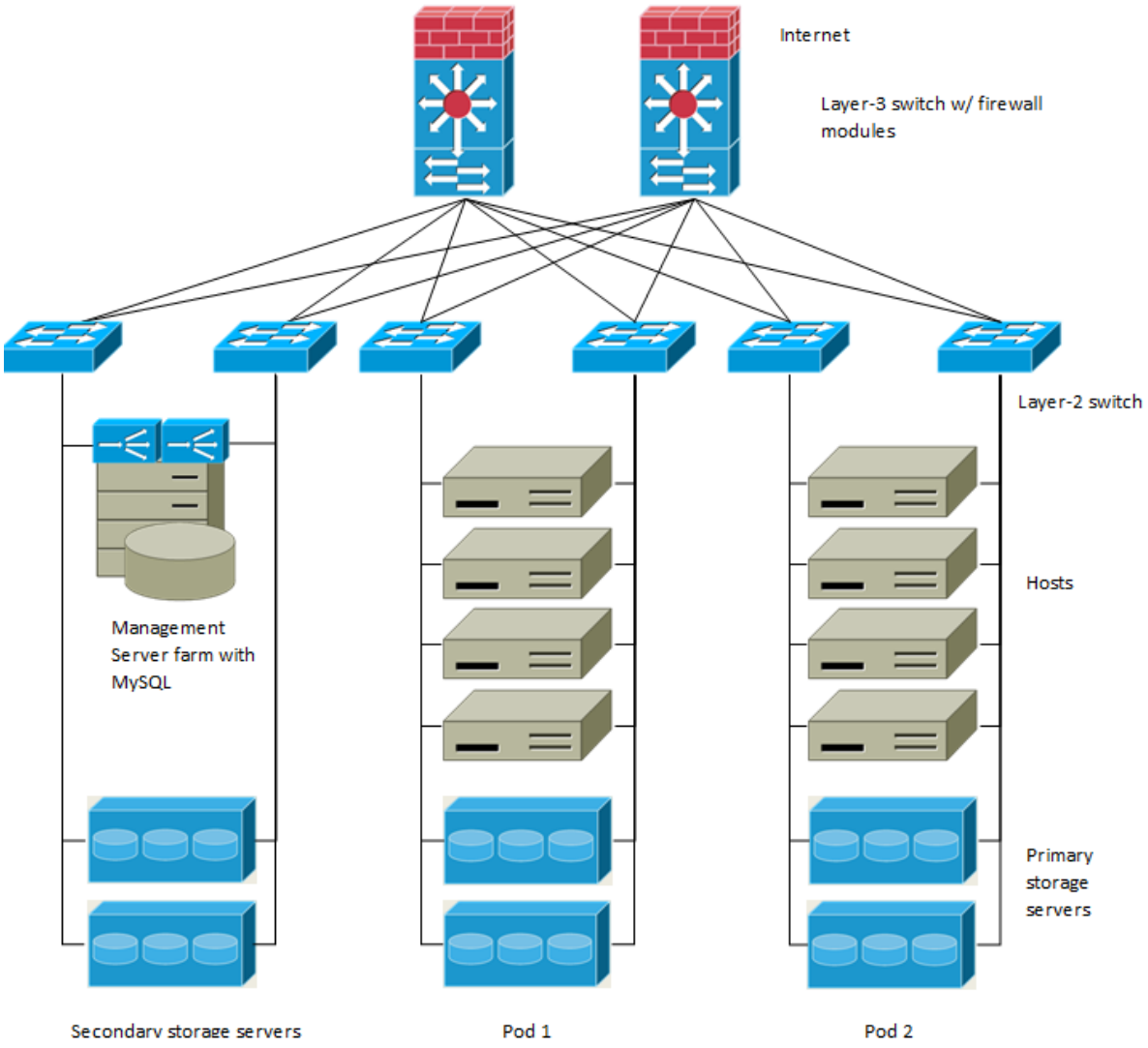
Servers are connected as follows:

- 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.

13.3. 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.

13.4. 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

13.5. 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.

13.5.1. 於Advanced Zone下設定Guest Traffic

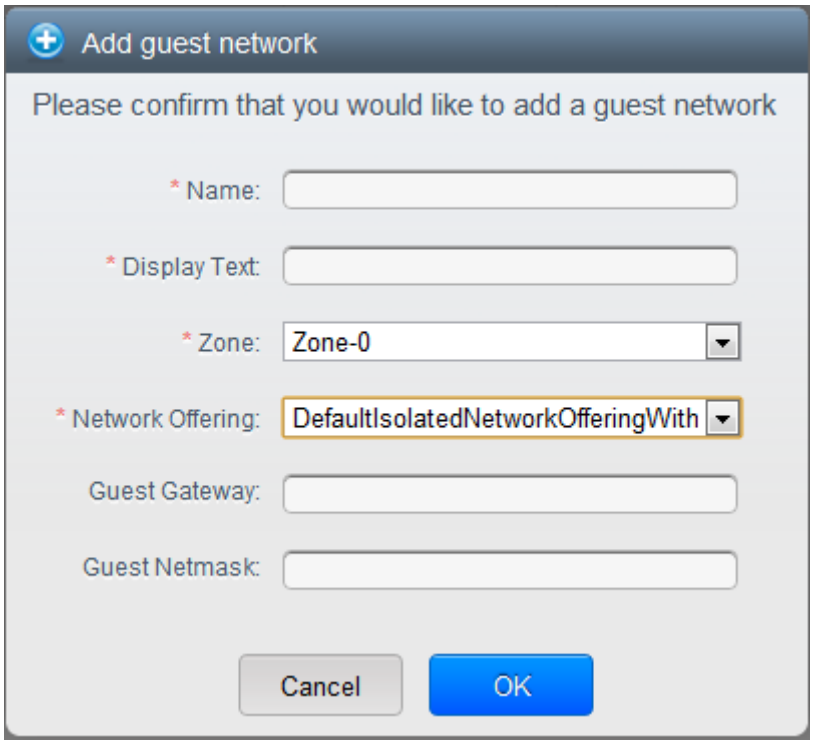
以下步驟將假設您已經登入CloudStack的UI並設定基礎的Guest網段:

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

13.5.2. 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.

13.6. 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.

13.6.1. 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

13.6.2. 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詳見Administrator's Guide的"Stopping and Starting Virtual Machines"
- 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

13.7. Security Groups

13.7.1. 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

13.7.2. 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

13.7.3. (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

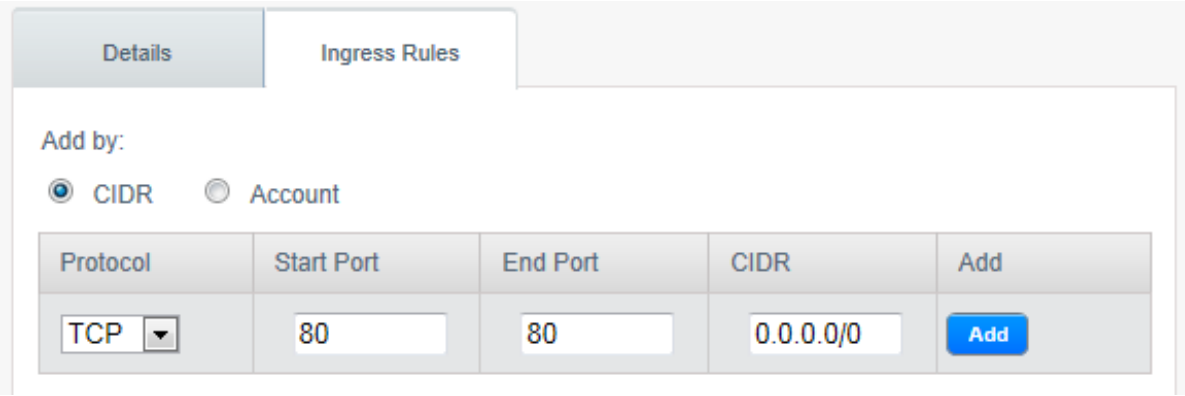
13.7.4. 啓用Security Groups

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

13.7.5. 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

13.8. 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.

13.8.1. 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.

13.8.2. 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
```

13.8.3. 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

13.8.4. 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

13.8.5. 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

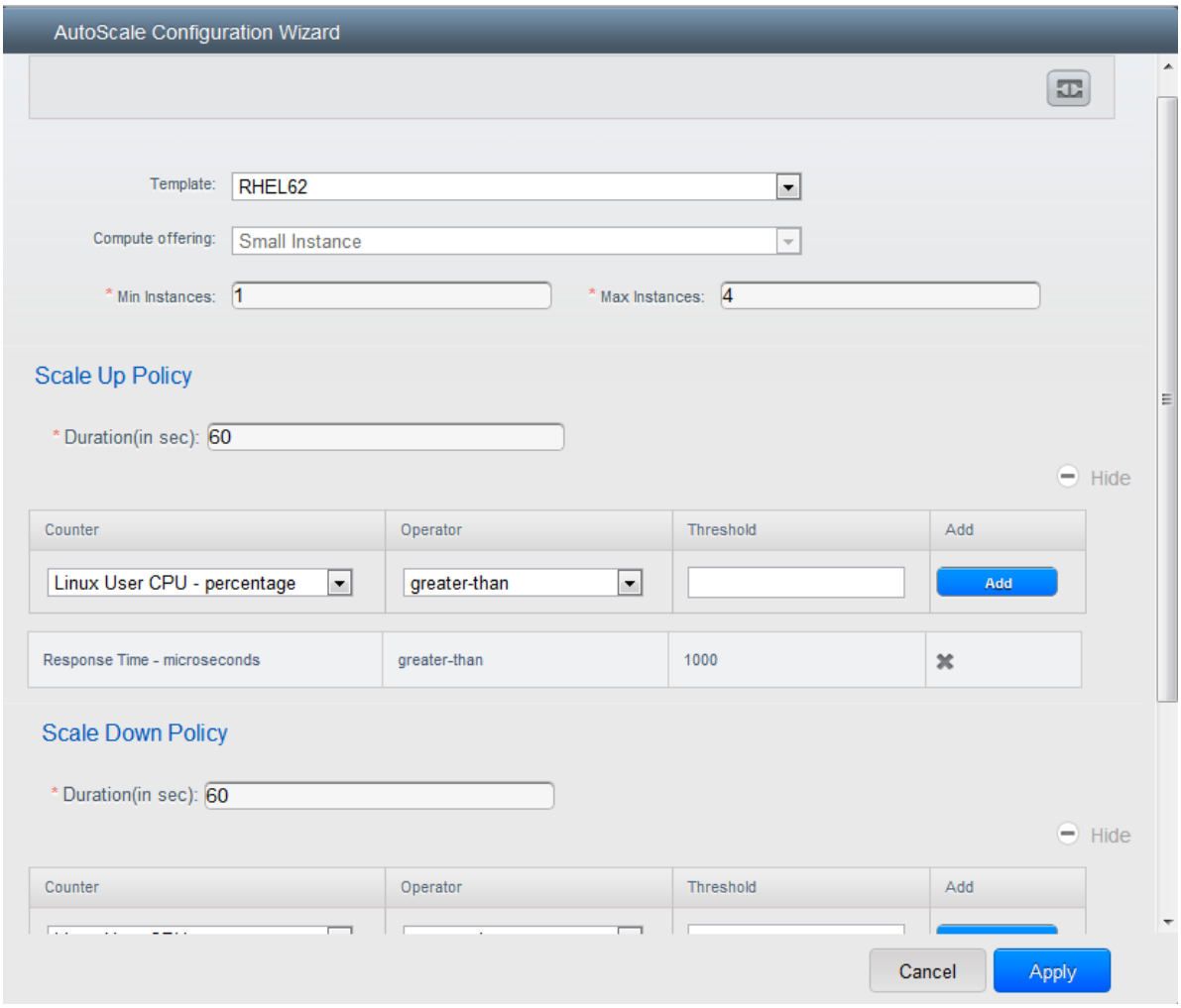
如果應用程式並未執行，NetScaler裝置會認為VM是無效的，並繼續無條件的配置VM，直到資源耗盡

- 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 13.8.2, “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.

13.9. 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

13.9.1. 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 13.8.5, “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

13.9.2. 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.

13.10. 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

13.11. 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

13.12. 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 

13.13. 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

13.13.1. 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

13.14. 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 13.14.1, “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 13.14.2, “Firewall Rules” and 節 13.14.3, “Port Forwarding”.

13.14.1. 建立Advanced區內的

注意

Egress firewall rules 僅支援虛擬路由器

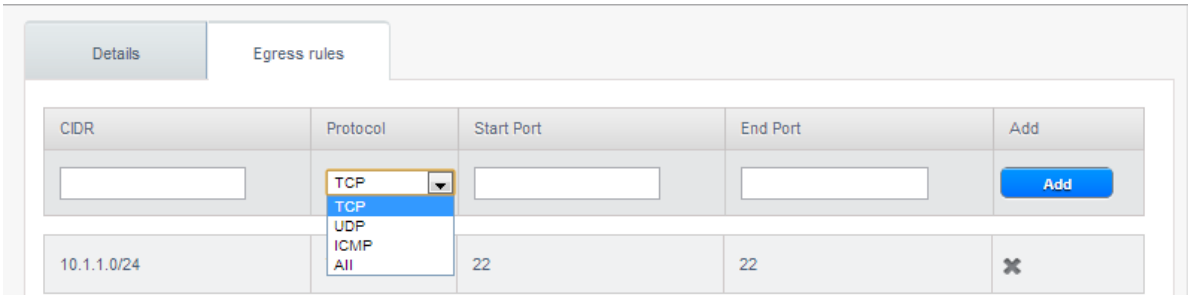
Egress traffic 是從私人網路到公用網路，例如Internet。Egress traffic在預設上是關閉的，也就是訪客網路無法輸出流量到Internet。然而，您可以在 Advanced 新增Egress traffic rule來控制Egress traffic，而套用此規則的流量將允許通過，其他則保持原樣。當所有防火牆規則被移除時，將會回到預設值

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

13.14.2. 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 13.14.1, “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

13.14.3. 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 13.11，“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

13.15. 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

13.16. 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

13.17. 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 13.17.4，“設定 Site-to-Site VPN連線”

13.17.1. 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

13.17.2. 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

13.17.3. 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.

13.17.4. 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 13.19, “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

13.17.4.1. 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

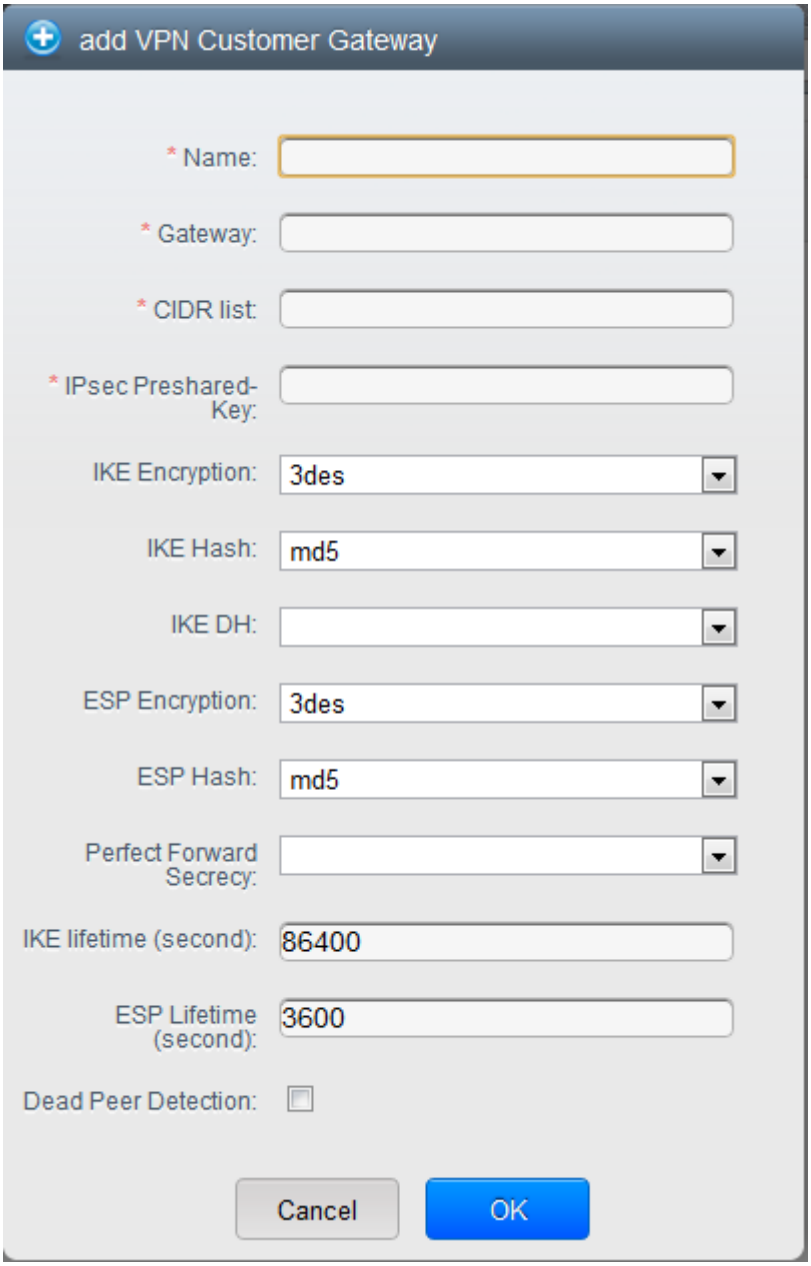
增加VPN客戶閘道:

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

13.17.4.2. 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

13.17.4.3. 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

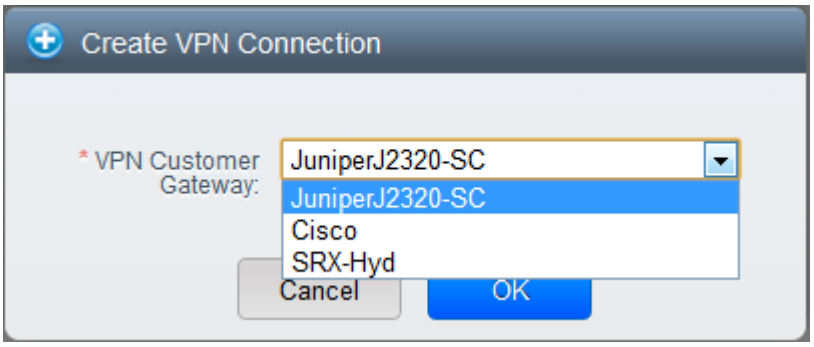
6. 選擇"Site-to-Site VPN"

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

13.17.4.4. 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 

13.18. 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 13.17.4.2, “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 13.19.5, “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

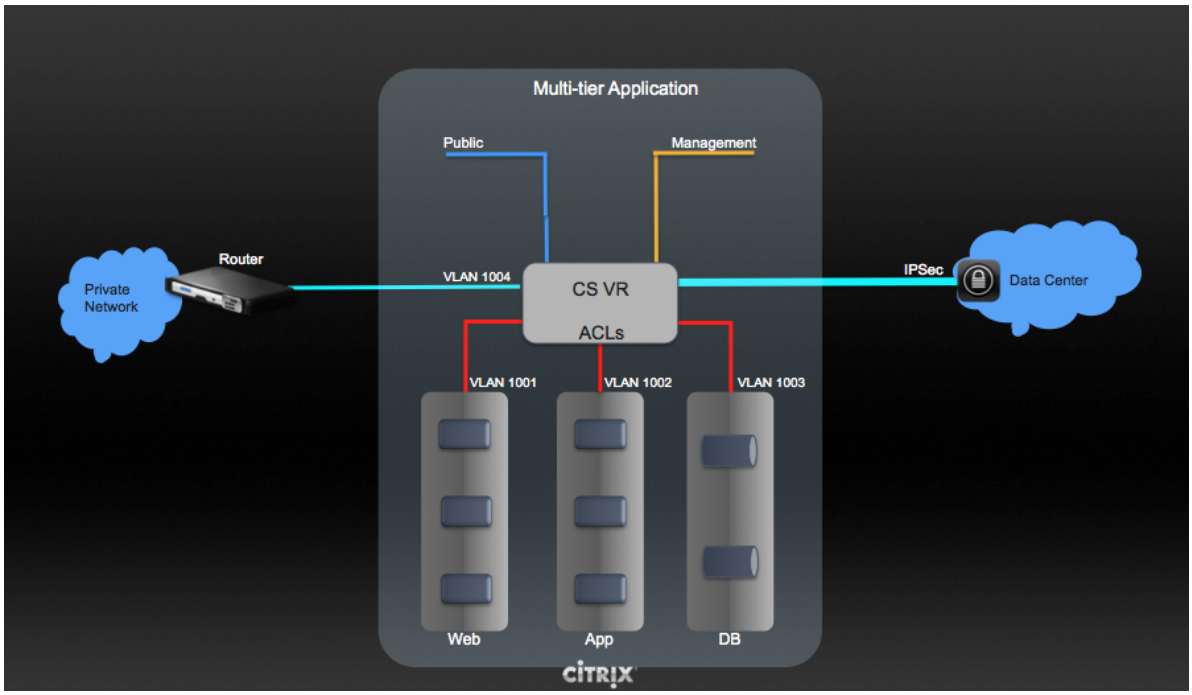
  例如:

  - 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 13.19, “設定虛擬私人雲端”

13.19. 設定虛擬私人雲端

13.19.1. 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 13.19.5, “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 13.17.4, “設定 Site-to-Site VPN連線”
- Customer Gateway: VPN連線的客戶端。更多資訊，詳見節 13.17.4.1, “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 13.19.9, “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:

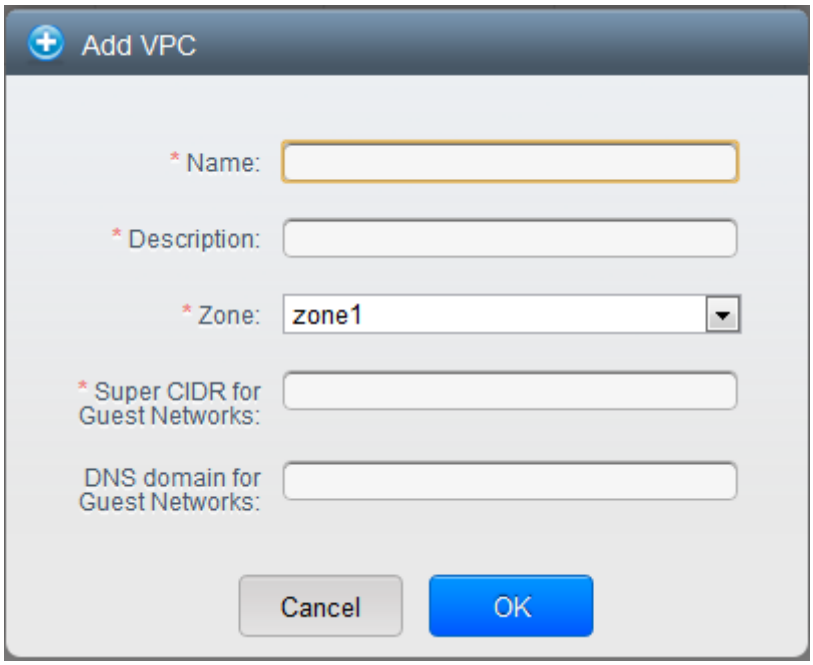
- 建立VPC後，預設為啓用狀態
- VPC僅能在進階區域建立，不能同時屬於多個區域

- 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

13.19.2. 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

13.19.3. 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

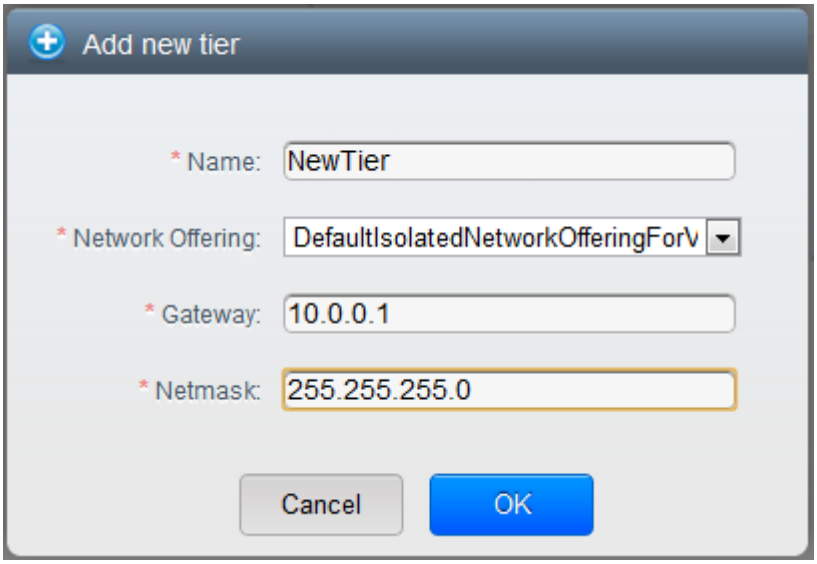
帳戶所有創建的VPC會表列在本頁

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

13.19.4. 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

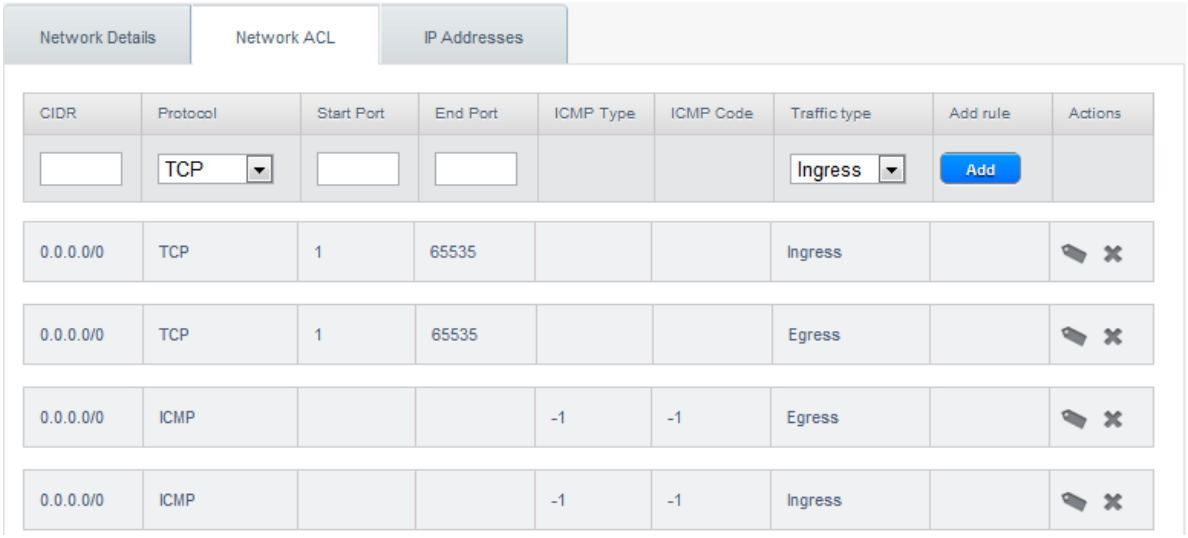
- CIDR: CIDR在 Ingress rules中扮演Source CIDR的腳色; 在Egress rules扮演Destination CIDR的腳色。為了在特定位址區域中允許流量自或到IP位址, 進入CIDR或CIDR的comma-separated list。CIDR是輸入流量的基礎IP。比如說, 192.168.0.0/22, 為了允許所有CIDR, 設定 0.0.0.0/0.
- Protocol: 來源送流量到層級的網路協定。TCP和UDP協定常被用作資料交換和終端使用者傳輸, ICMP協定常被用作傳送錯誤訊息或網路監視資料
- Start Port, End Port (TCP, 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

13.19.5. 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

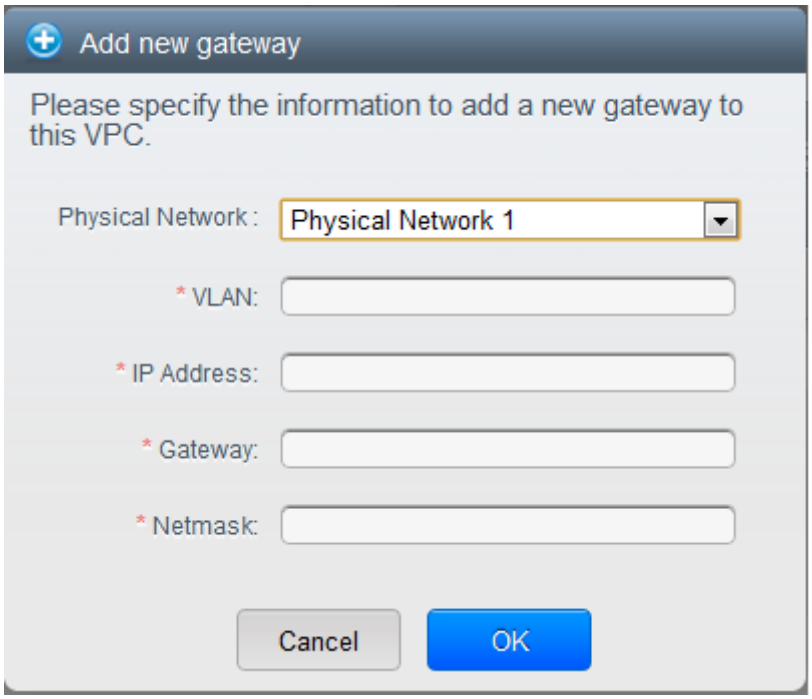
   帳戶所有創建的VPC會表列在本頁
4. 對想要設定load balancing rules的VPC按下"Configure"

   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

13.19.6. 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

13.19.7. 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.

13.19.8. 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 

13.19.9. 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

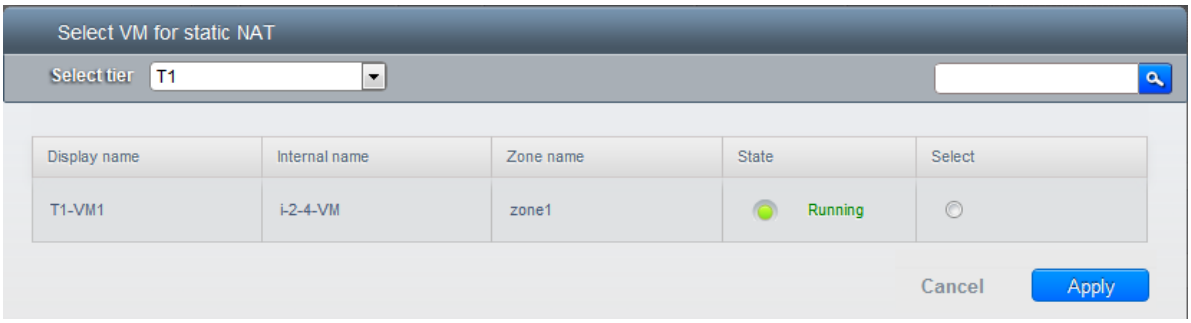
6. 選擇IP Addresses

   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

13.19.10. 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

13.19.11. 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

13.19.12. 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

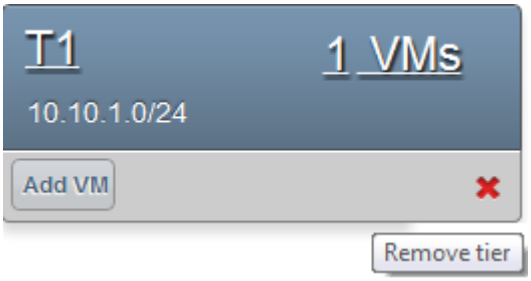
3. 在Select視窗選擇VPC

   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

13.19.13. 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

13.20. 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.

13.20.1. 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.

13.20.2. 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Administration Guide

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

附錄 A. 修訂記錄

修訂 1-0	October 5 2012	Jessica Tomechak , Radhika PC , Wido den Hollander

首次發表