

## Apache CloudStack 4.1.1

# Guia de instalação do CloudStack

Edição 1



## Apache CloudStack

---

### Nota Legal

Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to you under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

### Resumo

Guia de instalação do CloudStack.

---

#### 1. Conceitos

- 1.1. O que é o CloudStack?
- 1.2. O que o CloudStack pode fazer?
- 1.3. Visão geral da arquitetura de implementação
  - 1.3.1. Visão geral da arquitetura de implementação
  - 1.3.2. Visão geral da infraestrutura de nuvem
  - 1.3.3. Visão geral de serviços de rede

#### 2. Conceitos de infraestrutura de nuvem

- 2.1. About Regions
- 2.2. Sobre zonas
- 2.3. Sobre pods
- 2.4. Sobre clusters
- 2.5. Sobre hosts
- 2.6. Sobre storage primária
- 2.7. Sobre storage secundária
- 2.8. Sobre redes físicas
  - 2.8.1. Tipos de tráfego de rede da zona básica
  - 2.8.2. Endereços IP de hóspedes na zona básica
  - 2.8.3. Tipos de tráfego de rede da zona avançada
  - 2.8.4. Endereços IP de hóspedes na zona avançada
  - 2.8.5. Endereços IP públicos na zona avançada
  - 2.8.6. Endereços IP reservados pelo sistema

#### 3. Building from Source

- 3.1. Getting the release
- 3.2. Verifying the downloaded release
  - 3.2.1. Getting the KEYS
  - 3.2.2. GPG
  - 3.2.3. MD5
  - 3.2.4. SHA512
- 3.3. Prerequisites for building Apache CloudStack
- 3.4. Extracting source
- 3.5. Building DEB packages
  - 3.5.1. Setting up an APT repo
  - 3.5.2. Configuring your machines to use the APT repository
- 3.6. Building RPMs from Source
  - 3.6.1. Generating RPMS
- 3.7. Building Non-OSS
- 4. Instalação
  - 4.1. Quem deve ler este documento
  - 4.2. Visão geral dos passos de instalação
  - 4.3. Requerimentos mínimos de sistema
    - 4.3.1. Requerimentos de sistema dos servidores de gerenciamento, database, e storage
    - 4.3.2. Requerimentos de sistema do host/hipervisor
  - 4.4. Configure package repository
    - 4.4.1. DEB package repository
    - 4.4.2. RPM package repository
  - 4.5. Instalação do servidor de gerenciamento
    - 4.5.1. Visão geral da instalação do servidor de gerenciamento
    - 4.5.2. Preparando o sistema operacional
    - 4.5.3. Instale o servidor de gerenciamento no primeiro host.
    - 4.5.4. Instalar o servidor de banco de dados.
    - 4.5.5. Sobre senha e chave de criptografia
    - 4.5.6. Preparar os compartilhamentos NFS
    - 4.5.7. Preparar e ativar servidores de gerenciamento adicionais
    - 4.5.8. Prepare o template de máquina virtual de sistema
    - 4.5.9. Instalação completa! Próximos passos
- 5. Interface do usuário
  - 5.1. Login na interface de usuário
    - 5.1.1. End User's UI Overview
    - 5.1.2. Root Administrator's UI Overview
    - 5.1.3. Fazendo login como o administrador root
    - 5.1.4. Changing the Root Password
  - 5.2. Usando as chaves SSH para autenticação.
    - 5.2.1. Criando um template de instância que suporta chaves SSH
    - 5.2.2. Criando o par de chaves SSH
    - 5.2.3. Criando uma instância
    - 5.2.4. Fazendo login usando o par de chaves SSH
    - 5.2.5. Resetting SSH Keys
- 6. Passos para provisionamento de sua infraestrutura de nuvem
  - 6.1. Visão geral dos passos de provisionamento
  - 6.2. Adding Regions (optional)
    - 6.2.1. The First Region: The Default Region
    - 6.2.2. Adding a Region
    - 6.2.3. Adding Third and Subsequent Regions
    - 6.2.4. Deleting a Region
  - 6.3. Adicionando uma zona
    - 6.3.1. Configuração de zona básica
    - 6.3.2. Advanced Zone Configuration
  - 6.4. Adicionando um pod
  - 6.5. Adicionando um cluster
    - 6.5.1. Add Cluster: KVM or XenServer
    - 6.5.2. Add Cluster: vSphere
  - 6.6. Adding a Host

- 6.6.1. Adding a Host (XenServer or KVM)
  - 6.6.2. Adding a Host (vSphere)
- 6.7. Adicionar Storage Primário
  - 6.7.1. System Requirements for Primary Storage
  - 6.7.2. Adding Primary Storage
- 6.8. Adicionar Storage Secundário
  - 6.8.1. System Requirements for Secondary Storage
  - 6.8.2. Adding Secondary Storage
- 6.9. Initialize and Test
- 7. Global Configuration Parameters
  - 7.1. Setting Global Configuration Parameters
  - 7.2. About Global Configuration Parameters
- 8. Instalação de hipervisor
  - 8.1. Instalação de host hipervisor KVM
    - 8.1.1. Requisitos de sistema para hosts hipervisores KVM
    - 8.1.2. Visão geral da instalação do KVM
    - 8.1.3. Preparando o sistema operacional
    - 8.1.4. Install and configure the Agent
    - 8.1.5. Install and Configure libvirt
    - 8.1.6. Configure the Security Policies
    - 8.1.7. Configure the network bridges
    - 8.1.8. Configure the network using OpenVswitch
    - 8.1.9. Configuring the firewall
    - 8.1.10. Add the host to CloudStack
  - 8.2. Citrix XenServer Installation for CloudStack
    - 8.2.1. System Requirements for XenServer Hosts
    - 8.2.2. XenServer Installation Steps
    - 8.2.3. Configure XenServer dom0 Memory
    - 8.2.4. Usuário e Senha.
    - 8.2.5. Time Synchronization
    - 8.2.6. Licensing
    - 8.2.7. Install CloudStack XenServer Support Package (CSP)
    - 8.2.8. Primary Storage Setup for XenServer
    - 8.2.9. iSCSI Multipath Setup for XenServer (Optional)
    - 8.2.10. Physical Networking Setup for XenServer
    - 8.2.11. Upgrading XenServer Versions
  - 8.3. Instalação e configuração do VMware vSphere
    - 8.3.1. System Requirements for vSphere Hosts
    - 8.3.2. Preparation Checklist for VMware
    - 8.3.3. vSphere Installation Steps
    - 8.3.4. ESXi Host setup
    - 8.3.5. Physical Host Networking
    - 8.3.6. Storage Preparation for vSphere (iSCSI only)
    - 8.3.7. Add Hosts or Configure Clusters (vSphere)
    - 8.3.8. Applying Hotfixes to a VMware vSphere Host
- 9. Additional Installation Options
  - 9.1. Installing the Usage Server (Optional)
    - 9.1.1. Requirements for Installing the Usage Server
    - 9.1.2. Steps to Install the Usage Server
  - 9.2. SSL (Optional)
  - 9.3. Database Replication (Optional)
    - 9.3.1. Failover
- 10. Selecionando a arquitetura de implementação
  - 10.1. Implementação em pequena escala
  - 10.2. Configuração redundante em larga escala
  - 10.3. Rede dedicada de storage
  - 10.4. Servidor multi-node de gerenciamento
  - 10.5. Implementação multi-site
- 11. Amazon Web Services Compatible Interface
  - 11.1. Amazon Web Services Compatible Interface
  - 11.2. Supported API Version
  - 11.3. Enabling the EC2 and S3 Compatible Interface

## 11.3. Enabling the EC2 and SO Compatible Interface

- 11.3.1. Enabling the Services
- 11.3.2. Creating EC2 Compatible Service Offerings
- 11.3.3. Modifying the AWS API Port

## 11.4. AWS API User Setup

- 11.4.1. AWS API User Registration
- 11.4.2. AWS API Command-Line Tools Setup

## 11.5. Using Timeouts to Ensure AWS API Command Completion

## 11.6. Supported AWS API Calls

## 11.7. Examples

- 11.7.1. Boto Examples
- 11.7.2. JClouds Examples

## 12. Configuração de rede

### 12.1. Rede básica e avançada

### 12.2. VLAN Allocation Example

### 12.3. Example Hardware Configuration

- 12.3.1. Dell 62xx
- 12.3.2. Cisco 3750

### 12.4. Layer-2 Switch

- 12.4.1. Dell 62xx
- 12.4.2. Cisco 3750

### 12.5. Hardware Firewall

- 12.5.1. Generic Firewall Provisions
- 12.5.2. External Guest Firewall Integration for Juniper SRX (Optional)
- 12.5.3. External Guest Load Balancer Integration (Optional)

### 12.6. Management Server Load Balancing

### 12.7. Topology Requirements

- 12.7.1. Security Requirements
- 12.7.2. Runtime Internal Communications Requirements
- 12.7.3. Storage Network Topology Requirements
- 12.7.4. External Firewall Topology Requirements
- 12.7.5. Advanced Zone Topology Requirements
- 12.7.6. XenServer Topology Requirements
- 12.7.7. VMware Topology Requirements
- 12.7.8. KVM Topology Requirements

### 12.8. Guest Network Usage Integration for Traffic Sentinel

### 12.9. Setting Zone VLAN and Running VM Maximums

## 13. Gerenciando redes e tráfego

### 13.1. Tráfego de hóspedes

### 13.2. Rede em um pod

### 13.3. Rede em uma zona

### 13.4. Configuração de rede física de zona básica

### 13.5. Configuração de rede física de zona avançada

- 13.5.1. Configure o tráfego hóspede na zona avançada
- 13.5.2. Configure o tráfego público na zona avançada

### 13.6. Usando múltiplas redes hóspedes

- 13.6.1. Adicionando uma rede hóspede adicional
- 13.6.2. Alterando a oferta de rede em uma rede hóspede

### 13.7. Grupos de segurança

- 13.7.1. About Security Groups
- 13.7.2. Adicionando um grupo de segurança
- 13.7.3. Security Groups in Advanced Zones (KVM Only)
- 13.7.4. Habilitando grupos de segurança
- 13.7.5. Adicionando regras de ingresso e egresso a um grupo de segurança

### 13.8. Firewalls e balanceadores de carga externos

- 13.8.1. Sobre a utilização do balanceador de carga NetScaler
- 13.8.2. Configuring SNMP Community String on a RHEL Server
- 13.8.3. Configuração inicial de firewalls e balanceadores de carga externos
- 13.8.4. Configuração continuada de firewalls e balanceadores de carga externos
- 13.8.5. Configuring AutoScale

### 13.9. Regras de balanceamento de carga

- 13.9.1. Adding a Load Balancer Rule
- 13.9.2. Sticky Session Policies for Load Balancer Rules
- 13.10. Guest IP Ranges
- 13.11. Obtendo um novo endereço IP
- 13.12. Liberando um endereço IP
- 13.13. NAT estática
  - 13.13.1. Habilitando ou desabilitando NAT estática
- 13.14. Encaminhamento de IP e firewall
  - 13.14.1. Creating Egress Firewall Rules in an Advanced Zone
  - 13.14.2. Regras de firewall
  - 13.14.3. Encaminhamento de Porta
- 13.15. Balanceamento de carga de IP
- 13.16. DNS e DHCP
- 13.17. VPN
  - 13.17.1. Configurando VPN
  - 13.17.2. Usando VPN com Windows
  - 13.17.3. Using VPN with Mac OS X
  - 13.17.4. Configurando uma conexão VPN Site-to-Site
- 13.18. About Inter-VLAN Routing
- 13.19. Configuring a Virtual Private Cloud
  - 13.19.1. About Virtual Private Clouds
  - 13.19.2. Adding a Virtual Private Cloud
  - 13.19.3. Adding Tiers
  - 13.19.4. Configuring Access Control List
  - 13.19.5. Adicionando um gateway privado a uma VPC
  - 13.19.6. Implantando máquinas virtuais na camada
  - 13.19.7. Obtendo um novo endereço IP para uma VPC
  - 13.19.8. Liberando um endereço IP atribuído a uma VPC
  - 13.19.9. Habilitando ou desabilitando NAT estática em uma VPC
  - 13.19.10. Adicionando regras de balanceamento de carga em uma VPC
  - 13.19.11. Adicionando uma regra de encaminhamento de porta em uma VPC
  - 13.19.12. Removing Tiers
  - 13.19.13. Editing, Restarting, and Removing a Virtual Private Cloud
- 13.20. Persistent Networks
  - 13.20.1. Persistent Network Considerations
  - 13.20.2. Creating a Persistent Guest Network

## A Revision History

# Capítulo 1. Conceitos

- 1.1. O que é o CloudStack?
- 1.2. O que o CloudStack pode fazer?
- 1.3. Visão geral da arquitetura de implementação
  - 1.3.1. Visão geral da arquitetura de implementação
  - 1.3.2. Visão geral da infraestrutura de nuvem
  - 1.3.3. Visão geral de serviços de rede

## 1.1. O que é o CloudStack?

O CloudStack é uma plataforma de software de código aberto que gerencia recursos computacionais para construir nuvens "Infrastructure as a Service" (IaaS). O CloudStack gerencia a rede, storage, e nós computacionais que compõem a infraestrutura de nuvem. Use o CloudStack para implementar, gerenciar e configurar ambientes de computação em nuvem.

Provedores de serviços e empresas são os usuários típicos. Com o CloudStack, você pode:

- » Estabelecer um serviço sob demanda elástico de computação em nuvem. Provedores de serviços podem vender instâncias self service de máquinas virtuais, volumes de armazenamento e configurações de rede pela Internet.
- » Estabelecer na empresa uma nuvem privada para uso dos funcionários. Ao invés de gerenciar máquinas virtuais do mesmo modo que máquinas físicas, com o CloudStack uma empresa pode oferecer máquinas virtuais self-service para usuários sem envolver os departamentos de TI.





## 1.2. O que o CloudStack pode fazer?

### Suporte a múltiplos hipervisores

O CloudStack trabalha com uma variedade de hipervisores. Uma única implementação de nuvem pode conter múltiplas implementações de hipervisores. O release atual do CloudStack suporta soluções empresariais pre-packaged como o Citrix XenServer e o VMware vSphere, assim como KVM ou Xen executando no Ubuntu ou CentOS.

### Gestão de infraestrutura altamente escalável

O CloudStack pode gerenciar dezenas de milhares de servidores instalados em múltiplos centros de computação geograficamente distribuídos. O servidor de gerenciamento centralizado é linearmente escalável, eliminando a necessidade de servidores de gerenciamento de cluster intermediários. Nenhuma falha de componente único pode causar uma interrupção geral na nuvem. A manutenção periódica do servidor de gerenciamento pode ser executada sem afetar o funcionamento de máquinas virtuais que são executadas na nuvem.

### Gerenciamento automático de configuração

O CloudStack automaticamente configura os parâmetros de rede e armazenamento de cada máquina virtual hospede.

O CloudStack gerencia internamente um pool de dispositivos virtuais ("virtual appliances") para suporte à nuvem. Estes dispositivos oferecem serviços como firewall, roteamento, DHCP, acesso VPN, console proxy, acesso a storage e replicação de storage. O uso extensivo de dispositivos virtuais simplifica a instalação, configuração e gerenciamento contínuo de uma implementação de nuvem.

### Interface gráfica do usuário

O CloudStack oferece uma interface web para o administrador, usado para provisionamento e gestão da nuvem, assim como uma interface web do usuário final, usada para executar máquinas virtuais e gerenciar modelos (templates) de máquinas virtuais. A interface de usuário pode ser customizada para refletir os padrões de visuais de apresentação do provedor de serviços ou empresa.

### API e extensibilidade

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](#) and [Apache CloudStack API Reference](#) respectively.

A arquitetura de alocação de plataformas conectáveis do CloudStack permite a criação de novos tipos de alocadores para a seleção de storage e hosts. Veja o "Allocator Implementation Guide" ([http://docs.cloudstack.org/CloudStack\\_Documentation/Allocator\\_Implementation\\_Guide](http://docs.cloudstack.org/CloudStack_Documentation/Allocator_Implementation_Guide)).

### Alta disponibilidade

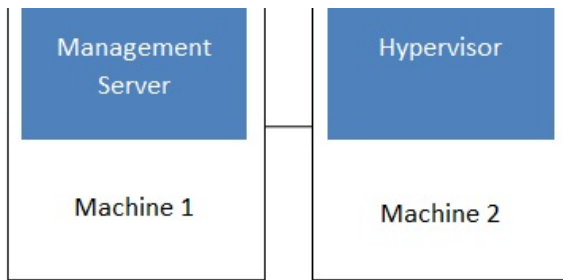
A plataforma do CloudStack tem um número de recursos para aumentar a disponibilidade do sistema. O próprio servidor de gerenciamento pode ser implementado em um ambiente com múltiplos nós onde é feito balanceamento de carga entre os servidores. MySQL pode ser configurado para usar replicação, provendo uma método manual de recuperação em caso de perda do database. Para os hosts, a plataforma CloudStack suporta NIC bonding e o uso de redes isoladas de storage, assim como iSCSI Multipath.

## 1.3. Visão geral da arquitetura de implementação

Uma instalação do CloudStack consiste em dois componentes: o servidor de gerenciamento e a infraestrutura de nuvem que ele gerencia. Quando você monta e gerencia uma nuvem CloudStack, você provê recursos como hosts, equipamentos de storage, e endereços IP no servidor de gerenciamento, e o servidor de gerenciamento gerencia estes recursos.

A instalação mínima de produção consiste em uma máquina executando o servidor de gerenciamento do CloudStack e outra atuando como a infraestrutura de rede (neste caso, uma infraestrutura muito simples consistindo em um host executando software hipervisor). Na menor implementação possível, uma única máquina pode atuar tanto como servidor de gerenciamento quanto o host hipervisor (usando o hipervisor KVM).





### Simplified view of a basic deployment

A more full-featured installation consists of a highly-available multi-node Management Server installation and up to tens of thousands of hosts using any of several advanced networking setups. For information about deployment options, see the "Choosing a Deployment Architecture" section of the \$PRODUCT; Installation Guide.

#### 1.3.1. Visão geral da arquitetura de implementação

O servidor de gerenciamento é o software do CloudStack que gerencia os recursos da nuvem. Pela interação com o servidor de gerenciamento através de sua interface de usuário ou API, você pode configurar e gerenciar sua infraestrutura de nuvem.

O servidor de gerenciamento é executado em um servidor dedicado ou máquina virtual. Ele controla a alocação de máquinas virtuais em hosts e atribui storage e endereços IP às instâncias de máquinas virtuais. O servidor de gerenciamento é executado em um container Tomcat e requer um database MySQL para persistência.

A máquina deve atender os requerimentos descritos em "Requerimentos do sistema".

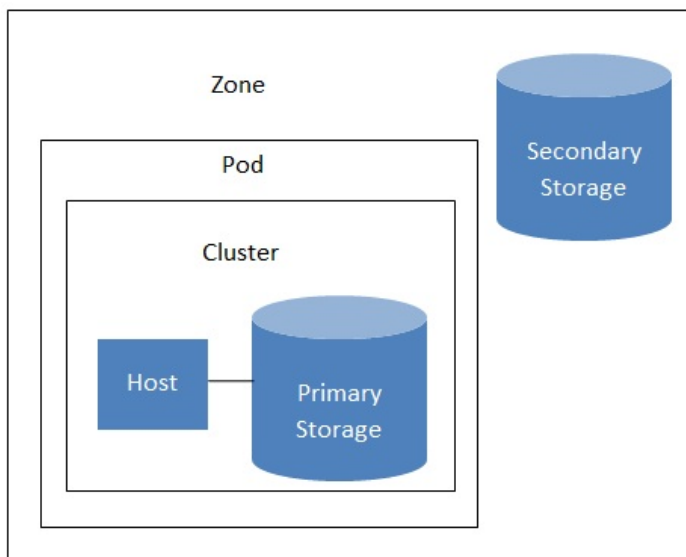
O servidor de gerenciamento:

- » Provê a interface web de usuário para o administrador e uma interface de referência de usuário para usuários finais.
- » Provê as APIs para o CloudStack.
- » Gerencia o assinalamento de máquinas virtuais hóspedes a hosts determinados.
- » Gerencia o assinalamento de endereços IP públicos e privados a determinadas contas.
- » Gerencia a alocação de storage - como discos virtuais - para hóspedes.
- » Gerencia snapshots, templates, e imagens ISO, possivelmente replicando estes elementos através de data centers.
- » Provê um ponto único de configuração para a nuvem.

#### 1.3.2. Visão geral da infraestrutura de nuvem

O servidor de gerenciamento gerencia uma ou mais zonas (tipicamente, datacenters) contendo hosts onde máquinas virtuais hóspedes serão executadas. A infraestrutura de nuvem é organizada como se segue:

- » Zona: tipicamente, uma zona é equivalente a um único datacenter. Uma zona consiste em um ou mais pods e storage secundária.
- » Pod: um pod é usualmente um rack de hardware que inclui uma switch layer-2 e um ou mais clusters.
- » Cluster: um cluster consiste em um ou mais hosts e storage primária.
- » Host: um nó computacional em um cluster. É nos hosts onde realmente os serviços de nuvem são executados, na forma de máquinas virtuais hóspedes.
- » Storage primária é associada com um cluster, e armazena os volumes de disco para todas as máquinas virtuais sendo executadas em hosts neste cluster.
- » Storage secundária é associada com uma zona, e armazena templates, imagens ISO e snapshots de volumes de disco.



---

## Nested organization of a zone

### Informações adicionais

Para informações adicionais, veja a documentação sobre conceitos de infraestrutura de nuvem.

### 1.3.3. Visão geral de serviços de rede

O CloudStack oferece dois tipos de ambiente de rede:

- Básico. Para redes no estilo AWS. Provê uma rede única onde isolamento de hóspedes pode ser provido através de recursos da camada 3 como grupos seguros (filtragem de endereço IP de origem).
- Avançada. Para topologias de rede mais sofisticadas. Este modelo de rede provê a mais alta flexibilidade na definição de redes hóspedes.

Para mais detalhes, veja Configuração de rede.

# Capítulo 2. Conceitos de infraestrutura de nuvem

## 2.1. About Regions

### 2.2. Sobre zonas

### 2.3. Sobre pods

### 2.4. Sobre clusters

### 2.5. Sobre hosts

### 2.6. Sobre storage primária

### 2.7. Sobre storage secundária

### 2.8. Sobre redes físicas

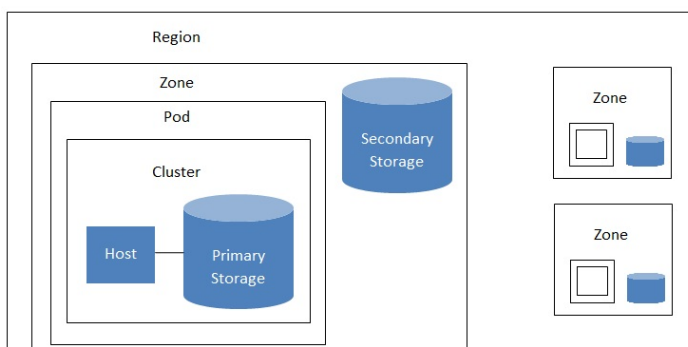
- 2.8.1. Tipos de tráfego de rede da zona básica
- 2.8.2. Endereços IP de hóspedes na zona básica
- 2.8.3. Tipos de tráfego de rede da zona avançada
- 2.8.4. Endereços IP de hóspedes na zona avançada
- 2.8.5. Endereços IP públicos na zona avançada
- 2.8.6. Endereços IP reservados pelo sistema

## 2.1. About Regions

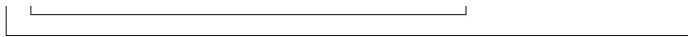
To increase reliability of the cloud, you can optionally group resources into multiple geographic regions. A region is the largest available organizational unit within a CloudStack deployment. A region is made up of several availability zones, where each zone is roughly equivalent to a datacenter. Each 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

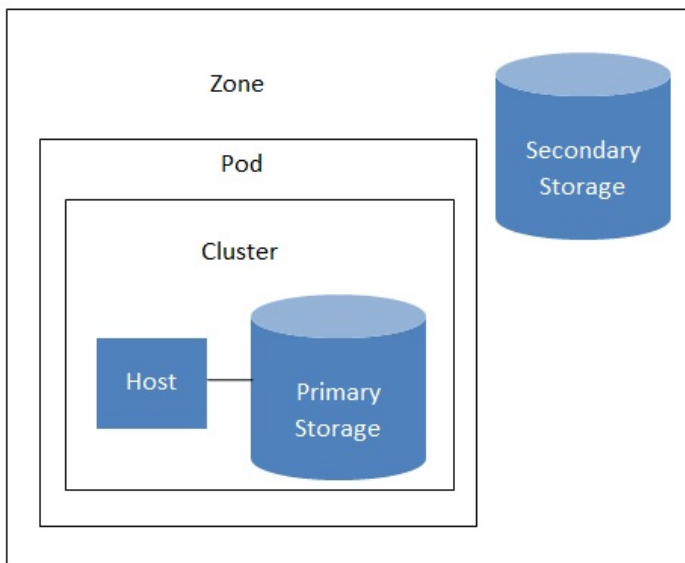
Regions are visible to the end user. When a user starts a guest VM, the user must select a region for their guest. Users might also be required to copy their private templates to additional regions to enable creation of guest VMs using their templates in those regions.

## 2.2. Sobre zonas

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).

Uma zona consiste em:

- » Um ou mais pods. Cada pod contém um ou mais clusters de hosts e um ou mais servidores de storage primária.
- » Storage secundária, compartilhada por todos os pods na zona.



#### Nested organization of a zone

Zonas são visíveis para o usuário final. Quando um usuário ativa uma máquina virtual hóspede, o usuário deve selecionar uma zona para seu hóspede. Usuários podem também ter que copiar seus templates privados para outras zonas para possibilitar a criação de máquinas virtuais hóspedes usando seus templates naquelas zonas.

Zonas podem ser públicas ou privadas. Zonas públicas são visíveis por todos usuários. Isto significa que qualquer usuário pode criar um hóspede na zona. Zonas privadas são reservadas para um domínio específico. Somente usuários no domínio ou seus subdomínios podem criar hóspedes na zona.

Hosts na mesma zona são diretamente acessíveis entre si, sem precisar passar por um firewall. Hosts em zonas distintas podem acessar um ao outro através de túneis VPN configurados estaticamente.

Para cada zona, o administrador deve decidir o seguinte:

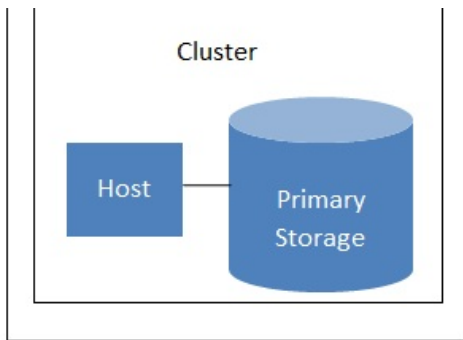
- » Quantos pods colocar na zona.
- » Quantos clusters colocar em cada pod.
- » Quantos hosts colocar em em cada cluster.
- » Quantos servidores de storage primária colocar em cada cluster e a capacidade total dos servidores de storage.
- » Quanto de storage secundária implantar em uma zona.

Quando você adiciona uma zona, você será solicitado a configurar a rede física da zona e adicionar o primeiro pod, primeiro cluster, primeiro host, storage primária inicial, e storage secundária inicial.

## 2.3. Sobre pods

A pod often represents a single rack. Hosts in the same pod are in the same subnet. A pod is the second-largest organizational unit within a CloudStack deployment. Pods are contained within zones. Each zone can contain one or more pods. A pod consists of one or more clusters of hosts and one or more primary storage servers. Pods are not visible to the end user.





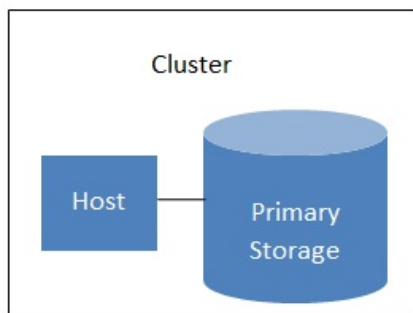
A simple pod

## 2.4. Sobre clusters

Um cluster provê um modo de agrupar hosts. Mais precisamente, um cluster é um pool de servidores XenServer, um conjunto de servidores KVM, um conjunto de servidores OVM, ou um cluster VMware pré-configurado no vCenter. Todos os hosts em um cluster têm hardwares idênticos, executam o mesmo hipervisor, estão na mesma subnet e acessam a mesma storage primária compartilhada. Instâncias de máquinas virtuais (VMs) ativas em um host podem ser migradas para outro host no mesmo cluster, sem interromper os serviços fornecidos ao usuário.

Um cluster é a terceira maior unidade organizacional em uma implementação do CloudStack. Clusters são contidos em pods, e pods são contidos em zonas. O tamanho do cluster é limitado pelo hipervisor subjacente, embora o CloudStack recomenda menos na maioria dos casos; veja "Melhores práticas".

Um cluster consiste em um ou mais hosts e um ou mais servidores de storage primária.



A simple cluster

O CloudStack permite múltiplos clusters em uma implementação de nuvem.

Mesmo quando exclusivamente armazenamento local é usado, clusters ainda são organizacionalmente requeridos, mesmo que haja somente um host por cluster.

Quando VMware é usado, todo cluster VMware é gerenciado por um servidor vCenter. O administrador deve registrar o servidor vCenter no CloudStack. Pode haver múltiplos servidores vCenter por zona. Cada servidor vCenter pode gerenciar múltiplos clusters VMware.

## 2.5. Sobre hosts

Um host é um único computador. Hosts fornecem os recursos computacionais que executam as máquinas virtuais hóspedes. Cada host tem software hipervisor instalado para gerenciar as máquinas virtuais hóspedes. Por exemplo, um servidor Linux com KVM habilitado, um servidor Citrix XenServer, e um servidor ESXi são hosts.

Um host é a menor unidade organizacional em uma implementação do CloudStack. Hosts estão contidos em clusters, clusters são contidos em pods, e pods são contidos em zonas.

Hosts em uma implementação do CloudStack:

- » Proveem os recursos de CPU, memória, storage e de rede necessários para hospedar as máquinas virtuais
- » Interconectam-se utilizando uma rede TCP/IP de alta capacidade e conectam-se à Internet
- » Podem residir em múltiplos centros de dados em localidades geograficamente diferentes
- » Podem ter diferentes capacidades (diferentes velocidades de CPU, diferentes quantidades de RAM, etc.), embora os hosts em um cluster devam ser homogêneos

Hosts adicionais podem ser adicionados a qualquer momento para prover mais capacidade para máquinas virtuais hóspedes.

O CloudStack automaticamente detecta as quantidades de recursos de CPU e memória fornecidas pelos hosts.

Hosts não são visíveis para o usuário final. Um usuário final não pode determinar a qual host sua máquina hóspede foi assinalada.

Para que um host funcione no CloudStack, você deve fazer o seguinte:

- ▶ Instalar software hipervisor no host
- ▶ Assinalar um endereço IP ao host
- ▶ Certificar-se de que o host está conectado ao servidor de gerenciamento do CloudStack

## 2.6. Sobre storage primária

Storage primária é associada com um cluster, e armazena os volumes de disco para todas as máquinas virtuais sendo executadas em hosts neste cluster. Você pode adicionar múltiplos servidores de storage primária a um cluster. No mínimo um é requerido. Normalmente é localizado perto dos hosts para um melhor desempenho.

O CloudStack é projetado para trabalhar com todos os servidores compatíveis com os padrões iSCSI e NFS que são suportados pelo hipervisor subjacente, incluindo, por exemplo:

- ▶ Dell EqualLogic™ for iSCSI
- ▶ Servidores de arquivo Network Appliances for NFS and iSCSI
- ▶ Scale Computing for NFS

Se você pretende utilizar somente o disco local na sua instalação, você pode passar para Adição de storage secundária.

## 2.7. Sobre storage secundária

Storage secundária é associada com um zona, e armazena o seguinte:

- ▶ Templates — imagens de sistemas operacionais que podem ser utilizadas no boot de máquinas virtuais e podem incluir configurações adicionais, tais como aplicativos pré-instalados
- ▶ Imagens ISO — imagens de disco contendo dados ou mídia bootável de sistema operacional
- ▶ Snapshots de volumes de disco — cópias de dados de máquinas virtuais que podem ser usadas para recuperação de dados ou na criação de novos templates

Os itens em storage secundária NFS da zona estão disponíveis para todos os hosts na zona. O CloudStack gerencia a alocação de discos virtuais hóspedes em equipamentos de storage primária.

Para tornar itens na storage secundária disponíveis para todos os hosts na nuvem, você pode adicionar OpenStack Object Storage (Swift, [swift.openstack.org](http://swift.openstack.org)) em adição à storage secundária NFS da zona. Ao utilizar Swift, você configura storage Swift para todo o CloudStack, em seguida configura storage NFS secundária para cada zona, como usual. A storage NFS em cada zona atua como uma área intermediária através da qual todos os templates e outros dados da storage secundária passam antes de serem encaminhados para a Swift. A storage Swift atua como um recurso da nuvem, tornando disponíveis para qualquer zona na nuvem templates e outros dados. Não há hierarquia na storage Swift, apenas um container Swift por objeto de storage. Qualquer storage secundária na nuvem pode obter um container da Swift quando necessário. Não é necessário copiar templates e snapshots de uma zona para outra, como seria requerido ao utilizar somente storage NFS na zona. Tudo está disponível em todo lugar.

## 2.8. Sobre redes físicas

Em parte, a adição de uma zona é configurar a rede física. Uma ou (em uma zona avançada) mais redes físicas podem ser associada com cada zona. A rede corresponde a uma NIC no host hipervisor. Cada rede física pode transportar um ou mais tipos de tráfego de rede. As escolhas de tipo de tráfego para cada rede variam dependendo se você está criando uma zona com rede básica ou rede avançada.

Uma rede física é o hardware de rede e o cabeamento em uma zona. Uma zona pode ter múltiplas redes físicas. Um administrador pode:

- ▶ Adicionar/Remover/Atualizar redes físicas em uma zona
- ▶ Configurar VLANs na rede física
- ▶ Configurar um nome para que a rede seja reconhecida pelos hipervisores
- ▶ Configurar os provedores de serviços (firewalls, balanceadores de carga, etc.) disponíveis em uma rede física
- ▶ Configurar os endereços IP implementados, ou trunked, para uma rede física
- ▶ Especificar o tipo de tráfego que é transportado na rede física, assim como outras propriedades como a velocidade da rede

### 2.8.1. Tipos de tráfego de rede da zona básica

Quando rede básica é utilizada, somente pode haver um tipo de rede física na zona. Tal rede física transporta os seguintes tipos de tráfego:

- ▶ Hóspede. Quando usuários finais executam máquinas virtuais, eles geram tráfego hóspede. As máquinas virtuais hóspedes podem se comunicar através de uma rede que pode ser referida como a rede hóspede. Cada pod em uma zona básica é um domínio de broadcast, e portanto cada pod tem um diferente intervalo IP para a rede hóspede. O administrador pode configurar o intervalo IP para cada 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.



#### Nota

Recomendamos fortemente o uso de placas de rede separadas para o tráfego de gerência e tráfego de hóspedes.

- ▶ **Público.** Tráfego público é gerado quando máquinas virtuais na nuvem acessam a Internet. Endereços IP publicamente acessíveis devem ser alocados para esta finalidade. Usuários finais podem usar a interface de usuário do CloudStack para obter estes endereços IP para implementar NAT entre sua rede hospede e a rede pública, como descrito em Obtendo um novo endereço IP.
- ▶ **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.

Em uma rede básica, a configuração da rede física é bastante simples. Na maioria dos casos, você precisa somente configurar uma rede hospede para transportar tráfego que é gerado pelas máquinas virtuais hóspedes. Se você usa um balanceador de carga NetScaler e habilita suas características de balanceamento elástico de IP e de carga (EIP e ELB), você pode também configurar uma rede para transportar tráfego público. O CloudStack apresenta na interface de usuário os passos de configuração de rede necessários quando você adiciona uma nova zona.

### 2.8.2. Endereços IP de hóspedes na zona básica

Quando rede básica é usada, o CloudStack irá assinalar endereços IP no CIDR do pod para hóspedes naquele pod. O administrador deve adicionar um intervalo IP direto no pod para este propósito. Estes IPs estão na mesma VLAN que os hosts.

### 2.8.3. Tipos de tráfego de rede da zona avançada

Quando rede avançada é usada, pode haver múltiplas redes físicas na zona. Cada rede física pode transportar um ou mais tipos de tráfego, e você precisa informar ao CloudStack qual o tipo de tráfego que você deseja que cada rede transporte. Os tipos de tráfego em uma zona avançada são:

- ▶ **Hóspede.** Quando usuários finais executam máquinas virtuais, eles geram tráfego hospede. As máquinas virtuais hóspedes comunicam-se através de uma rede que pode ser referida como a rede hospede. Esta rede pode ser isolada ou compartilhada. Em uma rede hospede isolada, o administrador precisa reservar intervalos de VLAN para prover isolamento para cada rede de conta do CloudStack (potencialmente um grande número de VLANs). Em uma rede hospede compartilhada, todas as máquinas virtuais hóspedes compartilham uma única rede.
- ▶ **Gerência.** Quando recursos internos do CloudStack comunicam-se entre si, eles geram tráfego de gerência. Isto inclui a comunicação entre hosts, máquinas virtuais do sistema (máquinas virtuais usadas pelo CloudStack para executar várias tarefas na nuvem), e qualquer outro componente que se comunica diretamente com o servidor de gerenciamento do CloudStack. Você deve configurar o intervalo de IP para uso das máquinas virtuais do sistema.
- ▶ **Público.** Tráfego público é gerado quando máquinas virtuais na nuvem acessam a Internet. Endereços IP publicamente acessíveis devem ser alocados para esta finalidade. Usuários finais podem usar a interface de usuário do CloudStack para obter estes endereços IP para implementar NAT entre sua rede hospede e a rede pública, como descrito em Obtendo um novo endereço IP no Guia de Administração.
- ▶ **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.

Cada um destes tipos de tráfego pode estar em uma rede física separada, ou eles podem ser combinados com certas restrições. Quando você usa o assistente Add Zone na interface de usuário para criar uma nova zona, você é orientado a fazer somente escolhas válidas.

### 2.8.4. Endereços IP de hóspedes na zona avançada

Quando rede avançada é usada, o administrador pode criar redes adicionais para uso dos hóspedes. Estas redes podem abranger a zona e ficar disponíveis para todas as contas, ou elas podem ser restritas para uma única conta, e neste caso somente a conta específica pode criar hóspedes que se ligam a estas redes. As redes são definidas pela identificação da VLAN, intervalo de IP, e gateway. Se quiser, o administrador pode prover milhares destas redes.

### 2.8.5. Endereços IP públicos na zona avançada

Quando rede avançada é usada, o administrador pode criar redes adicionais para uso dos hóspedes. Estas redes podem abranger a zona e ficar disponíveis para todas as contas, ou elas podem ser restritas para uma única conta, e neste caso somente a conta específica pode criar hóspedes que se ligam a estas redes. As redes são definidas pela identificação da VLAN, intervalo de IP, e gateway. Se quiser, o administrador pode prover milhares destas redes.

### 2.8.6. Endereços IP reservados pelo sistema

Em cada zona, você precisa configurar um intervalo de endereços IP reservados para a rede de gerência. Esta rede transporta a comunicação entre o servidor de gerenciamento do CloudStack e várias máquinas virtuais do sistema, tais como as máquinas virtuais de storage secundária, as máquinas virtuais de proxy de console, e DHCP.

Os endereços IP reservados devem ser únicos na nuvem. Você não pode, por exemplo, ter um host em uma zona com o mesmo endereço IP privado que um host em outra zona.

Aos hosts em um pod são assinalados endereços IP privados. Estes são tipicamente endereços da RFC1918. As máquinas virtuais de proxy de console e storage secundária também têm endereços IP privados alocados no CIDR do pod onde são criadas.

Certifique-se de que servidores de computação e servidores de gerenciamento utilizem endereços IP fora do intervalo de IP reservado pelo sistema. Por exemplo, suponha que o intervalo de IP reservado pelo sistema se inicia em 192.168.154.2 e termina em 192.168.154.7. O CloudStack pode usar .2 a .7 para máquinas virtuais do sistema. Isto deixa o restante do CIDR do pod, de .8 a .254, para o servidor de gerenciamento e para os hosts hipervisores.

**Em todas as zonas:**

Forneça IPs privados para o sistema em cada pod e disponibilize-os no CloudStack.

Para o KVM e o XenServer, o número recomendado de IPs privados por pod é um por host. Se você espera que o pod cresça, adicione agora IPs privados suficientes para permitir o crescimento.

#### Em uma zona que usa rede avançada:

Para zonas com rede avançada, recomendamos o fornecimento de IPs privados suficientes para o número total de usuários mais o requerido pelas máquinas virtuais de sistema. Tipicamente, cerca de 10 IPs adicionais são requeridos para as máquinas virtuais de sistema. Para informações adicionais sobre máquinas virtuais de sistema, veja [Trabalhando com máquinas virtuais de sistema no Guia do administrador](#).

Quando rede avançada está sendo usada, o número de endereços IP privados disponíveis em cada pod varia dependendo de qual hipervisor está sendo executado nos nós daquele pod. O Citrix XenServer e o KVM usam endereços de enlace local — 169.254.0.0/16 ou fe80::/64 —, o que em teoria provê mais de 65.000 endereços IP privados no bloco de endereçamento. Conforme o pod cresce, isto deveria ser mais que suficiente para qualquer número razoável de hosts, assim como endereços IP para roteadores virtuais hóspedes. O VMWare ESXi, em contraste, usa qualquer esquema de subnet especificada pelo administrador, e o administrador típico provê apenas 255 IPs por pod. Como estes são compartilhados por máquinas físicas, o roteador virtual hóspede, e outras entidades, é possível esgotar os IPs privados ao incrementar a configuração de um pod cujos nós executam ESXi.

Para garantir uma margem adequada para redimensionar o espaço de IPs privados em um pod ESXi que usa rede avançada, use uma ou ambas técnicas a seguir:

- Especifique um bloco CIDR maior para a subnet. Uma máscara de subnet com um sufixo /20 proverá mais de 4.000 endereços IP.
- Crie múltiplos pods, cada um com sua própria subnet. Por exemplo, se você criar 10 pods e cada pod tem 255 IPs, isto irá prover 2.550 endereços IP.

## Capítulo 3. Building from Source

### 3.1. Getting the release

### 3.2. Verifying the downloaded release

#### 3.2.1. Getting the KEYS

#### 3.2.2. GPG

#### 3.2.3. MD5

#### 3.2.4. SHA512

### 3.3. Prerequisites for building Apache CloudStack

### 3.4. Extracting source

### 3.5. Building DEB packages

#### 3.5.1. Setting up an APT repo

#### 3.5.2. Configuring your machines to use the APT repository

### 3.6. Building RPMs from Source

#### 3.6.1. Generating RPMs

### 3.7. Building Non-OSS

The official CloudStack release is always in source code form. You will likely be able to find "convenience binaries," the source is the canonical release. In this section, we'll cover acquiring the source release and building that so that you can deploy it using Maven or create Debian packages or RPMs.

Note that building and deploying directly from source is typically not the most efficient way to deploy an IaaS. However, we will cover that method as well as building RPMs or Debian packages for deploying CloudStack.

The instructions here are likely version-specific. That is, the method for building from source for the 4.0.x series is different from the 4.1.x series.

If you are working with an unreleased version of CloudStack, see the `INSTALL.md` file in the top-level directory of the release.

## 3.1. Getting the release

You can download the latest CloudStack release from the [Apache CloudStack project download page](#).

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

You'll notice several links under the 'Latest release' section. A link to a file ending in `tar.bz2`, as well as a PGP/GPG signature, MD5, and SHA512 file.

- The `tar.bz2` file contains the Bzip2-compressed tarball with the source code.
- The `.asc` file is a detached cryptographic signature that can be used to help verify the authenticity of the release.
- The `.md5` file is an MD5 hash of the release to aid in verifying the validity of the release download

- ▶ The `.md5` file is an MD5 hash of the release to aid in verify the validity of the release download.
- ▶ The `.sha` file is a SHA512 hash of the release to aid in verify the validity of the release download.

## 3.2. Verifying the downloaded release

There are a number of mechanisms to check the authenticity and validity of a downloaded release.

### 3.2.1. Getting the KEYS

To enable you to verify the GPG signature, you will need to download the [KEYS](#) file.

You next need to import those keys, which you can do by running:

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

### 3.2.2. GPG

The CloudStack project provides a detached GPG signature of the release. To check the signature, run the following command:

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

If the signature is valid you will see a line of output that contains 'Good signature'.

### 3.2.3. MD5

In addition to the cryptographic signature, CloudStack has an MD5 checksum that you can use to verify the download matches the release. You can verify this hash by executing the following command:

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

If this successfully completes you should see no output. If there is any output from them, then there is a difference between the hash you generated locally and the hash that has been pulled from the server.

### 3.2.4. SHA512

In addition to the MD5 hash, the CloudStack project provides a SHA512 cryptographic hash to aid in assurance of the validity of the downloaded release. You can verify this hash by executing the following command:

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

If this command successfully completes you should see no output. If there is any output from them, then there is a difference between the hash you generated locally and the hash that has been pulled from the server.

## 3.3. Prerequisites for building Apache CloudStack

There are a number of prerequisites needed to build CloudStack. This document assumes compilation on a Linux system that uses RPMs or DEBs for package management.

You will need, at a minimum, the following to compile CloudStack:

1. Maven (version 3)
2. Java (OpenJDK 1.6 or Java 7/OpenJDK 1.7)
3. Apache Web Services Common Utilities (ws-commons-util)
4. MySQL
5. MySQLdb (provides Python database API)
6. Tomcat 6 (not 6.0.35)
7. genisoimage
8. rpmbuild or dpkg-dev

## 3.4. Extracting source

Extracting the CloudStack release is relatively simple and can be done with a single command as follows:

```
$ tar -jxvf apache-cloudstack-4.1.1-src.tar.bz2
```

You can now move into the directory:

```
$ cd ./apache-cloudstack-4.1.1-src
```

## 3.5. Building DEB packages

In addition to the bootstrap dependencies, you'll also need to install several other dependencies. Note that we recommend using Maven 3, which is not currently available in 12.04.1 LTS. So, you'll also need to add a PPA repository that includes Maven 3. After running the command **add-apt-repository**, you will be prompted to continue and a GPG key will be added.

```
$ 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 liblog4j1.2-
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-buildpackage -uc -us
```

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

- ▶ cloudstack-agent\_4.1.1\_all.deb
- ▶ cloudstack-awsapi\_4.1.1\_all.deb
- ▶ cloudstack-cli\_4.1.1\_all.deb
- ▶ cloudstack-common\_4.1.1\_all.deb
- ▶ cloudstack-docs\_4.1.1\_all.deb
- ▶ cloudstack-management\_4.1.1\_all.deb
- ▶ cloudstack-usage\_4.1.1\_all.deb

### 3.5.1. Setting up an APT repo

After you've created the packages, you'll want to copy them to a system where you can serve the packages over HTTP. You'll create a directory for the packages and then use **dpkg-scanpackages** to create **Packages.gz**, which holds information about the archive structure. Finally, you'll add the repository to your system(s) so you can install the packages using APT.

The first step is to make sure that you have the **dpkg-dev** package installed. This should have been installed when you pulled in the **debhelper** application previously, but if you're generating **Packages.gz** on a different system, be sure that it's installed there as well.

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

The next step is to copy the DEBs to the directory where they can be served over HTTP. We'll use **/var/www/cloudstack/repo** in the examples, but change the directory to whatever works for you.

```
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

You can safely ignore the warning about a missing override file.

Now you should have all of the DEB packages and **Packages.gz** in the **binary** directory and available over HTTP. (You may want to use **wget** or **curl** to test this before moving on to the next step.)

### 3.5.2. Configuring your machines to use the APT repository

Now that we have created the repository, you need to configure your machine to make use of the APT repository. You can do this by adding a repository file under **/etc/apt/sources.list.d**. Use your preferred editor to create **/etc/apt/sources.list.d/cloudstack.list** with this line:

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

Now that you have the repository info in place, you'll want to run another update so that APT knows where to find the CloudStack packages.

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

You can now move on to the instructions under [Install on Ubuntu](#).

## 3.6. Building RPMs from Source

As mentioned previously in [Seção 3.3, "Prerequisites for building Apache CloudStack"](#), you will need to install several prerequisites before you can build packages for CloudStack. Here we'll assume you're working with a 64-bit build of CentOS or 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
```

Next, you'll need to install build-time dependencies for CloudStack with Maven. We're using Maven 3, so you'll want to [grab a Maven 3 tarball](#) and uncompress it in your home directory (or whatever location you prefer):

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

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

Maven also needs to know where Java is, and expects the `JAVA_HOME` environment variable to be set:

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

Verify that Maven is installed correctly:

```
$ mvn --version
```

You probably want to ensure that your environment variables will survive a logout/reboot. Be sure to update `~/.bashrc` with the `PATH` and `JAVA_HOME` variables.

Building RPMs for `$PRODUCT`; is fairly simple. Assuming you already have the source downloaded and have uncompressed the tarball into a local directory, you're going to be able to generate packages in just a few minutes.



### Packaging has Changed

If you've created packages for `$PRODUCT`; previously, you should be aware that the process has changed considerably since the project has moved to using Apache Maven. Please be sure to follow the steps in this section closely.

## 3.6.1. Generating RPMs

Now that we have the prerequisites and source, you will `cd` to the `packaging/centos63/` directory.

```
$ cd packaging/centos63
```

Generating RPMs is done using the `package.sh` script:

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

That will run for a bit and then place the finished packages in `dist/rpmbuild/RPMS/x86_64/`.

You should see six RPMs in that directory:

- » `cloudstack-agent-4.1.1.e16.x86_64.rpm`
- » `cloudstack-awsapi-4.1.1.e16.x86_64.rpm`
- » `cloudstack-cli-4.1.1.e16.x86_64.rpm`
- » `cloudstack-common-4.1.1.e16.x86_64.rpm`
- » `cloudstack-management-4.1.1.e16.x86_64.rpm`
- » `cloudstack-usage-4.1.1.e16.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 "e16" in the filename. (Fedora 18 isn't a supported platform at this time, just providing an example.)

### 3.6.1.1. Creating a yum repo

While RPMs is a useful packaging format - it's most easily consumed from Yum repositories over a network. The next step is to create a Yum Repo with the finished packages:

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

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

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

The files and directories within `~/tmp/repo` can now be uploaded to a web server and serve as a yum repository.

### 3.6.1.2. Configuring your systems to use your new yum repository

Now that your yum repository is populated with RPMs and metadata we need to configure the machines that need to install `$PRODUCT`; Create a file named `/etc/yum.repos.d/cloudstack.repo` with this information:

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

Completing this step will allow you to easily install `$PRODUCT`; on a number of machines across the network.

## 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](#).

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](#) page on the wiki.
2. You may also need to download [vhd-util](#), 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
$ mvn install -Dnonoss
```

4. Once you've built CloudStack with the **nonoss** profile, you can package it using the [Seção 3.6, "Building RPMs from Source"](#) or [Seção 3.5, "Building DEB packages"](#) instructions.

# Capítulo 4. Instalação

## 4.1. Quem deve ler este documento

## 4.2. Visão geral dos passos de instalação

## 4.3. Requerimentos mínimos de sistema

- 4.3.1. Requerimentos de sistema dos servidores de gerenciamento, database, e storage
- 4.3.2. Requerimentos de sistema do host/hipervisor

## 4.4. Configure package repository

- 4.4.1. DEB package repository
- 4.4.2. RPM package repository

## 4.5. Instalação do servidor de gerenciamento

- 4.5.1. Visão geral da instalação do servidor de gerenciamento
- 4.5.2. Preparando o sistema operacional
- 4.5.3. Instale o servidor de gerenciamento no primeiro host.
- 4.5.4. Instalar o servidor de banco de dados.
- 4.5.5. Sobre senha e chave de criptografia
- 4.5.6. Preparar os compartilhamentos NFS
- 4.5.7. Preparar e ativar servidores de gerenciamento adicionais
- 4.5.8. Prepare o template de máquina virtual de sistema
- 4.5.9. Instalação completa! Próximos passos

## 4.1. Quem deve ler este documento

Para aqueles que já passaram pela fase de design e planejam uma implementação mais sofisticada, ou aqueles que estão prontos para começar a incrementar uma instalação de avaliação. Com os procedimentos a seguir, você pode começar a utilizar recursos mais poderosos do CloudStack, tais como configuração avançada de VLAN, alta disponibilidade, elementos adicionais de rede como balanceadores de carga e firewalls, e suporte a múltiplos hipervisores, incluindo o Citrix XenServer, KVM, e o VMware vSphere.

## 4.2. Visão geral dos passos de instalação

Para qualquer coisa mais que uma simples instalação de avaliação, você precisará de orientação para uma variedade de opções de configuração. É altamente recomendado que você leia o seguinte:

- » Selecionando a arquitetura de implementação
- » Selecionando o hipervisor: recursos suportados
- » Configuração de rede
- » Configuração de storage
- » Melhores práticas

1. Certifique-se de que está pronto o hardware requerido. Veja [Seção 4.3, "Requerimentos mínimos de sistema"](#)
2. Instale o servidor de gerenciamento (selecione single-node ou multi-node). Veja [Seção 4.5, "Instalação do servidor de gerenciamento"](#)
3. Faça login na interface de usuário. Veja [Capítulo 5, Interface do usuário](#)
4. Adicione uma zona. Inclua o primeiro pod, cluster, e host. Veja [Seção 6.3, "Adicionando uma zona"](#)
5. Adicione mais pods (opcional). Veja [Seção 6.4, "Adicionando um pod"](#)

6. Adicione mais clusters (opcional). Veja [Seção 6.5, "Adicionando um cluster"](#)
7. Adicione mais hosts (opcional). Veja [Seção 6.6, "Adding a Host"](#)
8. Adicione mais storage primária (opcional). Veja [Seção 6.7, "Adicionar Storage Primário"](#)
9. Adicione mais storage secundária (opcional). Veja [Seção 6.8, "Adicionar Storage Secundário"](#)
10. Experimente o uso da rede. Veja [Seção 6.9, "Initialize and Test"](#)

## 4.3. Requerimentos mínimos de sistema

### 4.3.1. Requerimentos de sistema dos servidores de gerenciamento, database, e storage

As máquinas onde serão executados o servidor de gerenciamento e o database MySQL devem atender os seguintes requerimentos. As mesmas máquinas podem também ser utilizadas para prover armazenamento primário e secundário, tal como disco local ou via NFS. O servidor de gerenciamento pode ser alocado em uma máquina virtual.

- » Sistema operacional:
  - Preferencial: CentOS/RHEL 6.3+ ou Ubuntu 12.04(.1)
- » CPU x86 64-bit (mais cores resultam em melhor performance)
- » 4 GB de memória
- » 250 GB de disco local (mais resulta em melhor capacidade; 500 GB são recomendados)
- » No mínimo 1 NIC
- » Endereço IP estaticamente assinalado
- » Nome de domínio totalmente qualificado é retornado pelo comando hostname

### 4.3.2. Requerimentos de sistema do host/hipervisor

O host é onde os serviços de nuvem são executados na forma de máquinas virtuais hóspedes. Cada host é uma máquina que atende os seguintes requerimentos:

- » Deve suportar HVM (Intel-VT ou AMD-V habilitados).
- » CPU x86 64-bit (mais cores resultam em melhor performance)
- » Suporte de virtualização de hardware requerido
- » 4 GB de memória
- » 36 GB de disco local
- » No mínimo 1 NIC



#### Nota

Se DHCP é usado para hosts, certifique-se de que nenhum conflito ocorre entre o servidor DHCP usado para estes hosts e o roteador DHCP criado pelo CloudStack.

- » Mais recentes hotfixes aplicadas ao software do hipervisor
- » Quando você implementa o CloudStack, o host hipervisor não pode ter máquinas virtuais já ativas
- » All hosts within a cluster must be homogeneous. The CPUs must be of the same type, count, and feature flags.

Hosts têm requerimentos adicionais dependendo do hipervisor. Veja os requerimentos listados no início da seção Instalação relativa ao hipervisor de sua escolha:



#### Atenção

Certifique-se de atender os requerimentos adicionais do hipervisor e os passos de instalação fornecidos neste guia. Hosts hipervisores devem ser adequadamente preparados para trabalhar com o CloudStack. Por exemplo, os requerimentos para o XenServer são listados em Instalação do Citrix XenServer.

- » [Seção 8.1.1, "Requerimentos de sistema para hosts hipervisores KVM"](#)
- » [Seção 8.2.1, "System Requirements for XenServer Hosts"](#)
- » [Seção 8.3.1, "System Requirements for vSphere Hosts"](#)

## 4.4. Configure package repository

CloudStack é distribuído apenas a partir do código-fonte dos espelhos oficiais. No entanto, membros da comunidade CloudStack podem construir binários de conveniência para que os usuários possam instalar o Apache CloudStack sem precisar construir a partir do código-fonte.

Se você não seguiu os passos para construir seus próprios pacotes a partir do código-fonte nas seções [Seção 3.6, "Building RPMs from Source"](#) ou [Seção 3.5, "Building DEB packages"](#), você pode encontrar pacotes pré-construídos DEB e RPM para sua conveniência linkados a partir da [downloads](#) página.



#### Nota

These repositories contain both the Management Server and KVM Hypervisor packages.

These repositories contain both the Management Server and KVM Hypervisor packages.

#### 4.4.1. DEB package repository

You can add a DEB package repository to your apt sources with the following commands. Please note that only packages for Ubuntu 12.04 LTS (precise) are being built at this time.

Use your preferred editor and open (or create) `/etc/apt/sources.list.d/cloudstack.list`. Add the community provided repository to the file:

```
deb http://cloudstack.apt-get.eu/ubuntu precise 4.1
```

We now have to add the public key to the trusted keys.

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

Now update your local apt cache.

```
$ apt-get update
```

Your DEB package repository should now be configured and ready for use.

#### 4.4.2. RPM package repository

There is a RPM package repository for CloudStack so you can easily install on RHEL based platforms.

If you're using an RPM-based system, you'll want to add the Yum repository so that you can install CloudStack with Yum.

Yum repository information is found under `/etc/yum.repos.d`. You'll see several `.repo` files in this directory, each one denoting a specific repository.

To add the CloudStack repository, create `/etc/yum.repos.d/cloudstack.repo` and insert the following information.

```
[cloudstack]
name=cloudstack
baseurl=http://cloudstack.apt-get.eu/rhel/4.1/
enabled=1
gpgcheck=0
```

Now you should be able to install CloudStack using Yum.

## 4.5. Instalação do servidor de gerenciamento

### 4.5.1. Visão geral da instalação do servidor de gerenciamento

Esta seção descreve a instalação do servidor de gerenciamento. Há dois fluxos de instalação ligeiramente diferentes, dependendo de quantos nós servidores de gerenciamento haverá na sua nuvem:

- » Um único nó servidor de gerenciamento, com MySQL no mesmo nó.
- » Múltiplos nós servidores de gerenciamento, com MySQL em um nó separado dos servidores de gerenciamento.

Em qualquer caso, cada máquina deve atender os requerimentos descritos em Requerimentos do sistema.



### Atenção

Por razões de segurança, certifique-se de que as portas 8096 e 8250 do servidor de gerenciamento não possam ser acessadas pela Internet.

O procedimento para instalação do servidor de gerenciamento é:

1. Preparar o sistema operacional
2. (somente para XenServer) Faça download e instale vhd-util.
3. Instalar o primeiro servidor de gerenciamento
4. Instalar e configurar o database MySQL
5. Preparar os compartilhamentos NFS
6. Preparar e ativar servidores de gerenciamento adicionais (opcional)
7. Preparar o template de máquina virtual de sistema

### 4.5.2. Preparando o sistema operacional

O sistema operacional deve ser preparado para receber o servidor de gerenciamento usando os seguintes passos. Estes passos devem ser realizados em cada nó de servidor de gerenciamento.

1. Faça login no sistema operacional como root.
2. Verifique o hostname completamente qualificado.

```
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. Certifique-se de que a máquina tem acesso à Internet.

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

4. Ative NTP para sincronização de horário.

### Nota

NTP é requerido para sincronizar os relógios dos servidores na nuvem.

- a. Instale o NTP.

```
yum install ntp
```

```
apt-get install openntp
```

5. Repita todos estes passos em cada host que o servidor de gerenciamento será instalado.

## 4.5.3. Instale o servidor de gerenciamento no primeiro host.

O primeiro passo para a instalação, se você está instalando o servidor de gerenciamento em um host ou muitos, é instalar o software em um único nó.

### Nota

Se você estiver planejando instalar o servidor de gerenciamento em vários nós para alta disponibilidade, não avance para os nós adicionais ainda. Esse passo virá mais tarde.

O servidor de gerenciamento CloudStack pode ser instalado usando tanto pacotes RPM ou DEB. Estes pacotes vão depender tudo que você precisa para executar o servidor de gerenciamento.

### 4.5.3.1. Instale o CentOS/RHEL

Começamos instalando os pacotes necessários:

```
yum install cloudstack-management
```

### 4.5.3.2. Instale o Ubuntu

```
apt-get install cloudstack-management
```

### 4.5.3.3. Baixando o vhd-util

Este procedimento somente é necessário em instalações onde XenServer é instalado nos hosts hipervisores.

Antes de configurar o servidor de gerenciamento, baixe vhd-util de [vhd-util](#).

If the Management Server is RHEL or CentOS, copy vhd-util to `/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver`.

If the Management Server is Ubuntu, copy vhd-util to `/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver`.

## 4.5.4. Instalar o servidor de banco de dados.

O servidor de gerenciamento CloudStack usa um servidor de banco de dados MySQL para armazenar seus dados. Quando você está instalando o servidor de gerenciamento em um único nó, você pode instalar o servidor MySQL localmente. Para uma instalação que tem múltiplos nós servidores de gerenciamento, nós assumimos o banco de dados MySQL também é executado em um nó separado.

CloudStack foi testado com MySQL 5.1 e 5.5. Essas versões estão incluídos no RHEL / CentOS e Ubuntu.

### 4.5.4.1. Instale o banco de dados no nó do servidor de gerenciamento

Esta seção descreve como instalar o MySQL na mesma máquina que o servidor de gerenciamento. Esta técnica destina-se a uma implementação simples que tem um nó único do servidor de gerenciamento. Se você tem a implantação de múltiplos nós do servidor de gerenciamento, você vai tipicamente utilizar um nó separado para MySQL. Veja [Seção 4.5.4.2, "Instale o banco de dados em um nó separado"](#).

1. Install MySQL from the package repository of your distribution:

```
yum install mysql-server
```

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

2. Open the MySQL configuration file. The configuration file is `/etc/my.cnf` or `/etc/mysql/my.cnf`, depending on your OS.
3. Insert the following lines in the `[mysqld]` section.

You can put these lines below the `datadir` line. The `max_connections` parameter should be set to 350 multiplied by the number of Management Servers you are deploying. This example assumes one Management Server.

### Nota

On Ubuntu, you can also create a file `/etc/mysql/conf.d/cloudstack.cnf` and add these directives there. Don't forget to add `[mysqld]` on the first line of the file.

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

4. Inicie ou reinicie o MySQL para colocar a nova configuração em vigor.  
No RHEL/CentOS, o MySQL não é ativado automaticamente após a instalação. Ative-o manualmente.

```
# service mysqld restart
```

No Ubuntu, reinicie o MySQL.

```
# service mysqld restart
```

5. (Só no CentOS e RHEL, não é necessário no Ubuntu)



### Atenção

No RHEL e CentOS, o MySQL não define uma senha de root por padrão. É extremamente recomendável que você defina uma senha de root como medida de segurança.

Execute o seguinte comando para tornar segura sua instalação. Você pode responder "Y" a todas as questões.

```
mysql_secure_installation
```

6. CloudStack can be blocked by security mechanisms, such as SELinux. Disable SELinux to ensure + that the Agent has all the required permissions.

Configure SELinux (RHEL and CentOS):

- a. Check whether SELinux is installed on your machine. If not, you can skip this section.

In RHEL or CentOS, SELinux is installed and enabled by default. You can verify this with:

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

- b. Set the SELINUX variable in `/etc/selinux/config` to "permissive". This ensures that the permissive setting will be maintained after a system reboot.

No RHEL ou CentOS:

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

Change the following line

```
SELINUX=enforcing
```

to this:

```
SELINUX=permissive
```

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

```
$ setenforce permissive
```

7. Configure o banco de dados. O seguinte comando cria o usuário "cloud" no banco de dados.

- Em `dbpassword`, especifique a senha a ser atribuída ao usuário "cloud". Você pode escolher não fornecer uma senha, embora não seja recomendado.
- Em `deploy-as`, especifique o nome do usuário e senha do usuário que está implementando o banco de dados. No comando a seguir, é suposto que o usuário root está implementando o banco de dados e criando o usuário "cloud".
- (Opcional) Para `encryption_type`, use `file` ou `web` para indicar a técnica utilizada para passar a senha de criptografia de banco de dados. Padrão: `file`. Veja [Seção 4.5.5, "Sobre senha e chave de criptografia"](#).
- (Opcional) Para `management_server_key`, substitua a chave padrão que é usada para criptografar os parâmetros confidenciais no arquivo de propriedades do CloudStack. Padrão: `password`. É altamente recomendado que você substitua isso por um valor mais seguro. Veja [Seção 4.5.5, "Sobre senha e chave de criptografia"](#).
- (Opcional) Para `database_key`, substitua a chave padrão que é usada para criptografar os parâmetros confidenciais no banco de dados CloudStack. Padrão: `password`. É altamente recomendado que você substitua isso por um valor mais seguro. Veja [Seção 4.5.5, "Sobre senha e chave de criptografia"](#).
- (Optional) For `management_server_ip`, you may explicitly specify cluster management server node IP. If not specified, the local IP address will be used.

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

Quando o script estiver concluído, você deve ver uma mensagem como "Successfully initialized the database."

8. Se você estiver executando o hipervisor KVM na mesma máquina que o servidor de gerenciamento, edite o `/etc/sudoers` e adicione a seguinte linha:

```
Defaults:cloud !requiretty
```

9. Agora que o banco de dados está configurado, você pode terminar a configuração do sistema operacional para o servidor de gerenciamento. Este comando irá configurar iptables, sudoers, e iniciar o servidor de gerenciamento.

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

Você deverá ver a mensagem "CloudStack Management Server setup is done."

#### 4.5.4.2. Instale o banco de dados em um nó separado

Esta seção descreve como instalar o MySQL em uma máquina independente, separado do servidor de gerenciamento. Esta técnica destina-se a uma implantação que inclui vários nós servidor de gerenciamento. Se você tem um único nó implantado no servidor de gerenciamento, você vai utilizar o mesmo nó para o MySQL. Veja [Seção 4.5.4.1, "Instale o banco de dados no nó do servidor de gerenciamento"](#).

#### Nota

O servidor de gerenciamento não requer uma distribuição específica para o nó MySQL. Você pode usar uma distribuição ou sistema operacional de sua escolha. Usar a mesma distribuição que o servidor de gerenciamento é recomendável, mas não obrigatório. Veja [Seção 4.3.1, "Requerimentos de sistema dos servidores de gerenciamento, database, e storage"](#).

1. Instalar o MySQL a partir do repositório de pacotes de sua distribuição:

```
yum install mysql-server
```

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

2. Edite a configuração do MySQL (`/etc/my.cnf` ou o arquivo `/etc/mysql/my.cnf`, dependendo do seu sistema operacional) e insira as seguintes linhas na seção `[mysqld]`. Você pode colocar essas linhas abaixo da linha `datadir`. O parâmetro `max_connections` deveria ser definido para 350, multiplicado pelo número de servidores de gerenciamento que você está implantando. Este exemplo assume dois servidores de gerenciamento.

#### Nota

No Ubuntu, você também pode criar arquivo `/etc/mysql/conf.d/cloudstack.cnf` e adicionar essas directivas lá. Não se esqueça de adicionar `[mysqld]` na primeira linha do arquivo.

```
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. Iniciar ou reiniciar o MySQL para colocar a nova configuração em vigor.  
No RHEL/CentOS, o MySQL não inicia automaticamente depois da instalação. Inicia-lo manualmente.

```
# service mysqld restart
```

No Ubuntu, reinicie o MySQL.

```
# service mysqld restart
```

4. (Só no CentOS e RHEL, não é necessário no Ubuntu)



#### Atenção

No RHEL e CentOS, o MySQL não definir uma senha de root por padrão. É extremamente recomendável que você defina uma senha de root como medida de segurança.

Execute o seguinte comando para garantir a sua instalação. Você pode responder "Y" a todas as perguntas, exceto "Proibir login root remotamente?". O login remoto é necessário para configurar os bancos de dados.

```
mysql_secure_installation
```

5. Se um firewall estiver presente no sistema, abrir a porta TCP 3306 para conexões externas MySQL pode ser estabelecida.

No Ubuntu, o UFW é o firewall padrão. Abra a porta com o comando:

```
ufw allow mysql
```

No RHEL/CentOS:

- a. Edite o arquivo `/etc/sysconfig/iptables` e adicione a seguinte linha no início da cadeia INPUT.

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

- b. Agora recarregue as regras do iptables.

```
service iptables restart
```

6. Retorne para o shell de root em seu primeiro servidor de gerenciamento.
7. Configure o banco de dados. O seguinte comando cria o usuário no banco de dados em nuvem.

- ▶ Em `dbpassword`, especifique a senha a ser atribuída ao usuário nuvem. Você pode escolher por não fornecer a senha.
- ▶ Em `deploy-as`, especifique o username e senha do usuário que está implementando o database. No comando a seguir, é suposto que o usuário `root` está user implementando o database e criando o usuário `cloud`.
- ▶ (Opcional) Para `encryption_type`, use `arquivo` ou `web` para indicar a técnica utilizada para passar a senha de criptografia de banco de dados. Padrão: `arquivo`. Consulte sobre [Senha e Criptografia de Chave](#).
- ▶ (Opcional) Para `management_server_key`, substitua a chave padrão que é usada para criptografar os parâmetros confidenciais no arquivo de propriedades CloudStack. Padrão: `senha`. É altamente recomendado que você substitua isso com um valor mais seguro. Consulte sobre [Senha e Criptografia de chave](#).
- ▶ (Opcional) Para `database_key`, substitua a chave padrão que é usada para criptografar os parâmetros confidenciais no banco de dados CloudStack. Padrão: `senha`. É altamente recomendado que você substitua isso com um valor mais seguro. Veja [Seção 4.5.5, "Sobre senha e chave de criptografia"](#).
- ▶ (Optional) For `management_server_ip`, you may explicitly specify cluster management server node IP. If not specified, the local IP address will be used.

```
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>
```

Quando o script estiver concluído, você deveria ver uma mensagem como "Iniciou com sucesso o banco de dados."

### 4.5.5. Sobre senha e chave de criptografia

O CloudStack armazena diversas senhas sensíveis e chaves secretas que são usadas para fornecer segurança. Estes valores são sempre criptografados automaticamente:

- ▶ Chave secreta de banco de dados
- ▶ Senha de banco de dados
- ▶ Chaves SSH
- ▶ Senha de root do nó computacional
- ▶ Senha de VPN
- ▶ Chave secreta de API de usuário
- ▶ Senha de VNC

O CloudStack usa a biblioteca Java Simplified Encryption (JASYPT). Os dados são encriptados e decriptados usando uma chave secreta do banco de dados, a qual é armazenada em um dos arquivos de propriedades internas do CloudStack, juntamente com a senha do banco de dados. Os outros valores encriptados listados acima, tais como chaves SSH, estão no database interno do CloudStack.

Obviamente, a chave secreta do banco de dados não pode ser armazenada em claro – ela deve ser encriptada. Como então o CloudStack a lê? Uma segunda chave secreta deve ser fornecida por uma fonte externa durante a ativação do servidor de gerenciamento. Esta chave pode ser fornecida em um de dois modos: carregada de um arquivo ou fornecida pelo administrador do CloudStack. O banco de dados do CloudStack tem um novo item de configuração que indica qual destes métodos será usado. Se o tipo de encriptação é "file," a chave deve estar em um arquivo em uma localização conhecida. Se o tipo de encriptação é "web," o administrador executa o utilitário `com.cloud.utils.crypt.EncryptionSecretKeySender`, que transmite a chave para o servidor de gerenciamento através de uma porta conhecida.

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. Preparar os compartilhamentos NFS

O CloudStack precisa de um lugar para manter a storage primária e secundária (ver Visão geral da infraestrutura de nuvem). Ambas podem ser compartilhamentos NFS. Esta seção mostra como configurar os compartilhamentos NFS antes de adicionar a storage para o CloudStack.



#### Storage alternativa

NFS is not the only option for primary or secondary storage. For example, you may use Ceph RBD, GlusterFS, iSCSI, and others. The choice of storage system will depend on the choice of hypervisor and whether you are dealing with primary or secondary storage.

Os requisitos para storage primária e secundária são descritos em:

- ▶ [Seção 2.6, "Sobre storage primária"](#)
- ▶ [Seção 2.7, "Sobre storage secundária"](#)

Uma instalação de produção geralmente usa um servidor NFS separado. Veja [Seção 4.5.6.1, "Using a Separate NFS Server"](#).

Você também pode usar o nó servidor de gerenciamento como o servidor NFS. Isto é mais característico do processo de instalação de avaliação, mas é tecnicamente possível em uma implantação maior. Veja [Seção 4.5.6.2, "Using the Management Server as the NFS Server"](#).

#### 4.5.6.1. Using a Separate NFS Server

This section tells how to set up NFS shares for secondary and (optionally) primary storage on an NFS server running on a separate node from the Management Server.

The exact commands for the following steps may vary depending on your operating system version.



### Atenção

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

1. On the storage server, create an NFS share for secondary storage and, if you are using NFS for primary storage as well, create a second NFS share. For example:

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

2. To configure the new directories as NFS exports, edit `/etc/exports`. Export the NFS share(s) with `rw,async,no_root_squash`. For example:

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

Insert the following line.

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

3. Export the `/export` directory.

```
# exportfs -a
```

4. On the management server, create a mount point for secondary storage. For example:

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

5. Mount the secondary storage on your Management Server. Replace the example NFS server name and NFS share paths below with your own.

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

#### 4.5.6.2. Using the Management Server as the NFS Server

This section tells how to set up NFS shares for primary and secondary storage on the same node with the Management Server. This is more typical of a trial installation, but is technically possible in a larger deployment. It is assumed that you will have less than 16TB of storage on the host.

The exact commands for the following steps may vary depending on your operating system version.

1. On RHEL/CentOS systems, you'll need to install the `nfs-utils` package:

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

2. On the Management Server host, create two directories that you will use for primary and secondary storage. For example:

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

3. To configure the new directories as NFS exports, edit `/etc/exports`. Export the NFS share(s) with `rw,async,no_root_squash`. For example:

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

Insert the following line.

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

4. Export the `/export` directory.

```
# exportfs -a
```

5. Edit the `/etc/sysconfig/nfs` file.

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

Uncomment the following lines:

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

6. Edit the `/etc/sysconfig/iptables` file.

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

Add the following lines at the beginning of the INPUT chain where `<NETWORK>` is the network that you'll be using:

```
-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 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
```

- Run the following commands:

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

- If NFS v4 communication is used between client and server, add your domain to `/etc/idmapd.conf` on both the hypervisor host and Management Server.

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

Remove the character `#` from the beginning of the Domain line in `idmapd.conf` and replace the value in the file with your own domain. In the example below, the domain is `company.com`.

```
Domain = company.com
```

- Reboot the Management Server host.

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

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

- Log in to the hypervisor host.
- Be sure NFS and `rpcbind` are running. The commands might be different depending on your OS. For example:

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

- Log back in to the hypervisor host and try to mount the `/export` directories. For example (substitute your own management server name):

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

#### 4.5.7. Preparar e ativar servidores de gerenciamento adicionais

Para o segundo e subsequentes servidores de gerenciamento, você irá instalar o software servidor de gerenciamento, conectá-lo ao banco de dados e configurar o sistema operacional para o servidor de gerenciamento.

- Execute os passos em [Seção 4.5.2, "Preparando o sistema operacional"](#) e [Seção 3.6, "Building RPMs from Source"](#) ou [Seção 3.5, "Building DEB packages"](#) conforme apropriado.
- Este passo somente é necessário em instalações onde XenServer é instalado nos hosts hipervisores.

Baixe `vhd-util` de [vhd-util](#)

Copy `vhd-util` to `/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver`.

- Certifique-se de que os serviços necessários estão ativos e configurados como ativos no boot.

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

- Configure o cliente de banco de dados. Note a ausência do argumento `--deploy-as` neste caso. (Para mais detalhes sobre os argumentos para este comando, consulte [Seção 4.5.4.2, "Instale o banco de dados em um nó separado"](#).)

```
# cloudstack-setup-databases cloud:dbpassword@dbhost -e encryption_type -m
management_server_key -k database_key -i management_server_ip
```

- Configure o sistema operacional e inicie o servidor de gerenciamento:

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

O servidor de gerenciamento neste nó deve agora estar em execução.

- Repita estes passos em cada servidor de gerenciamento adicional.
- Be sure to configure a load balancer for the Management Servers. See [Seção 12.6, "Management Server Load Balancing"](#).

#### 4.5.8. Prepare o template de máquina virtual de sistema

Storage secundária deve ser gerada com um template que é usado por máquinas virtuais de sistema do CloudStack.



Nota

Ao copiar e colar um comando, certifique-se que o comando tenha colado como uma única linha antes de executar. Alguns visualizadores de documentos podem introduzir quebras de linha indesejadas no texto copiado.

1. No servidor de gerenciamento, execute um ou mais dos seguintes comandos `nuvem-install-sys-tmpl` para recuperar e descomprimir o template de máquina virtual de sistema. Execute o comando para cada tipo de hipervisor que você espera que os usuários finais executem nesta zona.  
Se o ponto de montagem da storage secundária não é nomeado `/mnt/secondary`, substitua pelo nome do seu próprio ponto de montagem.  
Se você definiu o tipo de criptografia do banco de dados do CloudStack para "web" quando você configurou o banco de dados, você deve agora adicionar o parâmetro `-s <management-server-secret-key>`. Veja [Seção 4.5.5, "Sobre senha e chave de criptografia"](#).  
Este processo requer aproximadamente 5 GB de espaço livre no sistema de arquivos local e até 30 minutos de cada vez que é executado.

► Para XenServer:

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

► Para vSphere:

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

► Para KVM:

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

On Ubuntu, use the following path instead:

```
# /usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmpl
```

2. Se você estiver usando um servidor NFS separado, execute este passo. Se você estiver usando o servidor de gerenciamento como servidor NFS, você não deve executar este passo.

Quando o script terminar, desmonte a storage secundária e remova o diretório criado.

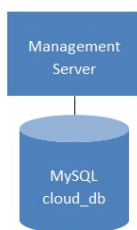
```
# umount /mnt/secondary  
# rmdir /mnt/secondary
```

3. Repita estes passos em cada servidor de storage secundária.

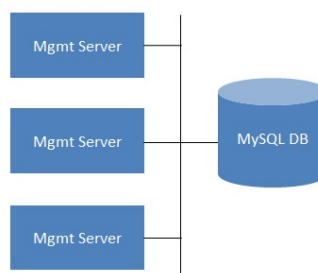
## 4.5.9. Instalação completa! Próximos passos

Parabéns! Você instalou o servidor de gerenciamento do CloudStack e o database que ele usa para armazenar dados persistentes.

### Single Management Server: Installation Complete!



### Multiple Management Servers: Installation Complete!



O que você deve fazer a seguir?

- Mesmo sem adicionar qualquer infraestrutura de nuvem, você pode executar a interface de usuário para ter uma ideia do que é oferecido e como interagir com o CloudStack numa base contínua. Veja [Capítulo 5, Interface do usuário](#).
- Quando você estiver pronto, adicione a infraestrutura de nuvem e tente executar algumas máquinas virtuais, assim você poderá ver como o CloudStack gerencia a infraestrutura. Veja [Capítulo 6, Passos para provisionamento de sua infraestrutura de nuvem](#).

# Capítulo 5. Interface do usuário

## 5.1. Login na interface de usuário

### 5.1.1. End User's UI Overview

### 5.1.2. Root Administrator's UI Overview

- 5.1.3. Fazendo login como o administrador root
- 5.1.4. Changing the Root Password

## 5.2. Usando as chaves SSH para autenticação.

- 5.2.1. Criando um template de instância que suporta chaves SSH
- 5.2.2. Criando o par de chaves SSH
- 5.2.3. Criando uma instância
- 5.2.4. Fazendo login usando o par de chaves SSH
- 5.2.5. Resetting SSH Keys

## 5.1. Login na interface de usuário

O CloudStack provê uma interface de usuário web que pode ser usada tanto por administradores e usuários finais. A versão apropriada da interface é apresentada dependendo das credenciais utilizadas para login. A interface de usuário está disponível em navegadores populares, incluindo o IE7, IE8, IE9, Firefox 3.5+, Firefox 4, Safari 4 e Safari 5. A URL é: (substitua pelo endereço IP de seu servidor de gerenciamento)

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

Em uma nova instalação do servidor de gerenciamento, uma tela de apresentação é exibida. Em visitas posteriores, você verá uma tela de login onde se especifica o seguinte para seguir para o painel de instrumentos:

### Nome de usuário

A identificação de usuário de sua conta. O nome default de usuário é admin.

### Senha

A senha associada com a identificação do usuário. A senha para identificação default é password.

### Domínio

Se você é um usuário root, deixe este campo em branco.

Se você é um usuário nos subdomínios, forneça o caminho completo para o domínio, excluindo o domínio root.

Por exemplo, suponha que múltiplos níveis são criados sob o domínio root, tal como Comp1/hr. Os usuários no domínio Comp1 devem informar Comp1 no campo Domain, enquanto os usuários no domínio Comp1/sales devem informar Comp1/sales.

Para mais orientação sobre as escolhas apresentadas quando você faz login na interface de usuário, veja [Seção 5.1.3, "Fazendo login como o administrador root"](#).

### 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. Fazendo login como o administrador root

Depois do software do servidor de gerenciamento estar instalado e executando, você pode executar a interface de usuário do CloudStack. Esta interface de usuário está disponível para ajudá-lo a montar, visualizar e gerenciar sua infraestrutura de nuvem.

1. Abra o seu navegador web favorito e acesse esta URL. Substitua o endereço IP de seu servidor de gerenciamento:

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

Após fazer login em um nova instalação do servidor de gerenciamento, uma tela de apresentação é exibida. Em visitas posteriores, você será levado diretamente ao painel de controle.

2. Se você vê a tela apresentada somente na primeira vez, escolha uma das opções seguintes.
  - ▶ **Continue with basic setup.** Escolha esta opção se você está apenas experimentando o CloudStack, e você deseja uma explicação guiada sobre a configuração mais simples possível de modo a iniciar o uso imediatamente. Iremos ajudá-lo a configurar uma nuvem com os seguintes recursos: uma máquina única executando o CloudStack e que provê storage através do NFS; uma máquina única executando máquinas virtuais sob um hipervisor XenServer ou KVM; uma rede pública compartilhada.  
Os prompts nesta visita guiada devem lhe fornecer toda a informação que você precisa, mas se você deseja um pouco mais de detalhe, você pode seguir o Guia de instalação de avaliação.
  - ▶ **I have used CloudStack before.** Escolha esta opção se você já passou pela fase de design e planejou uma implementação mais sofisticada, ou você está pronto para incrementar uma implementação de avaliação que você preparou anteriormente através das telas de configuração básica. Na interface de usuário do administrador, você pode iniciar a utilização dos recursos mais poderosos de CloudPlatform, tais como

configuração avançada de rede VLAN, alta disponibilidade, elementos adicionais de rede tais como balanceadores de carga e firewalls, e suporte para múltiplos hipervisores, incluindo Citrix XenServer, KVM, e VMware vSphere.

O painel de instrumentos do administrador root é exibido.

3. Você deve escolher uma nova senha de root. Se você escolheu configuração básica, você será requisitado a criar uma nova senha imediatamente. Se você selecionou usuário experiente, siga os passos em [Seção 5.1.4, "Changing the Root Password"](#).



### Atenção


Você está fazendo login como o administrador root. Esta conta gerencia a implementação do CloudStack, incluindo a infraestrutura física. O administrador root pode modificar opções de configuração para alterar funcionalidade básica, criar ou apagar contas de usuários, e tomar várias ações que somente devem ser executadas por uma pessoa autorizada. Por favor, altere a senha default para uma nova e única senha.

## 5.1.4. Changing the Root Password

During installation and ongoing cloud administration, you will need to log in to the UI as the root administrator. The root administrator account manages the CloudStack deployment, including physical infrastructure. The root administrator can modify configuration settings to change basic functionality, create or delete user accounts, and take many actions that should be performed only by an authorized person. When first installing CloudStack, be sure to change the default password to a new, unique value.

1. Open your favorite Web browser and go to this URL. Substitute the IP address of your own Management Server:

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

2. Log in to the UI using the current root user ID and password. The default is admin, password.
3. Click Accounts.
4. Click the admin account name.
5. Click View Users.
6. Click the admin user name.
7. Click the Change Password button. 
8. Type the new password, and click OK.

## 5.2. Usando as chaves SSH para autenticação.

Além da autenticação de usuário e senha, o CloudStack suporta o uso de chaves SSH para efetuar login em infraestrutura de nuvem para segurança adicional. Você pode usar a API `createSSHKeyPair` para gerar as chaves SSH.

Como cada usuário da nuvem tem sua própria chave SSH, um usuário da nuvem não pode efetuar login em instâncias de outro usuário da nuvem, a menos que eles compartilham seus arquivos de chave SSH. Usando um único par chave SSH, você pode gerenciar várias instâncias.

### 5.2.1. Criando um template de instância que suporta chaves SSH

Crie um template de instância que suporta chaves SSH.

1. Crie uma nova instância usando o template fornecido pelo cloudstack.  
Para informações adicionais na criação de nova instância, veja
2. Faça download do script cloudstack de [The SSH Key Gen Script](#) para a instância que você criou.

```
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. Copie o arquivo para `/etc/init.d`.

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

4. Dê as permissões necessárias ao script:

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

5. Execute o script ao iniciar o sistema operacional:

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

6. Pare a instância.

### 5.2.2. Criando um par de chaves SSH

Você deve fazer uma chamada para o método `api createSSHKeyPair`. Você pode usar a biblioteca API Python do CloudStack ou os comandos `curl` para fazer a chamada para a API CloudStack.

Por exemplo, faça uma chamada a partir do servidor CloudStack para criar um par de chaves SSH chamado de "keypair-doc" para a conta admin no domínio root:



### Nota



# Capítulo 6. Passos para provisionamento de sua infraestrutura de nuvem

## 6.1. Visão geral dos passos de provisionamento

### 6.2. Adding Regions (optional)

- 6.2.1. The First Region: The Default Region
- 6.2.2. Adding a Region
- 6.2.3. Adding Third and Subsequent Regions
- 6.2.4. Deleting a Region

### 6.3. Adicionando uma zona

- 6.3.1. Configuração de zona básica
- 6.3.2. Advanced Zone Configuration

### 6.4. Adicionando um pod

### 6.5. Adicionando um cluster

- 6.5.1. Add Cluster: KVM or XenServer
- 6.5.2. Add Cluster: vSphere

### 6.6. Adding a Host

- 6.6.1. Adding a Host (XenServer or KVM)
- 6.6.2. Adding a Host (vSphere)

### 6.7. Adicionar Storage Primário

- 6.7.1. System Requirements for Primary Storage
- 6.7.2. Adding Primary Storage

### 6.8. Adicionar Storage Secundário

- 6.8.1. System Requirements for Secondary Storage
- 6.8.2. Adding Secondary Storage

### 6.9. Initialize and Test

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 [Capítulo 2, Conceitos de infraestrutura de nuvem](#).

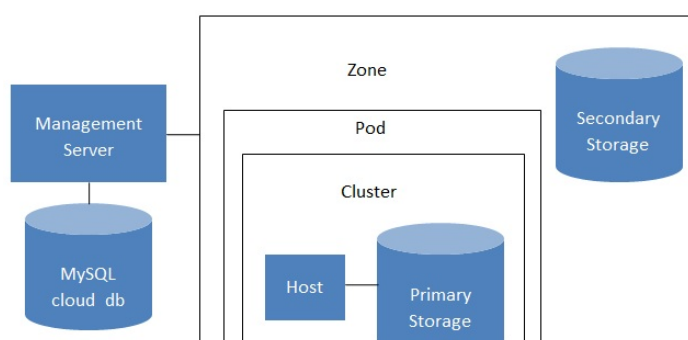
## 6.1. Visão geral dos passos de provisionamento

Depois do servidor de gerenciamento ser instalado e estar funcionando, você pode adicionar os recursos de computação para gerenciá-lo. Para uma visão geral de como uma infraestrutura de nuvem CloudStack é organizada, veja [Seção 1.3.2, “Visão geral da infraestrutura de nuvem”](#).

Para provisionar a infraestrutura de nuvem, ou para escalá-la a qualquer momento, siga estes procedimentos:

1. Define regions (optional). See [Seção 6.2, “Adding Regions \(optional\)”](#).
2. Add a zone to the region. See [Seção 6.3, “Adicionando uma zona”](#).
3. Add more pods to the zone (optional). See [Seção 6.4, “Adicionando um pod”](#).
4. Add more clusters to the pod (optional). See [Seção 6.5, “Adicionando um cluster”](#).
5. Add more hosts to the cluster (optional). See [Seção 6.6, “Adding a Host”](#).
6. Add primary storage to the cluster. See [Seção 6.7, “Adicionar Storage Primário”](#).
7. Add secondary storage to the zone. See [Seção 6.8, “Adicionar Storage Secundário”](#).
8. Inicialize e teste a nova nuvem. Veja [Seção 6.9, “Initialize and Test”](#).

Quando você terminar estes passos, você terá uma implantação com a seguinte estrutura básica:





## 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 [Seção 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_sdah0BpjNejPgEst35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&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_sdah0BpjNejPgEst35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP001hU%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_sdah0BpjNejPgEst35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP001hU%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/c
lient&apiKey=miVr6X7u6bN_sdah0BpjNejPgEst35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP001hU%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/c
lient&apiKey=miVr6X7u6bN_sdah0BpjNejPgEst35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP001hU%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_sdah0BpjNejPgEst35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP001hU%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/c
lient&apiKey=miVr6X7u6bN_sdah0BpjNejPgEst35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP001hU%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_sdah0BpjNejPgEst35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP001h
U%3D

http://<IP_of_region_2_Management_Server>:8080/client/api?
command=removeRegion&id=3&apiKey=miVr6X7u6bN_sdah0BpjNejPgEst35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP001h
U%3D
```

## 6.3. Adicionando uma zona

Nestes passos se supõe que você já está logado na interface de usuário do CloudStack. Veja [Seção 5.1, "Login na interface de usuário"](#).

1. (Opcional) Se você irá usar Swift para storage secundária na nuvem, você precisa adicioná-la antes de adicionar zonas.

- a. Faça login na interface de usuário do CloudStack como administrador.
- b. Se esta é a primeira vez utilizando a interface de usuário, você verá uma tela de apresentação. Selecione "Experienced user." O painel de instrumentos é exibido.
- c. Na barra de navegação à esquerda, clique em Global Settings.
- d. Na caixa de pesquisa, digite swift.enable e clique no botão de pesquisa.
- e. Clique no botão de edit e marque swift.enable como true. 
- f. Reinicie o servidor de gerenciamento.

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

- g. Recarregue a interface de usuário do CloudStack no navegador e faça logon novamente.

2. Na barra de navegação à esquerda, selecione Infrastructure.



2. Na barra de navegação à esquerda, clique em **Networks**.
  3. Em **Zones**, clique em **View More**.
  4. (Opcional) Se você está utilizando **storage Swift**, clique **Enable Swift**. Forneça o seguinte:
    - ▶ **URL**. A URL Swift.
    - ▶ **Account**. A conta Swift.
    - ▶ **Username**. O nome de usuário associado à conta Swift.
    - ▶ **Key**. A chave Swift.
  5. Clique em **Add Zone**. O consultor de criação de zona será exibido.
  6. Selecione um dos seguintes tipos de rede:
    - ▶ **Basic**. Para redes no estilo AWS. Provê um rede única a cada instância de máquina virtual é assinalado um endereço IP diretamente da rede. O isolamento de hóspedes pode ser provido através de recursos da camada 3 como grupos seguros (filtragem de endereço IP de origem).
    - ▶ **Advanced**. Para topologias de rede mais sofisticadas. Este modelo de rede provê a mais alta flexibilidade na definição de redes hóspedes e oferece customização de rede como firewall, VPN, ou suporte a balanceador de carga.
- For more information about the network types, see [Seção 2.8, "Sobre redes físicas"](#).
7. O restante dos passos diferem dependendo se você escolheu **Basic** ou **Advanced**. Continue com os passos que se aplicam a você:
    - ▶ [Seção 6.3.1, "Configuração de zona básica"](#)
    - ▶ [Seção 6.3.2, "Advanced Zone Configuration"](#)

### 6.3.1. Configuração de zona básica

1. Após selecionar **Basic** no assistente de **Adicionar Zona** e clicar em **Next**, você será solicitado a digitar os seguintes detalhes. Em seguida, clique em **Next**.
  - ▶ **Name**. O nome da zona.
  - ▶ **DNS 1 and 2**. Estes são os servidores DNS utilizados pelas máquinas virtuais na zona. Estes servidores serão acessados pela rede pública que será adicionada posteriormente. Os IPs públicos da zona deverão ter acesso a estes servidores.
  - ▶ **Internal DNS 1 and Internal DNS 2**. Estes são os servidores DNS utilizados pelas máquinas virtuais na zona (estas são máquinas virtuais usadas pelo CloudStack tais como os roteadores virtuais, proxies console e máquinas virtuais de storage secundária). Estes servidores DNS serão acessados através da interface de gerenciamento de tráfego rede das máquinas virtuais de sistema. O endereço IP privado que você fornecer para os pods devem ter uma rota para o servidor DNS interno identificado aqui.
  - ▶ **Hypervisor**. (Introduzido na versão 3.0.1) Escolha o hipervisor para primeiro cluster na zona. Você pode adicionar clusters com diferentes hipervisores mais tarde, depois de você terminar de adicionar a zona.
  - ▶ **Network Offering**. Sua escolha aqui determina quais serviços de rede estarão disponíveis na rede para máquinas virtuais hóspedes.

Network Offering	Descrição
DefaultSharedNetworkOfferingWithSGService	Se você quer habilitar grupos de segurança para isolamento de tráfego de hóspedes, escolha esta. (Veja Utilizando grupos de segurança para controlar o tráfego de máquinas virtuais).
DefaultSharedNetworkOffering	Se você não precisa de grupos de segurança, escolha esta.
DefaultSharedNetscalerEIPandELBNetworkOffering	Se você tiver instalado o dispositivo Citrix NetScaler como parte de sua rede de zona, e você estará usando o seu IP elástico e características de balanceamento de carga elástica, escolha esta. Com os recursos de EIP e ELB, uma zona básica com grupos de segurança habilitados pode oferecer NAT estático 1:1 e balanceamento de carga.

- ▶ **Network Domain**. (Opcional) Se você quiser atribuir um nome de domínio especial à rede de máquina virtual hóspede, especifique o sufixo DNS.
  - ▶ **Public**. Uma zona pública está disponível para todos usuários. Uma zona que não é pública será atribuída a um domínio específico. Somente a usuários nesse domínio será permitido criar máquinas virtuais hóspedes nesta zona.
2. Escolha os tipos de tráfego que serão transportados pela rede física.
 

Os tipos de tráfego são: gerência, público, hóspede, e storage. Para mais informações sobre os tipos, role sobre os ícones para exibir suas dicas de ferramentas, ou veja **Tipos de tráfego de rede de zona básica**. Esta tela começa com alguns tipos de tráfego já atribuídos. Para adicionar mais, arraste e solte os tipos de tráfego na rede. Você também pode alterar o nome da rede, se desejar.
  3. (Introduced in version 3.0.1) Assign a network traffic label to each traffic type on the physical network. These labels must match the labels you have already defined on the hypervisor host. To assign each label, click the **Edit** button under the traffic type icon. A popup dialog appears where you can type the label, then click **OK**.
 

Essas etiquetas de tráfego serão definidas apenas para o hipervisor selecionado para o primeiro cluster. Para todos os outros hipervisores, as etiquetas podem ser configuradas depois que a zona é criada.
  4. Clique em **Next**.
  5. (Somente NetScaler) Se você escolheu a oferta de rede para **NetScaler**, você tem uma tela adicional para preencher. Forneça as informações solicitadas para configurar o **NetScaler**, em seguida, clique em **Next**.
    - ▶ **IP address**. O endereço NSIP (NetScaler IP) do dispositivo NetScaler.
    - ▶ **Username/Password**. A autenticação de credenciais para acessar o dispositivo. O CloudStack usa essas credenciais para acessar o dispositivo.
    - ▶ **Type**. O tipo de dispositivo NetScaler que está sendo adicionado. Pode ser **NetScaler VPX**, o **NetScaler MPX**, ou **NetScaler SDX**. Para uma comparação dos tipos, veja **Sobre como usar um balanceador de carga**

NetScaler.

- » **Public interface.** A Interface de NetScaler que está configurada para ser parte da rede pública.
  - » **Private interface.** A Interface de NetScaler que está configurada para ser parte da rede privada.
  - » **Number of retries.** Número de vezes para tentar um comando no dispositivo antes de considerar falhas na operação. O default é 2.
  - » **Capacity.** Número de redes hóspedes/contas que irão compartilhar este dispositivo NetScaler.
  - » **Dedicated.** Quando marcado como dedicado, este dispositivo será dedicado a uma única conta. Quando dedicado é verificado, o valor no campo Capacity não tem significado - implicitamente, o seu valor é 1.
6. (NetScaler apenas) Configure a faixa de IP para tráfego público. Os IPs nesta faixa serão usados para a capacidade de NAT estática que você ativou selecionando a oferta de rede para NetScaler com EIP e ELB. Insira os detalhes seguintes, e então clique em Add. Se desejar, você pode repetir este passo para adicionar mais intervalos de IP. Quando terminar, clique em Next.
- » **Gateway.** O gateway em uso para estes endereços IPs.
  - » **Netmask.** A netmask associada com este intervalo de IP.
  - » **VLAN.** A VLAN que será usada pelo tráfego público.
  - » **Start IP/End IP.** Um intervalo de endereços IP que se supõe serem acessíveis da Internet e que serão alocados para acesso a máquinas virtuais hóspedes.
7. Em uma nova zona, o CloudStack adiciona o primeiro pod para você. Você sempre pode adicionar pods mais tarde. Para uma visão geral do que é pod, veja [Seção 2.3 "Sobre pods"](#). Para configurar o primeiro pod, informe o que se segue, então clique em Next:
- » **Pod Name.** Um nome para o pod.
  - » **Reserved system gateway.** O gateway para os hosts no pod.
  - » **Reserved system netmask.** O prefixo de rede que define a sub-rede do pod. Use notação CIDR.
  - » **Start/End Reserved System IP.** O intervalo IP na rede de gerenciamento que o CloudStack usa para gerenciar várias máquinas virtuais de sistema, tais como as máquinas virtuais de storage secundária, máquinas virtuais de proxy de console, e DHCP. Para mais informações, veja Endereços IP reservados pelo sistema.
8. Configure a rede para o tráfego de hóspedes. Forneça o que se segue, então clique em Next:
- » **Guest gateway.** O gateway que os hóspedes devem utilizar.
  - » **Guest netmask.** A máscara de rede em uso na sub-rede que os hóspedes utilizarão.
  - » **Guest start IP/End IP.** Informe o primeiro e o último endereços IP que definem um intervalo que o CloudStack pode atribuir aos convidados.  
Recomendamos fortemente o uso de várias placas de rede. Se várias placas de rede são usadas, elas podem estar em uma sub-rede diferente.  
Se uma placa de rede é utilizada, estes IPs devem estar na mesma CIDR que o CIDR do pod.
9. Em um novo pod, o CloudStack adiciona o primeiro cluster para você. Você sempre pode adicionar clusters mais tarde. Para uma visão geral do que um cluster é, veja Sobre clusters. Para configurar o primeiro cluster, informe o que segue, então clique em Next:
- » **Hypervisor.** (Versão 3.0.0 apenas; na 3.0.1, este campo é somente leitura) Escolha o tipo de software hipervisor que todos os hosts deste cluster executarão. Se você escolher VMware, campos adicionais aparecem para que você possa dar informações sobre um cluster vSphere. Para os servidores vSphere, recomendamos criar o cluster de hosts em vCenter e então adicionar o cluster inteiro no CloudStack. Veja Adicionar cluster: vSphere.
  - » **Cluster name.** Informe um nome para o cluster. Este pode ser um texto de sua escolha e não é usado pelo CloudStack.
10. Em um novo cluster, o CloudStack adiciona o primeiro host para você. Você sempre pode adicionar mais hosts depois. Para uma visão geral do que um host é, veja Sobre hosts.



### Nota

Quando você adicionar um host hipervisor ao CloudStack, o host não deve ter nenhuma máquina virtual já executando.

Antes de configurar o host, você precisa instalar o software hipervisor no host. Você precisará saber qual versão do software hipervisor é suportada pelo CloudStack e qual configuração adicional é requerida para garantir que o host trabalhará com CloudStack. Para encontrar detalhes dessa instalação, veja:

- » Instalação e configuração do Citrix XenServer
- » Instalação e configuração do VMware vSphere
- » Instalação e configuração do KVM

Para configurar o primeiro host, informe o que segue, então clique em Next:

- » **Host Name.** O nome DNS ou endereço IP do host.
- » **Username.** O nome do usuário é root.
- » **Password.** Esta é a senha para o usuário identificado acima (da sua instalação XenServer ou KVM).
- » **Host Tags.** (Opcional) Qualquer rótulo que você usa para categorizar hosts para facilidade de manutenção. Por exemplo, você pode definir isso para o rótulo de alta disponibilidade da nuvem (definido no parâmetro de configuração `ha.tag global`) se você quer este host a ser usado apenas para máquinas virtuais com o recurso "alta disponibilidade" habilitado. Para mais informações, veja Máquinas virtuais HA-Enabled, assim como HA para hosts.

11. Em um novo cluster, o CloudStack acrescenta o primeiro servidor de storage primária para você. Você sempre pode adicionar mais servidores mais tarde. Para uma visão geral do que é storage primária, veja Sobre storage primária.

Para configurar o primeiro servidor de storage primária, entre o que segue, então clique em Next:

- » **Name.** O nome do dispositivo do storage.
- » **Protocol.** Para XenServer, escolha NFS, iSCSI ou PreSetup. Para o KVM, escolha NFS, SharedMountPoint.

... ou NFS. Para vSphere escolha VMFS (iSCSI ou FiberChannel) ou NFS. Os campos restantes na tela variam dependendo do que você escolher aqui.

### 6.3.2. Advanced Zone Configuration

1. After you select Advanced in the Add Zone wizard and click Next, you will be asked to enter the following details. Then click Next.
  - **Nome.** O nome da zona.
  - **DNS 1 e 2.** Serão os servidores DNS utilizados pelas máquinas virtuais na Zona. Estes servidores serão acessados pela rede pública que será adicionada a frente. Os ips públicos da zona deverão ter acesso a estes servidores.
  - **Internal DNS 1 and Internal DNS 2.** These are DNS servers for use by system VMs in the zone (these are VMs used by CloudStack itself, such as virtual routers, console proxies, and Secondary Storage VMs.) These DNS servers will be accessed via the management traffic network interface of the System VMs. The private IP address you provide for the pods must have a route to the internal DNS server named here.
  - **Network Domain.** (Opcional) Se você quiser atribuir um nome de domínio especial à rede de máquina virtual convidada, especificar o sufixo DNS.
  - **Guest CIDR.** This is the CIDR that describes the IP addresses in use in the guest virtual networks in this zone. For example, 10.1.1.0/24. As a matter of good practice you should set different CIDRs for different zones. This will make it easier to set up VPNs between networks in different zones.
  - **Hypervisor.** (Introduced in version 3.0.1) Escolha o hipervisor para primeiro cluster na zona. Você pode adicionar clusters com diferentes hipervisores mais tarde
  - **Public.** Uma zona pública está disponível para todos usuários. Uma zona que não é público será atribuído a um domínio particular. Somente usuários nesse domínio serão permitido criar máquinas virtuais convidadas nesta zona.
2. Escolher os tipos de tráfego serão transmitidos pela rede física.

The traffic types are management, public, guest, and storage traffic. For more information about the types, roll over the icons to display their tool tips, or see [Seção 2.8.3, "Tipos de tráfego de rede da zona avançada"](#). This screen starts out with one network already configured. If you have multiple physical networks, you need to add more. Drag and drop traffic types onto a greyed-out network and it will become active. You can move the traffic icons from one network to another; for example, if the default traffic types shown for Network 1 do not match your actual setup, you can move them down. You can also change the network names if desired.
3. (Introduced in version 3.0.1) Assign a network traffic label to each traffic type on each physical network. These labels must match the labels you have already defined on the hypervisor host. To assign each label, click the Edit button under the traffic type icon within each physical network. A popup dialog appears where you can type the label, then click OK.

Esses label de tráfego serão definidos apenas para o hipervisor selecionado para o primeiro cluster. Para todos os outros hipervisores, os rótulos podem ser configurados depois que a zona é criado.
4. Clicar em Next
5. Configure the IP range for public Internet traffic. Enter the following details, then click Add. If desired, you can repeat this step to add more public Internet IP ranges. When done, click Next.
  - **Gateway.** O gateway em uso para estes endereços IPs.
  - **Netmask.** O netmask associado com esta faixa de IP
  - **VLAN.** A VLAN que será usada pelo tráfego público will be used for public traffic.
  - **Start IP/End IP.** A range of IP addresses that are assumed to be accessible from the Internet and will be allocated for access to guest networks.
6. Em uma nova zona, CloudStack acrescenta primeiro pod para você. Você sempre pode adicionar pods mais tarde. Para uma visão geral do que é pod, veja [Seção 2.3, "Sobre pods"](#). Para configurar o primeiro pod, enter o seguinte, clique em Next
  - **Pod Name.** Um nome para o pod.
  - **Reserved system gateway.** O gateway para hóspedes em que pod
  - **Reserved system netmask.** O prefixo de rede que define a subrede do pod. Use notação CIDR.
  - **Start/End Reserved System IP.** The IP range in the management network that CloudStack uses to manage various system VMs, such as Secondary Storage VMs, Console Proxy VMs, and DHCP. For more information, see [Seção 2.8.6, "Endereços IP reservados pelo sistema"](#).
7. Specify a range of VLAN IDs to carry guest traffic for each physical network (see VLAN Allocation Example ), then click Next.
8. In a new pod, CloudStack adds the first cluster for you. You can always add more clusters later. For an overview of what a cluster is, see [Seção 2.4, "Sobre clusters"](#).

Para configurar o primeiro cluster, Entre o seguinte, então clique Next:

  - **Hypervisor.** (Version 3.0.0 only; in 3.0.1, this field is read only) Choose the type of hypervisor software that all hosts in this cluster will run. If you choose VMware, additional fields appear so you can give information about a vSphere cluster. For vSphere servers, we recommend creating the cluster of hosts in vCenter and then adding the entire cluster to CloudStack. See Add Cluster: vSphere .
  - (Versão 3.0.0 só, em 3.0.1, este campo é somente leitura) Escolha o tipo de software hypervisor que todos os anfitriões deste cluster será executado. Se você escolher a VMware, campos adicionais aparecem assim que você pode dar informações sobre um cluster vSphere. Para os servidores vSphere, recomendamos criar o cluster de hosts em vCenter e adicionando todo o cluster para CloudStack. Consulte Adicionar Cluster: vSphere.
9. In a new cluster, CloudStack adds the first host for you. You can always add more hosts later. For an overview of what a host is, see [Seção 2.5, "Sobre hosts"](#).



#### Nota

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

Antes de configurar o host, você precisa instalar o software hipervisor no host. Você precisará saber qual versão do software hipervisor é suportada pelo CloudStack e qual configuração adicional é requerida para

- Citrix XenServer Installation for CloudStack
- Instalação e configuração do VMware vSphere
- KVM Installation and Configuration

Para configurar o primeiro host, Entre o seguinte, então clique Next:

- **Host Name.** O nome DNS ou endereço IP do host.
- **Username.** Usually root.
- **Password.** Esta é a senha para o usuário chamado acima ( do seu XenServer ou instalação KVM).
- **Host Tags.** (Optional) Any labels that you use to categorize hosts for ease of maintenance. For example, you can set to the cloud's HA tag (set in the ha.tag global configuration parameter) if you want this host to be used only for VMs with the "high availability" feature enabled. For more information, see HA-Enabled Virtual Machines as well as HA for Hosts, both in the Administration Guide.

10. In a new cluster, CloudStack adds the first primary storage server for you. You can always add more servers later. For an overview of what primary storage is, see [Seção 2.6, "Sobre storage primária"](#).

Para configurar o primeiro servidor de storage primário, entre o seguinte, então clique Next.

- **Name.** O nome do dispositivo do storage.
- **Protocol.** For XenServer, choose either NFS, iSCSI, or PreSetup. For KVM, choose NFS, SharedMountPoint, CLVM, and RBD. For vSphere choose either VMFS (iSCSI or FiberChannel) or NFS. The remaining fields in the screen vary depending on what you choose here.

NFS	<p><b>Server.</b> The IP address or DNS name of the storage device.</p> <p><b>Path.</b> The exported path from the server.</p> <p><b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</p> <p>The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</p>
iSCSI	<p><b>Server.</b> The IP address or DNS name of the storage device.</p> <p><b>Target IQN.</b> The IQN of the target. For example, iqn.1986-03.com.sun:02:01ec9bb549-1271378984.</p> <p><b>Lun.</b> The LUN number. For example, 3.</p> <p><b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</p> <p>The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</p>
preSetup	<p><b>Server.</b> The IP address or DNS name of the storage device.</p> <p><b>SR Name-Label.</b> Enter the name-label of the SR that has been set up outside CloudStack.</p> <p><b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</p> <p>The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</p>
SharedMountPoint	<p><b>Path.</b> The path on each host that is where this primary storage is mounted. For example, "/mnt/primary".</p> <p><b>Tags (optional).</b> The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.</p> <p>The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.</p>
VMFS	<p><b>Server.</b> The IP address or DNS name of the vCenter server.</p> <p><b>Path.</b> A combination of the datacenter name and the datastore name. The format is "/" datacenter name "/" datastore name. For example,</p>

name / datastore name. For example, "/cloud.dc.VM/cluster1datastore".

**Tags (optional).** The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings.

The tag sets on primary storage across clusters in a Zone must be identical. For example, if cluster A provides primary storage that has tags T1 and T2, all other clusters in the Zone must also provide primary storage that has tags T1 and T2.

11. In a new zone, CloudStack adds the first secondary storage server for you. For an overview of what secondary storage is, see [Seção 2.7, "Sobre storage secundária"](#).  
Before you can fill out this screen, you need to prepare the secondary storage by setting up NFS shares and installing the latest CloudStack System VM template. See Adding Secondary Storage :
  - » **NFS Server.** The IP address of the server or fully qualified domain name of the server.
  - » **Path.** The exported path from the server.
12. Click Launch.

## 6.4. Adicionando um pod

Quando você cria uma nova zona, o CloudStack adiciona o primeiro pod para você. Você pode adicionar mais pods a qualquer momento usando o procedimento nesta seção.

1. Faça login na interface de usuário do CloudStack. Veja [Seção 5.1, "Login na interface de usuário"](#).
2. No painel de navegação à esquerda, selecione Infrastructure. Em Zones, clique View More, então clique na zona à qual você deseja adicionar um pod.
3. Clique na aba Compute and Storage. No nó Pods do diagrama, clique em View All.
4. Clique em Add Pod.
5. Forneça os seguintes detalhes no diálogo.
  - » **Name.** O nome do pod.
  - » **Gateway.** O gateway para os hosts no pod.
  - » **Netmask.** O prefixo de rede que define a subrede deste pod. Utilize a notação CIDR.
  - » **Start/End Reserved System IP.** O intervalo IP na rede de gerenciamento que o CloudStack usa para gerenciar várias máquinas virtuais de sistema, tais como as máquinas virtuais de storage secundária, máquinas virtuais de proxy de console, e DHCP. Para mais informações, veja Endereços IP reservados pelo sistema.
6. Clique em OK.

## 6.5. Adicionando um cluster

Você precisa informar ao CloudStack sobre os hosts que ele irá gerenciar. Hosts existem em clusters, portanto antes de você começar a adicionar hosts à nuvem, você deve adicionar pelo menos um cluster.

### 6.5.1. Add Cluster: KVM or XenServer

These steps assume you have already installed the hypervisor on the hosts and logged in to the CloudStack UI.

1. In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone in which you want to add the cluster.
2. Click the Compute tab.
3. In the Clusters node of the diagram, click View All.
4. Click Add Cluster.
5. Choose the hypervisor type for this cluster.
6. Choose the pod in which you want to create the cluster.
7. Enter a name for the cluster. This can be text of your choosing and is not used by CloudStack.
8. Clique em OK.

### 6.5.2. Add Cluster: vSphere

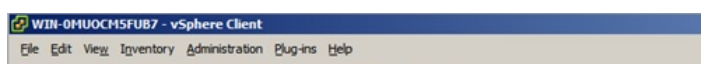
Host management for vSphere is done through a combination of vCenter and the CloudStack admin UI. CloudStack requires that all hosts be in a CloudStack cluster, but the cluster may consist of a single host. As an administrator you must decide if you would like to use clusters of one host or of multiple hosts. Clusters of multiple hosts allow for features like live migration. Clusters also require shared storage such as NFS or iSCSI.

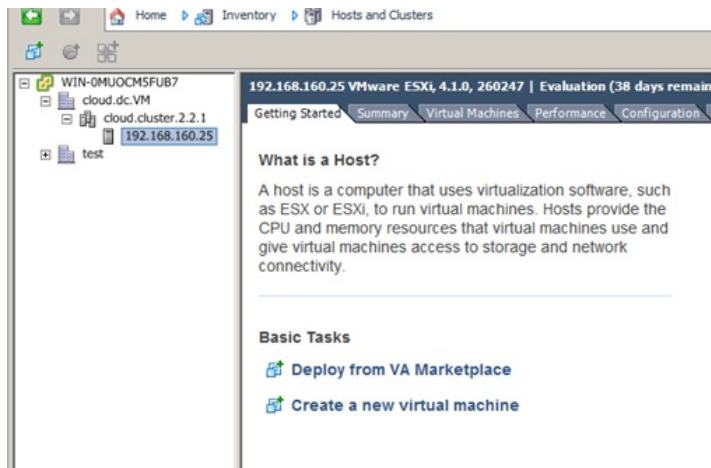
For vSphere servers, we recommend creating the cluster of hosts in vCenter and then adding the entire cluster to CloudStack. Follow these requirements:

- » Do not put more than 8 hosts in a vSphere cluster
- » Make sure the hypervisor hosts do not have any VMs already running before you add them to CloudStack.

To add a vSphere cluster to CloudStack:

1. Create the cluster of hosts in vCenter. Follow the vCenter instructions to do this. You will create a cluster that looks something like this in vCenter.





2. Log in to the UI.
3. In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone in which you want to add the cluster.
4. Click the Compute tab, and click View All on Pods. Choose the pod to which you want to add the cluster.
5. Click View Clusters.
6. Click Add Cluster.
7. In Hypervisor, choose VMware.
8. Provide the following information in the dialog. The fields below make reference to values from vCenter.
  - » Cluster Name. Enter the name of the cluster you created in vCenter. For example, "cloud.cluster.2.2.1"
  - » vCenter Host. Enter the hostname or IP address of the vCenter server.
  - » vCenter Username. Enter the username that CloudStack should use to connect to vCenter. This user must have all administrative privileges.
  - » vCenter Password. Enter the password for the user named above
  - » vCenter Datacenter. Enter the vCenter datacenter that the cluster is in. For example, "cloud.dc.VM".

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

## 6.6. Adding a Host

1. Before adding a host to the CloudStack configuration, you must first install your chosen hypervisor on the host. CloudStack can manage hosts running VMs under a variety of hypervisors. The CloudStack Installation Guide provides instructions on how to install each supported hypervisor and configure it for use with CloudStack. See the appropriate section in the Installation Guide for information about which version of your chosen hypervisor is supported, as well as crucial additional steps to configure the hypervisor hosts for use with CloudStack.



### Atenção

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

2. Now add the hypervisor host to CloudStack. The technique to use varies depending on the hypervisor.

- ▶ [Seção 6.6.1, "Adding a Host \(XenServer or KVM\)"](#)
- ▶ [Seção 6.6.2, "Adding a Host \(vSphere\)"](#)

## 6.6.1. Adding a Host (XenServer or KVM)

XenServer and KVM hosts can be added to a cluster at any time.

### 6.6.1.1. Requirements for XenServer and KVM Hosts



#### Atenção

Make sure the hypervisor host does not have any VMs already running before you add it to CloudStack.

Configuration requirements:

- ▶ Each cluster must contain only hosts with the identical hypervisor.
- ▶ For XenServer, do not put more than 8 hosts in a cluster.
- ▶ For KVM, do not put more than 16 hosts in a cluster.

For hardware requirements, see the installation section for your hypervisor in the CloudStack Installation Guide.

#### 6.6.1.1.1. XenServer Host Additional Requirements

If network bonding is in use, the administrator must cable the new host identically to other hosts in the cluster.

For all additional hosts to be added to the cluster, run the following command. This will cause the host to join the master in a XenServer pool.

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



#### Nota

Ao copiar e colar um comando, certifique-se que o comando tenha colado como uma única linha antes de executar. Alguns viewers documento pode introduzir quebras de linha indesejadas no texto copiado.

With all hosts added to the XenServer pool, run the cloud-setup-bond script. This script will complete the configuration and setup of the bonds on the new hosts in the cluster.

1. Copy the script from the Management Server in `/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/cloud-setup-bonding.sh` to the master host and ensure it is executable.
2. Run the script:

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

#### 6.6.1.1.2. KVM Host Additional Requirements

- ▶ If shared mountpoint storage is in use, the administrator should ensure that the new host has all the same mountpoints (with storage mounted) as the other hosts in the cluster.
- ▶ Make sure the new host has the same network configuration (guest, private, and public network) as other hosts in the cluster.
- ▶ If you are using OpenVswitch bridges edit the file `agent.properties` on the KVM host and set the parameter `network.bridge.type` to `openvswitch` before adding the host to CloudStack

#### 6.6.1.2. Adding a XenServer or KVM Host

- ▶ If you have not already done so, install the hypervisor software on the host. You will need to know which version of the hypervisor software version is supported by CloudStack and what additional configuration is required to ensure the host will work with CloudStack. To find these installation details, see the appropriate section for your hypervisor in the CloudStack Installation Guide.
- ▶ Faça login na interface de usuário do CloudStack como administrador.
- ▶ In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone in which you want to add the host.
- ▶ Click the Compute tab. In the Clusters node, click View All.
- ▶ Click the cluster where you want to add the host.
- ▶ Click View Hosts.
- ▶ Click Add Host.
- ▶ Provide the following information.
  - Host Name. The DNS name or IP address of the host.
  - Username. Usually root.
  - Password. This is the password for the user from your XenServer or KVM install).
  - Host Tags (Optional). Any labels that you use to categorize hosts for ease of maintenance. For example, you can set to the cloud's HA tag (set in the `ha.tag` global configuration parameter) if you want this host to be used only for VMs with the "high availability" feature enabled. For more information, see HA-Enabled Virtual Machines as well as

HA for Hosts.

There may be a slight delay while the host is provisioned. It should automatically display in the UI.

- » Repeat for additional hosts.

## 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. Adicionar Storage Primário

### 6.7.1. System Requirements for Primary Storage

Hardware requirements:

- » Any standards-compliant iSCSI or NFS server that is supported by the underlying hypervisor.
- » The storage server should be a machine with a large number of disks. The disks should ideally be managed by a hardware RAID controller.
- » Minimum required capacity depends on your needs.

When setting up primary storage, follow these restrictions:

- » Primary storage cannot be added until a host has been added to the cluster.
- » If you do not provision shared primary storage, you must set the global configuration parameter `system.vm.local.storage.required` to true, or else you will not be able to start VMs.

### 6.7.2. Adding Primary Storage

When you create a new zone, the first primary storage is added as part of that procedure. You can add primary storage servers at any time, such as when adding a new cluster or adding more servers to an existing cluster.



#### Atenção

Be sure there is nothing stored on the server. Adding the server to CloudStack will destroy any existing data.

1. Log in to the CloudStack UI (see [Seção 5.1, "Login na interface de usuário"](#)).
2. In the left navigation, choose Infrastructure. In Zones, click View More, then click the zone in which you want to add the primary storage.
3. Click the Compute tab.
4. In the Primary Storage node of the diagram, click View All.
5. Click Add Primary Storage.
6. Provide the following information in the dialog. The information required varies depending on your choice in Protocol.
  - » **Pod.** The pod for the storage device.
  - » **Cluster.** The cluster for the storage device.
  - » **Name.** O nome do dispositivo do storage.
  - » **Protocol.** For XenServer, choose either NFS, iSCSI, or PreSetup. For KVM, choose NFS or SharedMountPoint. For vSphere choose either VMFS (iSCSI or FiberChannel) or NFS.
  - » **Server (for NFS, iSCSI, or PreSetup).** The IP address or DNS name of the storage device.
  - » **Server (for VMFS).** The IP address or DNS name of the vCenter server.
  - » **Path (for NFS).** In NFS this is the exported path from the server.
  - » **Path (for VMFS).** In vSphere this is a combination of the datacenter name and the datastore name. The format is `"/" datacenter name "/" datastore name`. For example, `"/cloud.dc.VM/cluster1datastore"`.
  - » **Path (for SharedMountPoint).** With KVM this is the path on each host that is where this primary storage is mounted. For example, `"/mnt/primary"`.
  - » **SR Name-Label (for PreSetup).** Enter the name-label of the SR that has been set up outside CloudStack.
  - » **Target IQN (for iSCSI).** In iSCSI this is the IQN of the target. For example, `iqn.1986-03.com.sun:02:01ec9bb549-1271378984`.
  - » **Lun # (for iSCSI).** In iSCSI this is the LUN number. For example, 3.
  - » **Tags (optional).** The comma-separated list of tags for this storage device. It should be an equivalent set or superset of the tags on your disk offerings..
7. Clique em OK.

## 6.8. Adicionar Storage Secundário

### 6.8.1. System Requirements for Secondary Storage

- » NFS storage appliance or Linux NFS server
- » (Optional) OpenStack Object Storage (Swift) (see <http://swift.openstack.org>)
- » 100GB minimum capacity



– 200GB minimum capacity

- ▶ A secondary storage device must be located in the same zone as the guest VMs it serves.
- ▶ Each Secondary Storage server must be available to all hosts in the zone.

## 6.8.2. Adding Secondary Storage

When you create a new zone, the first secondary storage is added as part of that procedure. You can add secondary storage servers at any time to add more servers to an existing zone.




### Atenção

Be sure there is nothing stored on the server. Adding the server to CloudStack will destroy any existing data.

1. If you are going to use Swift for cloud-wide secondary storage, you must add the Swift storage to CloudStack before you add the local zone secondary storage servers. See [Seção 6.3, "Adicionando uma zona"](#).
2. To prepare for local zone secondary storage, you should have created and mounted an NFS share during Management Server installation. See [Seção 4.5.6, "Preparar os compartilhamentos NFS"](#).
3. Make sure you prepared the system VM template during Management Server installation. See [Seção 4.5.8, "Prepare o template de máquina virtual de sistema"](#).
4. Now that the secondary storage server for per-zone storage is prepared, add it to CloudStack. Secondary storage is added as part of the procedure for adding a new zone. See [Seção 6.3, "Adicionando uma zona"](#).

## 6.9. Initialize and Test

After everything is configured, CloudStack will perform its initialization. This can take 30 minutes or more, depending on the speed of your network. When the initialization has completed successfully, the administrator's Dashboard should be displayed in the CloudStack UI.

1. Verify that the system is ready. In the left navigation bar, select Templates. Click on the CentOS 5.5 (64bit) no Gui (KVM) template. Check to be sure that the status is "Download Complete." Do not proceed to the next step until this status is displayed.
2. Go to the Instances tab, and filter by My Instances.
3. Click Add Instance and follow the steps in the wizard.
  - a. Choose the zone you just added.
  - b. In the template selection, choose the template to use in the VM. If this is a fresh installation, likely only the provided CentOS template is available.
  - c. Select a service offering. Be sure that the hardware you have allows starting the selected service offering.
  - d. In data disk offering, if desired, add another data disk. This is a second volume that will be available to but not mounted in the guest. For example, in Linux on XenServer you will see `/dev/xvdb` in the guest after rebooting the VM. A reboot is not required if you have a PV-enabled OS kernel in use.
  - e. In default network, choose the primary network for the guest. In a trial installation, you would have only one option here.
  - f. Optionally give your VM a name and a group. Use any descriptive text you would like.
  - g. Click Launch VM. Your VM will be created and started. It might take some time to download the template and complete the VM startup. You can watch the VM's progress in the Instances screen.
4. To use the VM, click the View Console button. 

For more information about using VMs, including instructions for how to allow incoming network traffic to the VM, start, stop, and delete VMs, and move a VM from one host to another, see Working With Virtual Machines in the Administrator's Guide.

Congratulations! You have successfully completed a CloudStack Installation.

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

# Capítulo 7. Global Configuration Parameters

## 7.1. Setting Global Configuration Parameters

### 7.2. About Global Configuration Parameters

## 7.1. Setting Global Configuration Parameters

CloudStack provides parameters that you can set to control many aspects of the cloud. When CloudStack is first installed, and periodically thereafter, you might need to modify these settings.

1. Log in to the UI as administrator.
2. Na barra de navegação à esquerda, clique em Global Settings.
3. In Select View, choose one of the following:
  - ▶ Global Settings. This displays a list of the parameters with brief descriptions and current values.

- Hypervisor Capabilities. This displays a list of hypervisor versions with the maximum number of guests supported for each.
4. Use the search box to narrow down the list to those you are interested in.
  5. Click the Edit icon to modify a value. If you are viewing Hypervisor Capabilities, you must click the name of the hypervisor first to display the editing screen.

## 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	Valor
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.  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 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.

# Capítulo 8. Instalação de hipervisor

## 8.1. Instalação de host hipervisor KVM

- 8.1.1. [Requerimentos de sistema para hosts hipervisores KVM](#)
- 8.1.2. [Visão geral da instalação do KVM](#)
- 8.1.3. [Preparando o sistema operacional](#)
- 8.1.4. [Install and configure the Agent](#)
- 8.1.5. [Install and Configure libvirt](#)
- 8.1.6. [Configure the Security Policies](#)
- 8.1.7. [Configure the network bridges](#)
- 8.1.8. [Configure the network using OpenVswitch](#)
- 8.1.9. [Configuring the firewall](#)
- 8.1.10. [Add the host to CloudStack](#)

## 8.2. Citrix XenServer Installation for CloudStack

- 8.2.1. [System Requirements for XenServer Hosts](#)
- 8.2.2. [XenServer Installation Steps](#)
- 8.2.3. [Configure XenServer dom0 Memory](#)
- 8.2.4. [Usuário e Senha.](#)
- 8.2.5. [Time Synchronization](#)
- 8.2.6. [Licensing](#)
- 8.2.7. [Install CloudStack XenServer Support Package \(CSP\)](#)
- 8.2.8. [Primary Storage Setup for XenServer](#)
- 8.2.9. [iSCSI Multipath Setup for XenServer \(Optional\)](#)
- 8.2.10. [Physical Networking Setup for XenServer](#)
- 8.2.11. [Upgrading XenServer Versions](#)

## 8.3. Instalação e configuração do VMware vSphere

- 8.3.1. [System Requirements for vSphere Hosts](#)
- 8.3.2. [Preparation Checklist for VMware](#)
- 8.3.3. [vSphere Installation Steps](#)
- 8.3.4. [ESXi Host setup](#)
- 8.3.5. [Physical Host Networking](#)
- 8.3.6. [Storage Preparation for vSphere \(iSCSI only\)](#)
- 8.3.7. [Add Hosts or Configure Clusters \(vSphere\)](#)
- 8.3.8. [Applying Hotfixes to a VMware vSphere Host](#)

## 8.1. Instalação de host hipervisor KVM

### 8.1.1. Requerimentos de sistema para hosts hipervisores KVM

O KVM é incluído em vários sistemas operacionais baseados no Linux. Embora você não seja obrigado a executar uma destas distribuições, as seguintes são recomendadas:

- » CentOS / RHEL: 6.3
- » Ubuntu: 12.04(.1)

O principal requerimento para hipervisores KVM é a versão de libvirt e de Qemu. Para qualquer distribuição Linux que esteja em uso, certifique-se de que os seguintes requerimentos são atendidos:

- » libvirt: 0.9.4 ou mais recente
- » Qemu/KVM: 1.0 ou mais recente

A `bridge default` no CloudStack é a implementação bridge nativa do Linux (`bridge module`). O CloudStack inclui uma opção para trabalhar com OpenVswitch, os requerimentos são listados abaixo

- » libvirt: 0.9.11 ou mais recente
- » openvswitch: 1.7.1 ou mais recente

Adicionalmente, os seguintes requerimentos de hardware se aplicam:

- » Em um cluster, os hosts devem ser da mesma versão da distribuição.
- » Todos os em um cluster devem ser homogêneos. As CPUs devem ser do mesmo tipo, número e mesmos recursos.
- » Deve suportar HVM (Intel-VT ou AMD-V habilitados).
- » CPU x86 64-bit (mais cores resultam em melhor performance)
- » 4 GB de memória

- ▶ No mínimo 1 NIC
- ▶ Quando você implementa o CloudStack, o host hipervisor não pode ter máquinas virtuais já ativas

### 8.1.2. Visão geral da instalação do KVM

Se você deseja usar o hipervisor Linux Kernel Virtual Machine (KVM) para executar máquinas virtuais hóspedes, instale o KVM nos host(s) em sua nuvem. O material nesta seção não duplica a documentação de instalação do KVM. São fornecidos os passos específicos para o CloudStack que são necessários para preparar um host KVM para trabalhar com o CloudStack.



#### Atenção

Antes de continuar, certifique-se de que você aplicou as mais recentes atualizações no seu host.



#### Atenção

NÃO é recomendado executar serviços neste host que não sejam controlados pelo CloudStack.

O procedimento para instalação de um host hipervisor KVM é:

1. Preparar o sistema operacional
2. Instalar e configurar o libvirt
3. Configurar as políticas de segurança (AppArmor e SELinux)
4. Instalar e configurar o agente

### 8.1.3. Preparando o sistema operacional

O sistema operacional do host deve ser preparado para hospedar o agente do CloudStack e executar instâncias do KVM.

1. Faça login no sistema operacional como root.
2. Verifique se o hostname é completamente qualificado.

```
$ hostname --fqdn
```

Isto deve retornar um hostname completamente qualificado tal como "kvm1.lab.example.org". Caso contrário, edite /etc/hosts para que isto aconteça.

3. Certifique-se de que a máquina tem acesso à Internet.

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

4. Ative NTP para sincronização de horário.



#### Nota

NTP é requerido para sincronizar os relógios dos servidores na nuvem. Relógios não sincronizados podem causar problemas inesperados.

- a. Instale o NTP

```
$ yum install ntp
```

```
$ apt-get install openntp
```

5. Repita todos estes passos em todos os host hipervisores.

### 8.1.4. Install and configure the Agent

To manage KVM instances on the host CloudStack uses a Agent. This Agent communicates with the Management server and controls all the instances on the host.

First we start by installing the agent:

No RHEL ou CentOS:

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

In Ubuntu:

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

The host is now ready to be added to a cluster. This is covered in a later section, see [Seção 6.6, "Adding a Host"](#). It is recommended that you continue to read the documentation before adding the host!

### 8.1.5. Install and Configure 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. In order to have live migration working libvirt has to listen for unsecured TCP connections. We also need to turn off

- in order to have the migration working, it needs to listen for unencrypted TCP connections. We also need to turn on libvirtds attempt to use Multicast DNS advertising. Both of these settings are in **/etc/libvirt/libvirtd.conf**  
Set the following parameters:

```
listen_tls = 0
```

```
listen_tcp = 1
```

```
tcp_port = "16509"
```

```
auth_tcp = "none"
```

```
mdns_adv = 0
```

- Turning on "listen\_tcp" in libvirtd.conf is not enough, we have to change the parameters as well:  
On RHEL or CentOS modify **/etc/sysconfig/libvirtd**:  
Uncomment the following line:

```
#LIBVIRT_ARGS="--listen"
```

On Ubuntu: modify **/etc/init/libvirt-bin.conf**

Change the following line (at the end of the file):

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

to (just add -l)

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

- Restart libvirt

No RHEL ou CentOS:

```
$ service libvirtd restart
```

In Ubuntu:

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

### 8.1.6. Configure the Security Policies

CloudStack does various things which can be blocked by security mechanisms like AppArmor and SELinux. These have to be disabled to ensure the Agent has all the required permissions.

- Configure SELinux (RHEL and CentOS)

- Check to see whether SELinux is installed on your machine. If not, you can skip this section.

In RHEL or CentOS, SELinux is installed and enabled by default. You can verify this with:

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

- Set the SELINUX variable in **/etc/selinux/config** to "permissive". This ensures that the permissive setting will be maintained after a system reboot.

No RHEL ou CentOS:

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

Change the following line

```
SELINUX=enforcing
```

to this

```
SELINUX=permissive
```

- Então configure SELinux como permissiva imediatamente, sem que um boot do sistema seja requerido.

```
$ setenforce permissive
```

- Configure Apparmor (Ubuntu)

- Check to see whether AppArmor is installed on your machine. If not, you can skip this section.

In Ubuntu AppArmor is installed and enabled by default. You can verify this with:

```
$ dpkg --get-selections | grep apparmor
```

- Disable the AppArmor profiles for libvirt

```
$ 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. Configure the network bridges



## Atenção

This is a very important section, please make sure you read this thoroughly.



## Nota

This section details how to configure bridges using the native implementation in Linux. Please refer to the next section if you intend to use OpenVswitch

In order to forward traffic to your instances you will need at least two bridges: *public* and *private*.

By default these bridges are called *cloudbr0* and *cloudbr1*, but you do have to make sure they are available on each hypervisor.

The most important factor is that you keep the configuration consistent on all your hypervisors.

### 8.1.7.1. Network example

There are many ways to configure your network. In the Basic networking mode you should have two (V)LAN's, one for your private network and one for the public network.

We assume that the hypervisor has one NIC (eth0) with three tagged VLAN's:

1. VLAN 100 for management of the hypervisor
2. VLAN 200 for public network of the instances (cloudbr0)
3. VLAN 300 for private network of the instances (cloudbr1)

On VLAN 100 we give the Hypervisor the IP-Address 192.168.42.11/24 with the gateway 192.168.42.1



## Nota

The Hypervisor and Management server don't have to be in the same subnet!

### 8.1.7.2. Configuring the network bridges

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



## Nota

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

#### 8.1.7.2.1. Configure in RHEL or CentOS

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

First we configure 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 now have to configure the three VLAN interfaces:

```
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

```

```
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
```

Now we have the VLAN interfaces configured we can add the bridges on top of them.

```
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
```

We do the same for cloudbr1

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

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

With this configuration you should be able to restart the network, although a reboot is recommended to see if everything works properly.



### Atenção

Make sure you have an alternative way like IPMI or ILO to reach the machine in case you made a configuration error and the network stops functioning!

#### 8.1.7.2.2. Configure in Ubuntu

All the required packages were installed when you installed libvirt, so we only have to configure the network.

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

Modify the interfaces file to look like this:

```
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
```

With this configuration you should be able to restart the network, although a reboot is recommended to see if everything

with this configuration you should be able to restart the network, although a reboot is recommended to see if everything works properly.



### Atenção

Make sure you have an alternative way like IPMI or ILO to reach the machine in case you made a configuration error and the network stops functioning!

## 8.1.8. Configure the network using OpenVswitch



### Atenção

This is a very important section, please make sure you read this thoroughly.

In order to forward traffic to your instances you will need at least two bridges: *public* and *private*.

By default these bridges are called *cloudbr0* and *cloudbr1*, but you do have to make sure they are available on each hypervisor.

The most important factor is that you keep the configuration consistent on all your hypervisors.

### 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. Network example

There are many ways to configure your network. In the Basic networking mode you should have two (V)LAN's, one for your private network and one for the public network.

We assume that the hypervisor has one NIC (`eth0`) with three tagged VLAN's:

1. VLAN 100 for management of the hypervisor
2. VLAN 200 for public network of the instances (`cloudbr0`)
3. VLAN 300 for private network of the instances (`cloudbr1`)

On VLAN 100 we give the Hypervisor the IP-Address `192.168.42.11/24` with the gateway `192.168.42.1`



### Nota

The Hypervisor and Management server don't have to be in the same subnet!

### 8.1.8.3. Configuring the network bridges

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



### Nota

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. Configure in RHEL or CentOS

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

First we configure `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
```

With this configuration you should be able to restart the network, although a reboot is recommended to see if everything works properly.



### Atenção

Make sure you have an alternative way like IPMI or ILO to reach the machine in case you made a configuration error and the network stops functioning!

## 8.1.9. Configuring the firewall

The hypervisor needs to be able to communicate with other hypervisors and the management server needs to be able to reach the hypervisor.

In order to do so we have to open the following TCP ports (if you are using a firewall):

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

It depends on the firewall you are using how to open these ports. Below you'll find examples how to open these ports in RHEL/CentOS and Ubuntu.

### 8.1.9.1. Open ports in RHEL/CentOS

RHEL and CentOS use iptables for firewalling the system, you can open extra ports by executing the following iptable commands:

```
$ 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
```

These iptable settings are not persistent across reboots, we have to save them first.

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

### 8.1.9.2. Open ports in Ubuntu

The default firewall under Ubuntu is UFW (Uncomplicated FireWall), which is a Python wrapper around iptables.

To open the required ports, execute the following commands:

```
$ 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
```



#### Nota

By default UFW is not enabled on Ubuntu. Executing these commands with the firewall disabled does not enable the firewall.

### 8.1.10. Add the host to CloudStack

The host is now ready to be added to a cluster. This is covered in a later section, see [Seção 6.6, "Adding a Host"](#). It is recommended that you continue to read the documentation before adding the host!

## 8.2. Citrix XenServer Installation for CloudStack

If you want to use the Citrix XenServer hypervisor to run guest virtual machines, install XenServer 6.1 or XenServer 6.0.2 on the host(s) in your cloud. For an initial installation, follow the steps below. If you have previously installed XenServer and want to upgrade to another version, see [Seção 8.2.11, "Upgrading XenServer Versions"](#).

### 8.2.1. System Requirements for XenServer Hosts

- ▶ The host must be certified as compatible with one of the following. See the Citrix Hardware Compatibility Guide: <http://hcl.xensource.com>
  - XenServer 5.6 SP2
  - XenServer 6.0
  - XenServer 6.0.2
- ▶ Você deve reinstalar o Citrix XenServer caso queira utilizar uma instalação anterior.
- ▶ Deve suportar HVM (Intel-VT ou AMD-V habilitados).
- ▶ Be sure all the hotfixes provided by the hypervisor vendor are applied. Track the release of hypervisor patches through your hypervisor vendor's support channel, and apply patches as soon as possible after they are released. CloudStack will not track or notify you of required hypervisor patches. It is essential that your hosts are completely up to date with the provided hypervisor patches. The hypervisor vendor is likely to refuse to support any system that is not up to date with patches.
- ▶ All hosts within a cluster must be homogeneous. The CPUs must be of the same type, count, and feature flags.
- ▶ Must support HVM (Intel-VT or AMD-V enabled in BIOS)
- ▶ CPU x86 64-bit (mais cores resultam em melhor performance)
- ▶ Suporte de virtualização de hardware requerido
- ▶ 4 GB de memória
- ▶ 36 GB de disco local
- ▶ No mínimo 1 NIC
- ▶ Endereço IP estaticamente assinalado
- ▶ Quando você implementa o CloudStack, o host hipervisor não pode ter máquinas virtuais já ativas



#### Atenção

A falta de hotfixes atualizadas pode levar a dados corrompidos e à perda de máquinas virtuais.

## 8.2.2. XenServer Installation Steps

1. From <https://www.citrix.com/English/ss/downloads/>, download the appropriate version of XenServer for your CloudStack version (see [Seção 8.2.1, "System Requirements for XenServer Hosts"](#)). Install it using the Citrix XenServer Installation Guide.



### Finding Older XenServer Releases

You can download the current release of XenServer through the "Free Trials" page, but if you wish to download older versions of XenServer, you will need a Citrix account and will have to browse through the download archives.

2. After installation, perform the following configuration steps, which are described in the next few sections:

Obrigatório	Opcional
<a href="#">Seção 8.2.3, "Configure XenServer dom0 Memory"</a>	<a href="#">Seção 8.2.7, "Install CloudStack XenServer Support Package (CSP)"</a>
<a href="#">Seção 8.2.4, "Usuário e Senha."</a>	Set up SR if not using NFS, iSCSI, or local disk; see <a href="#">Seção 8.2.8, "Primary Storage Setup for XenServer"</a>
<a href="#">Seção 8.2.5, "Time Synchronization"</a>	<a href="#">Seção 8.2.9, "iSCSI Multipath Setup for XenServer (Optional)"</a>
<a href="#">Seção 8.2.6.1, "Getting and Deploying a License"</a>	<a href="#">Seção 8.2.10, "Physical Networking Setup for XenServer"</a>

## 8.2.3. Configure XenServer dom0 Memory

Configure the XenServer dom0 settings to allocate more memory to dom0. This can enable XenServer to handle larger numbers of virtual machines. We recommend 2940 MB of RAM for XenServer dom0. For instructions on how to do this, see <http://support.citrix.com/article/CTX126531>. The article refers to XenServer 5.6, but the same information applies to XenServer 6.0.

## 8.2.4. Usuário e Senha.

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

## 8.2.5. Time Synchronization

The host must be set to use NTP. All hosts in a pod must have the same time.

1. Instale o NTP

```
# yum install ntp
```

2. Edite o arquivo de configuração do NTP para apontar para o seu servidor NTP.

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

Add one or more server lines in this file with the names of the NTP servers you want to use. For example:

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

3. Reinicie o cliente NTP.

```
# service ntpd restart
```

4. Certifique-se de que o NTP será iniciado novamente após um boot.

```
# chkconfig ntpd on
```

## 8.2.6. Licensing

Citrix XenServer Free version provides 30 days usage without a license. Following the 30 day trial, XenServer requires a free activation and license. You can choose to install a license now or skip this step. If you skip this step, you will need to install a license when you activate and license the XenServer.

### 8.2.6.1. Getting and Deploying a License

If you choose to install a license now you will need to use the XenCenter to activate and get a license.

1. In XenCenter, click Tools > License manager.
2. Select your XenServer and select Activate Free XenServer.
3. Request a license.

You can install the license with XenCenter or using the xe command line tool.

## 8.2.7. Install CloudStack XenServer Support Package (CSP)

(Optional)

To enable security groups, elastic load balancing, and elastic IP on XenServer, download and install the CloudStack XenServer Support Package (CSP). After installing XenServer, perform the following additional steps on each XenServer host

.....

1. Download the CSP software onto the XenServer host from one of the following links:

For XenServer 6.0.2:

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

For XenServer 5.6 SP2:

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

For XenServer 6.0:

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

2. Extract the file:

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

3. Run the following script:

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

4. If the XenServer host is part of a zone that uses basic networking, disable Open vSwitch (OVS):

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

Restart the host machine when prompted.

The XenServer host is now ready to be added to CloudStack.

### 8.2.8. Primary Storage Setup for XenServer

CloudStack natively supports NFS, iSCSI and local storage. If you are using one of these storage types, there is no need to create the XenServer Storage Repository ("SR").

If, however, you would like to use storage connected via some other technology, such as FiberChannel, you must set up the SR yourself. To do so, perform the following steps. If you have your hosts in a XenServer pool, perform the steps on the master node. If you are working with a single XenServer which is not part of a cluster, perform the steps on that XenServer.

1. Connect FiberChannel cable to all hosts in the cluster and to the FiberChannel storage host.
2. Rescan the SCSI bus. Either use the following command or use XenCenter to perform an HBA rescan.

```
# scsi-rescan
```

3. Repeat step 2 on every host.
4. Check to be sure you see the new SCSI disk.

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

The output should look like this, although the specific file name will be different (scsi-<scsiID>):

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

5. Repeat step 4 on every host.
6. On the storage server, run this command to get a unique ID for the new SR.

```
# uuidgen
```

The output should look like this, although the specific ID will be different:

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

7. Create the FiberChannel SR. In name-label, use the unique ID you just generated.

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

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

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

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

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

Make note of the values you will need when you add this storage to CloudStack later (see [Seção 6.7, "Adicionar Storage Primário"](#)). In the Add Primary Storage dialog, in Protocol, you will choose PreSetup. In SR Name-Label, you will enter the name-label you set earlier (in this example, e6849e96-86c3-4f2c-8fcc-350cc711be3d).

9. (Optional) If you want to enable multipath I/O on a FiberChannel SAN, refer to the documentation provided by the SAN vendor.

### 8.2.9. iSCSI Multipath Setup for XenServer (Optional)

When setting up the storage repository on a Citrix XenServer, you can enable multipath I/O, which uses redundant physical components to provide greater reliability in the connection between the server and the SAN. To enable multipathing, use a SAN solution that is supported for Citrix servers and follow the procedures in Citrix documentation. The following links provide a starting point:

- ▶ <http://support.citrix.com/article/CTX118791>
- ▶ <http://support.citrix.com/article/CTX125403>

You can also ask your SAN vendor for advice about setting up your Citrix repository for multipathing.

Make note of the values you will need when you add this storage to the CloudStack later (see [Seção 6.7, "Adicionar Storage Primário"](#)). In the Add Primary Storage dialog, in Protocol, you will choose PreSetup. In SR Name-Label, you will enter the same name used to create the SR.

If you encounter difficulty, address the support team for the SAN provided by your vendor. If they are not able to solve your issue, see [Contacting Support](#).

## 8.2.10. Physical Networking Setup for XenServer

Once XenServer has been installed, you may need to do some additional network configuration. At this point in the installation, you should have a plan for what NICs the host will have and what traffic each NIC will carry. The NICs should be cabled as necessary to implement your plan.

If you plan on using NIC bonding, the NICs on all hosts in the cluster must be cabled exactly the same. For example, if eth0 is in the private bond on one host in a cluster, then eth0 must be in the private bond on all hosts in the cluster.

The IP address assigned for the management network interface must be static. It can be set on the host itself or obtained via static DHCP.

CloudStack configures network traffic of various types to use different NICs or bonds on the XenServer host. You can control this process and provide input to the Management Server through the use of XenServer network name labels. The name labels are placed on physical interfaces or bonds and configured in CloudStack. In some simple cases the name labels are not required.

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

CloudStack supports the use of a second NIC (or bonded pair of NICs, described in [Seção 8.2.10.4, "NIC Bonding for XenServer \(Optional\)"](#)) for the public network. If bonding is not used, the public network can be on any NIC and can be on different NICs on the hosts in a cluster. For example, the public network can be on eth0 on node A and eth1 on node B. However, the XenServer name-label for the public network must be identical across all hosts. The following examples set the network label to "cloud-public". After the management server is installed and running you must configure it with the name of the chosen network label (e.g. "cloud-public"); this is discussed in [Seção 4.5, "Instalação do servidor de gerenciamento"](#).

If you are using two NICs bonded together to create a public network, see [Seção 8.2.10.4, "NIC Bonding for XenServer \(Optional\)"](#).

If you are using a single dedicated NIC to provide public network access, follow this procedure on each new host that is added to CloudStack before adding the host.

1. Run `xe network-list` and find the public network. This is usually attached to the NIC that is public. Once you find the network make note of its UUID. Call this <UUID-Public>.
2. Run the following command.

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

### 8.2.10.2. Configuring Multiple Guest Networks for XenServer (Optional)

CloudStack supports the use of multiple guest networks with the XenServer hypervisor. Each network is assigned a name-label in XenServer. For example, you might have two networks with the labels "cloud-guest" and "cloud-guest2". After the management server is installed and running, you must add the networks and use these labels so that CloudStack is aware of the networks.

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

1. Run `xe network-list` and find one of the guest networks. Once you find the network make note of its UUID. Call this <UUID-Guest>.
2. Run the following command, substituting your own name-label and uuid values.

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

3. Repeat these steps for each additional guest network, using a different name-label and uuid each time.

### 8.2.10.3. Separate Storage Network for XenServer (Optional)

You can optionally set up a separate storage network. This should be done first on the host, before implementing the bonding steps below. This can be done using one or two available NICs. With two NICs bonding may be done as above. It is the administrator's responsibility to set up a separate storage network.

Give the storage network a different name-label than what will be given for other networks.

For the separate storage network to work correctly, it must be the only interface that can ping the primary storage device's IP address. For example, if eth0 is the management network NIC, `ping -I eth0 <primary storage device IP>` must fail. In all deployments, secondary storage devices must be pingable from the management network NIC or bond. If a secondary storage device has been placed on the storage network, it must also be pingable via the storage network NIC or bond on the hosts as well.

You can set up two separate storage networks as well. For example, if you intend to implement iSCSI multipath, dedicate two non-bonded NICs to multipath. Each of the two networks needs a unique name-label.

If no bonding is done, the administrator must set up and name-label the separate storage network on all hosts (masters and slaves).

Here is an example to set up eth5 to access a storage network on 172.16.0.24.

```
# xe pif-list host-name-label='hostname' device=eth5
uuid(R0): ab0d3dd4-5744-8fae-9693-a022c7a3471d
device ( R0): 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 Bonding for XenServer (Optional)

XenServer supports Source Level Balancing (SLB) NIC bonding. Two NICs can be bonded together to carry public, private, and guest traffic, or some combination of these. Separate storage networks are also possible. Here are some example supported configurations:

- 2 NICs on private, 2 NICs on public, 2 NICs on storage
- 2 NICs on private, 1 NIC on public, storage uses management network
- 2 NICs on private, 2 NICs on public, storage uses management network
- 1 NIC for private, public, and storage

All NIC bonding is optional.

XenServer expects all nodes in a cluster will have the same network cabling and same bonds implemented. In an installation the master will be the first host that was added to the cluster and the slave hosts will be all subsequent hosts added to the cluster. The bonds present on the master set the expectation for hosts added to the cluster later. The procedure to set up bonds on the master and slaves are different, and are described below. There are several important implications of this:

- You must set bonds on the first host added to a cluster. Then you must use `xe` commands as below to establish the same bonds in the second and subsequent hosts added to a cluster.
- Slave hosts in a cluster must be cabled exactly the same as the master. For example, if `eth0` is in the private bond on the master, it must be in the management network for added slave hosts.

##### 8.2.10.4.1. Management Network Bonding

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

##### 8.2.10.4.2. Creating a Private Bond on the First Host in the Cluster

Use the following steps to create a bond in XenServer. These steps should be run on only the first host in a cluster. This example creates the cloud-private network with two physical NICs (`eth0` and `eth1`) bonded into it.

1. Find the physical NICs that you want to bond together.

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

These command shows the `eth0` and `eth1` NICs and their UUIDs. Substitute the `ethX` devices of your choice. Call the UUID's returned by the above command `slave1-UUID` and `slave2-UUID`.

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

**This label is important. CloudStack looks for a network by a name you configure. You must use the same name-label for all hosts in the cloud for the management network.**

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

Now you have a bonded pair that can be recognized by CloudStack as the management network.

##### 8.2.10.4.3. Public Network Bonding

Bonding can be implemented on a separate, public network. The administrator is responsible for creating a bond for the public network if that network will be bonded and will be separate from the management network.

##### 8.2.10.4.4. Creating a Public Bond on the First Host in the Cluster

These steps should be run on only the first host in a cluster. This example creates the cloud-public network with two physical NICs (`eth2` and `eth3`) bonded into it.

1. Find the physical NICs that you want to bond together.

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

These command shows the `eth2` and `eth3` NICs and their UUIDs. Substitute the `ethX` devices of your choice. Call the UUID's returned by the above command `slave1-UUID` and `slave2-UUID`.

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

**This label is important. CloudStack looks for a network by a name you configure. You must use the same name-label for all hosts in the cloud for the public network.**

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

Now you have a bonded pair that can be recognized by CloudStack as the public network.

#### 8.2.10.4.5. Adding More Hosts to the Cluster

With the bonds (if any) established on the master, you should add additional, slave hosts. Run the following command for all additional hosts to be added to the cluster. This will cause the host to join the master in a single XenServer pool.

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

#### 8.2.10.4.6. Complete the Bonding Setup Across the Cluster

With all hosts added to the pool, run the cloud-setup-bond script. This script will complete the configuration and set up of the bonds across all hosts in the cluster.

1. Copy the script from the Management Server in `/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/cloud-setup-bonding.sh` to the master host and ensure it is executable.
2. Run the script:

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

Now the bonds are set up and configured properly across the cluster.

### 8.2.11. Upgrading XenServer Versions

This section tells how to upgrade XenServer software on CloudStack hosts. The actual upgrade is described in XenServer documentation, but there are some additional steps you must perform before and after the upgrade.



#### Nota

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

To upgrade XenServer:

1. Upgrade the database. On the Management Server node:
  - a. Back up the database:

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

- b. You might need to change the OS type settings for VMs running on the upgraded hosts.
  - If you upgraded from XenServer 5.6 GA to XenServer 5.6 SP2, change any VMs that have the OS type CentOS 5.5 (32-bit), Oracle Enterprise Linux 5.5 (32-bit), or Red Hat Enterprise Linux 5.5 (32-bit) to Other Linux (32-bit). Change any VMs that have the 64-bit versions of these same OS types to Other Linux (64-bit).
  - If you upgraded from XenServer 5.6 SP2 to XenServer 6.0.2, change any VMs that have the OS type 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), or Red Hat Enterprise Linux 5.7 (32-bit) to Other Linux (32-bit). Change any VMs that have the 64-bit versions of these same OS types to Other Linux (64-bit).
  - If you upgraded from XenServer 5.6 to XenServer 6.0.2, do all of the above.
- c. Restart the Management Server and Usage Server. You only need to do this once for all clusters.

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

2. Disconnect the XenServer cluster from CloudStack.
  - a. Log in to the CloudStack UI as root.
  - b. Navigate to the XenServer cluster, and click Actions – Unmanage.
  - c. Watch the cluster status until it shows Unmanaged.
3. Log in to one of the hosts in the cluster, and run this command to clean up the VLAN:

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

4. Still logged in to the host, run the upgrade preparation script:

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

Troubleshooting: If you see the error "can't eject CD," log in to the VM and unmount the CD, then run the script again.

5. Upgrade the XenServer software on all hosts in the cluster. Upgrade the master first.
  - a. Live migrate all VMs on this host to other hosts. See the instructions for live migration in the Administrator's Guide.

Troubleshooting: You might see the following error when you migrate a VM:

```
[root@xenserver-qa-2-49-4 ~]# xe vm-migrate live=true host=xenserver-qa-2-49-5
vm=i-2-8-VM
You attempted an operation on a VM which requires
PV drivers to be installed but the drivers were not detected.
vm: b6cf79c8-02ee-050b-922f-49583d9f1a14 (i-2-8-VM)
```

To solve this issue, run the following:

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

- b. Reboot the host.
- c. Upgrade to the newer version of XenServer. Use the steps in XenServer documentation.
- d. After the upgrade is complete, copy the following files from the management server to this host, in the directory locations shown below:

Copy this Management Server file...	...to this location on the XenServer host
/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/xenserver60/NFSSR.py	/opt/xensource/sm/NFSSR.py
/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/setupxenserver.sh	/opt/xensource/bin/setupxenserver.sh
/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/make_migratable.sh	/opt/xensource/bin/make_migratable.sh
/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/cloud-clean-vlan.sh	/opt/xensource/bin/cloud-clean-vlan.sh

- e. Run the following script:

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

Troubleshooting: If you see the following error message, you can safely ignore it.

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

- f. Plug in the storage repositories (physical block devices) to the XenServer host:

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

Note: If you add a host to this XenServer pool, you need to migrate all VMs on this host to other hosts, and eject this host from XenServer pool.

6. Repeat these steps to upgrade every host in the cluster to the same version of XenServer.
7. Run the following command on one host in the XenServer cluster to clean up the host tags:

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

### Nota

Ao copiar e colar um comando, certifique-se que o comando tenha colado como uma única linha antes de executar. Alguns viewers documento pode introduzir quebras de linha indesejadas no texto copiado.

8. Reconnect the XenServer cluster to CloudStack.
  - a. Log in to the CloudStack UI as root.
  - b. Navigate to the XenServer cluster, and click Actions – Manage.
  - c. Watch the status to see that all the hosts come up.
9. After all hosts are up, run the following on one host in the cluster:

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

## 8.3. Instalação e configuração do VMware vSphere

If you want to use the VMware vSphere hypervisor to run guest virtual machines, install vSphere on the host(s) in your cloud.

### 8.3.1. System Requirements for vSphere Hosts

#### 8.3.1.1. Software requirements:

- ▶ vSphere and vCenter, both version 4.1 or 5.0.  
vSphere Standard is recommended. Note however that customers need to consider the CPU constraints in place with vSphere licensing. See [http://www.vmware.com/files/pdf/vsphere\\_pricing.pdf](http://www.vmware.com/files/pdf/vsphere_pricing.pdf) and discuss with your VMware sales representative.  
vCenter Server Standard is recommended.
- ▶ Be sure all the hotfixes provided by the hypervisor vendor are applied. Track the release of hypervisor patches through your hypervisor vendor's support channel, and apply patches as soon as possible after they are released. CloudStack will not track or notify you of required hypervisor patches. It is essential that your hosts are completely up to date with the provided hypervisor patches. The hypervisor vendor is likely to refuse to support any system that is not up to date with patches.



### Apply All Necessary Hotfixes

A falta de hotfixes atualizadas pode levar a dados corrompidos e à perda de máquinas virtuais.

#### 8.3.1.2. Hardware requirements:



- ▶ The host must be certified as compatible with vSphere. See the VMware Hardware Compatibility Guide at <http://www.vmware.com/resources/compatibility/search.php>.
- ▶ All hosts must be 64-bit and must support HVM (Intel-VT or AMD-V enabled).
- ▶ All hosts within a cluster must be homogenous. That means the CPUs must be of the same type, count, and feature flags.
- ▶ CPU x86 64-bit (mais cores resultam em melhor performance)
- ▶ Suporte de virtualização de hardware requerido
- ▶ 4 GB de memória
- ▶ 36 GB de disco local
- ▶ No mínimo 1 NIC
- ▶ Endereço IP estaticamente assinalado

### 8.3.1.3. vCenter Server requirements:

- ▶ Processor - 2 CPUs 2.0GHz or higher Intel or AMD x86 processors. Processor requirements may be higher if the database runs on the same machine.
- ▶ Memory - 3GB RAM. RAM requirements may be higher if your database runs on the same machine.
- ▶ Disk storage - 2GB. Disk requirements may be higher if your database runs on the same machine.
- ▶ Microsoft SQL Server 2005 Express disk requirements. The bundled database requires up to 2GB free disk space to decompress the installation archive.
- ▶ Networking - 1Gbit or 10Gbit.

For more information, see "vCenter Server and the vSphere Client Hardware Requirements" at [http://pubs.vmware.com/vsp40/wwhelp/wwhtml/js/html/wwhelp.htm#href=install/c\\_vc\\_hw.html](http://pubs.vmware.com/vsp40/wwhelp/wwhtml/js/html/wwhelp.htm#href=install/c_vc_hw.html).

### 8.3.1.4. Other requirements:

- ▶ VMware vCenter Standard Edition 4.1 or 5.0 must be installed and available to manage the vSphere hosts.
- ▶ vCenter must be configured to use the standard port 443 so that it can communicate with the CloudStack Management Server.
- ▶ You must re-install VMware ESXi if you are going to re-use a host from a previous install.
- ▶ CloudStack requires VMware vSphere 4.1 or 5.0. VMware vSphere 4.0 is not supported.
- ▶ All hosts must be 64-bit and must support HVM (Intel-VT or AMD-V enabled). All hosts within a cluster must be homogeneous. That means the CPUs must be of the same type, count, and feature flags.
- ▶ The CloudStack management network must not be configured as a separate virtual network. The CloudStack management network is the same as the vCenter management network, and will inherit its configuration. See [Seção 8.3.5.2, "Configure vCenter Management Network"](#).
- ▶ CloudStack requires ESXi. ESX is not supported.
- ▶ All resources used for CloudStack must be used for CloudStack only. CloudStack cannot share instance of ESXi or storage with other management consoles. Do not share the same storage volumes that will be used by CloudStack with a different set of ESXi servers that are not managed by CloudStack.
- ▶ Put all target ESXi hypervisors in a cluster in a separate Datacenter in vCenter.
- ▶ The cluster that will be managed by CloudStack should not contain any VMs. Do not run the management server, vCenter or any other VMs on the cluster that is designated for CloudStack use. Create a separate cluster for use of CloudStack and make sure that they are no VMs in this cluster.
- ▶ All the required VLANS must be trunked into all network switches that are connected to the ESXi hypervisor hosts. These would include the VLANS for Management, Storage, vMotion, and guest VLANS. The guest VLAN (used in Advanced Networking; see Network Setup) is a contiguous range of VLANS that will be managed by CloudStack.

## 8.3.2. Preparation Checklist for VMware

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

- ▶ Information listed in [Seção 8.3.2.1, "vCenter Checklist"](#)
- ▶ Information listed in [Seção 8.3.2.2, "Networking Checklist for VMware"](#)

### 8.3.2.1. vCenter Checklist

You will need the following information about vCenter.

vCenter Requirement	Valor	Notes
vCenter User		This user must have admin privileges.
vCenter User Password		Password for the above user.
vCenter Datacenter Name		Name of the datacenter.
vCenter Cluster Name		Name of the cluster.

### 8.3.2.2. Networking Checklist for VMware

You will need the following information about VLAN.

VLAN Information	Valor	Notes
ESXi VLAN		VLAN on which all your ESXi hypervisors reside.
ESXi VLAN IP Address		IP Address Range in the ESXi VLAN. One address per Virtual Router is

ESXi VLAN IP Gateway		used from this range.
ESXi VLAN Netmask		
Management Server VLAN		VLAN on which the CloudStack Management server is installed.
Public VLAN		VLAN for the Public Network.
Public VLAN Gateway		
Public VLAN Netmask		
Public VLAN IP Address Range		Range of Public IP Addresses available for CloudStack use. These addresses will be used for virtual router on CloudStack to route private traffic to external networks.
VLAN Range for Customer use		A contiguous range of non-routable VLANs. One VLAN will be assigned for each customer.

### 8.3.3. vSphere Installation Steps

1. If you haven't already, you'll need to download and purchase vSphere from the VMware Website (<https://www.vmware.com/tryvmware/index.php?p=vmware-vsphere&lp=1>) and install it by following the VMware vSphere Installation Guide.
2. Following installation, perform the following configuration, which are described in the next few sections:

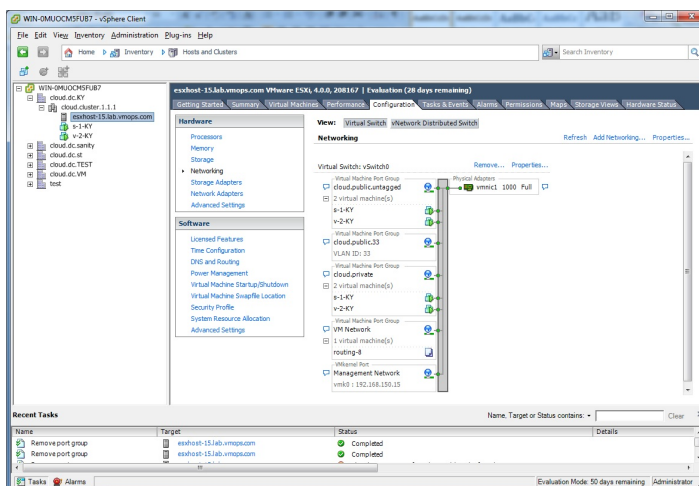
Obrigatório	Opcional
ESXi host setup	NIC bonding
Configure host physical networking, virtual switch, vCenter Management Network, and extended port range	Multipath storage
Prepare storage for iSCSI	
Configure clusters in vCenter and add hosts to them, or add hosts without clusters to vCenter	

### 8.3.4. ESXi Host setup

All ESXi hosts should enable CPU hardware virtualization support in BIOS. Please note hardware virtualization support is not enabled by default on most servers.

### 8.3.5. Physical Host Networking

You should have a plan for cabling the vSphere hosts. Proper network configuration is required before adding a vSphere host to CloudStack. To configure an ESXi host, you can use vClient to add it as standalone host to vCenter first. Once you see the host appearing in the vCenter inventory tree, click the host node in the inventory tree, and navigate to the Configuration tab.



In the host configuration tab, click the "Hardware/Networking" link to bring up the networking configuration page as above.

#### 8.3.5.1. Configure Virtual Switch

A default virtual switch vSwitch0 is created. CloudStack requires all ESXi hosts in the cloud to use the same set of virtual switch names. If you change the default virtual switch name, you will need to configure one or more CloudStack configuration variables as well.

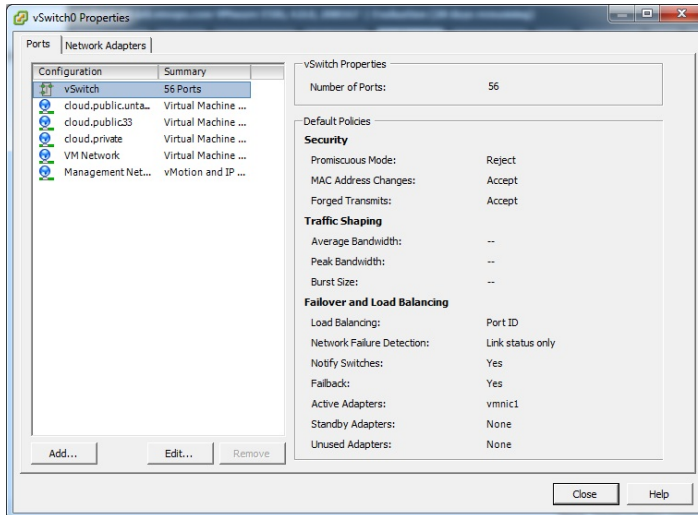
##### 8.3.5.1.1. Separating Traffic

CloudStack allows you to use vCenter to configure three separate networks per ESXi host. These networks are identified by the name of the vSwitch they are connected to. The allowed networks for configuration are public (for traffic to/from the public internet), guest (for guest-guest traffic), and private (for management and usually storage traffic). You can use the default virtual switch for all three, or create one or two other vSwitches for those traffic types.

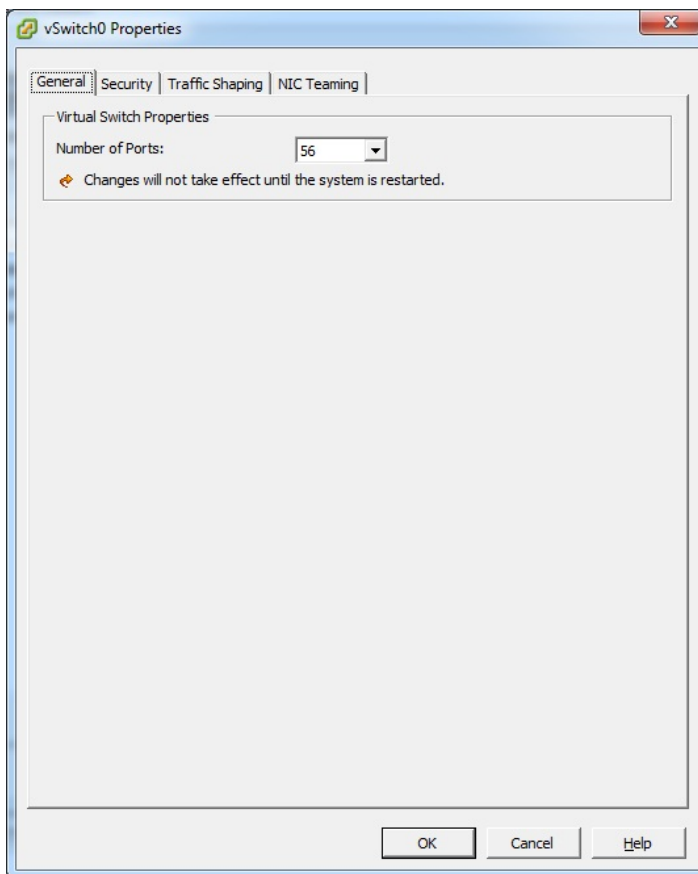
If you want to separate traffic in this way you should first create and configure vSwitches in vCenter according to the vCenter instructions. Take note of the vSwitch names you have used for each traffic type. You will configure CloudStack to use these vSwitches.

### 8.3.5.1.2. Increasing Ports

By default a virtual switch on ESXi hosts is created with 56 ports. We recommend setting it to 4088, the maximum number of ports allowed. To do that, click the "Properties..." link for virtual switch (note this is not the Properties link for Networking).



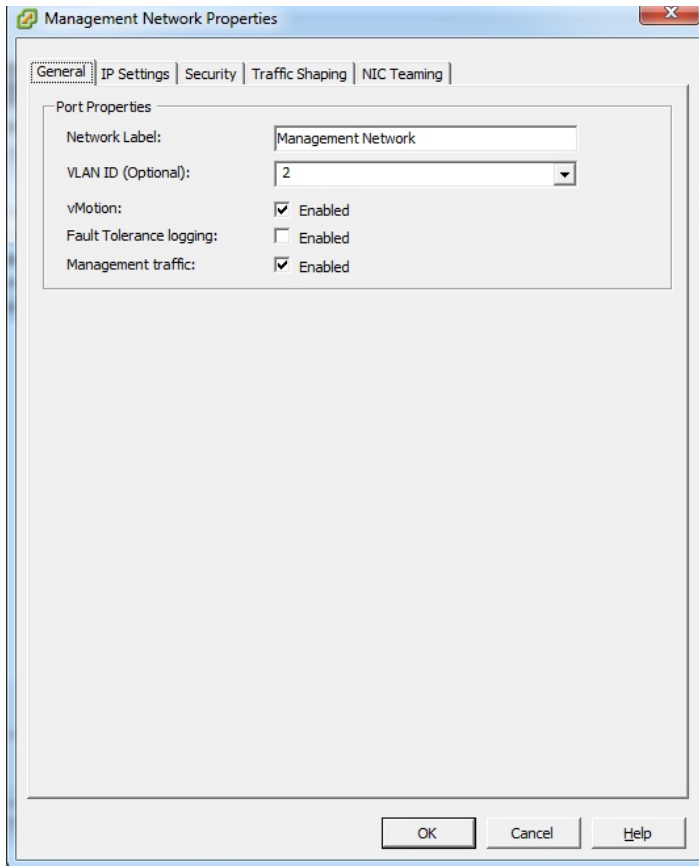
In vSwitch properties dialog, select the vSwitch and click Edit. You should see the following dialog:



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

### 8.3.5.2. Configure vCenter Management Network

In the vSwitch properties dialog box, you may see a vCenter management network. This same network will also be used as the CloudStack management network. CloudStack requires the vCenter management network to be configured properly. Select the management network item in the dialog, then click Edit.



Make sure the following values are set:

- » VLAN ID set to the desired ID
- » vMotion enabled.
- » Management traffic enabled.

If the ESXi hosts have multiple VMKernel ports, and ESXi is not using the default value "Management Network" as the management network name, you must follow these guidelines to configure the management network port group so that CloudStack can find it:

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

### 8.3.5.3. Extend Port Range for CloudStack Console Proxy

(Applies only to VMware vSphere version 4.x)

You need to extend the range of firewall ports that the console proxy works with on the hosts. This is to enable the console proxy to work with VMware-based VMs. The default additional port range is 59000-60000. To extend the port range, log in to the VMware ESX service console on each host and run the following commands:

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

### 8.3.5.4. Configure NIC Bonding for vSphere

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

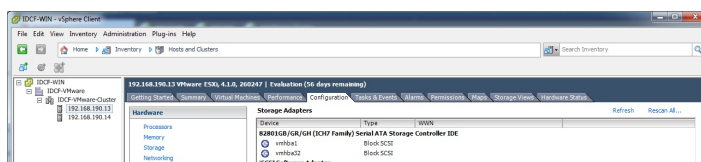
## 8.3.6. Storage Preparation for vSphere (iSCSI only)

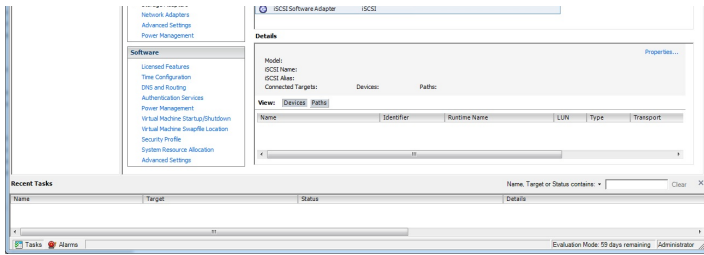
Use of iSCSI requires preparatory work in vCenter. You must add an iSCSI target and create an iSCSI datastore.

If you are using NFS, skip this section.

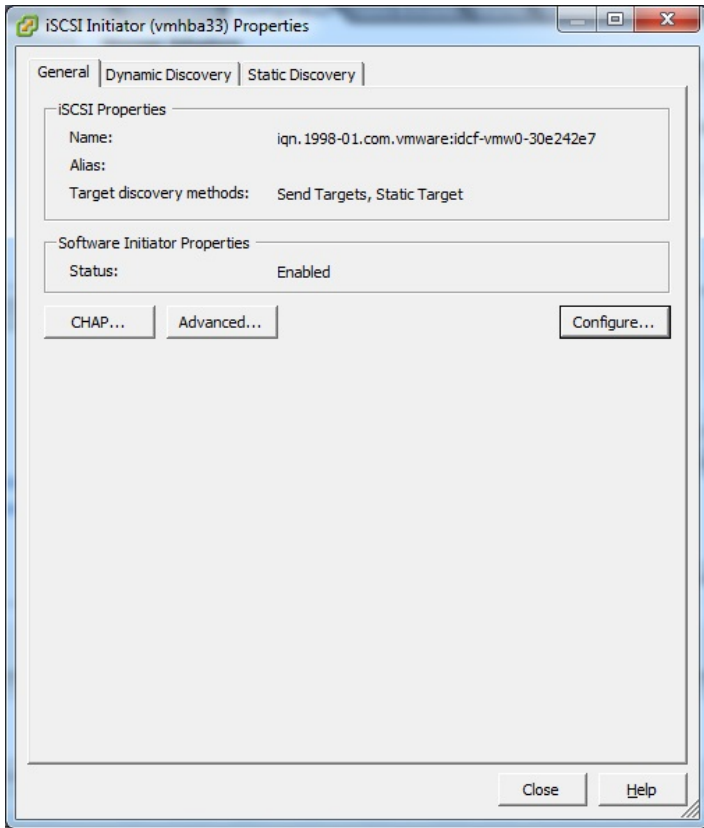
### 8.3.6.1. Enable iSCSI initiator for ESXi hosts

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

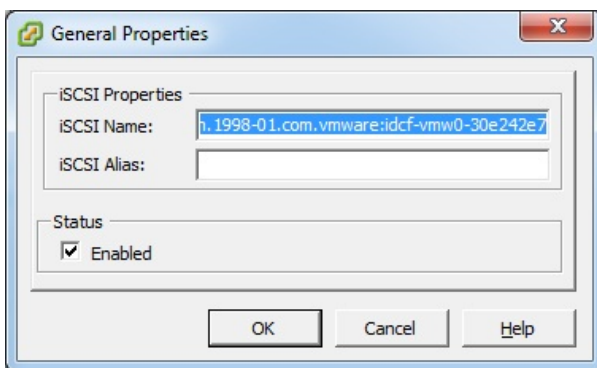




2. Select iSCSI software adaptor and click Properties.



3. Click the Configure... button.

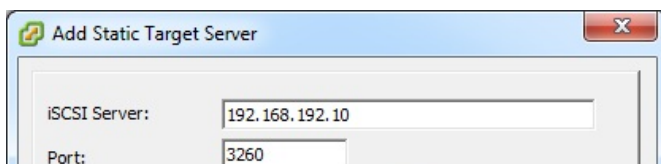


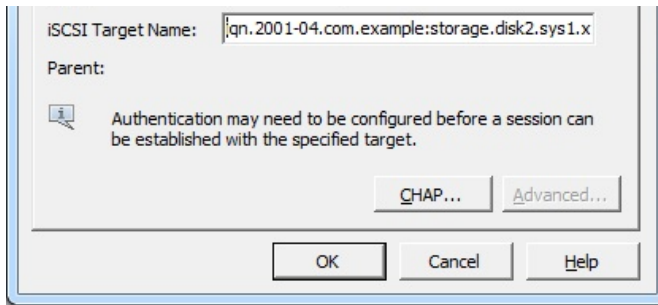
4. Check Enabled to enable the initiator.

5. Click OK to save.

### 8.3.6.2. Add iSCSI target

Under the properties dialog, add the iSCSI target info:





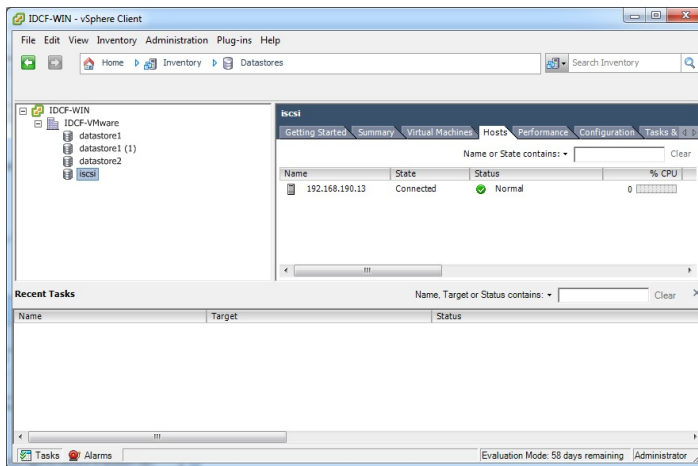
Repeat these steps for all ESXi hosts in the cluster.

### 8.3.6.3. Create an iSCSI datastore

You should now create a VMFS datastore. Follow these steps to do so:

1. Select Home/Inventory/Datastores.
2. Right click on the datacenter node.
3. Choose Add Datastore... command.
4. Follow the wizard to create a iSCSI datastore.

This procedure should be done on one host in the cluster. It is not necessary to do this on all hosts.



### 8.3.6.4. Multipathing for vSphere (Optional)

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

### 8.3.7. Add Hosts or Configure Clusters (vSphere)

Use vCenter to create a vCenter cluster and add your desired hosts to the cluster. You will later add the entire cluster to CloudStack. (see [Seção 6.5.2, "Add Cluster: vSphere"](#)).

### 8.3.8. Applying Hotfixes to a VMware vSphere Host

1. Disconnect the VMware vSphere cluster from CloudStack. It should remain disconnected long enough to apply the hotfix on the host.
  - a. Log in to the CloudStack UI as root.  
See [Seção 5.1, "Login na interface de usuário"](#).
  - b. Navigate to the VMware cluster, click Actions, and select Unmanage.
  - c. Watch the cluster status until it shows Unmanaged.
2. Perform the following on each of the ESXi hosts in the cluster:
  - a. Move each of the ESXi hosts in the cluster to maintenance mode.
  - b. Ensure that all the VMs are migrated to other hosts in that cluster.
  - c. If there is only one host in that cluster, shutdown all the VMs and move the host into maintenance mode.
  - d. Apply the patch on the ESXi host.
  - e. Restart the host if prompted.
  - f. Cancel the maintenance mode on the host.
3. Reconnect the cluster to CloudStack:
  - a. Log in to the CloudStack UI as root.
  - b. Navigate to the VMware cluster, click Actions, and select Manage.
  - c. Watch the status to see that all the hosts come up. It might take several minutes for the hosts to come up. Alternatively, verify the host state is properly synchronized and updated in the CloudStack database.

# Capítulo 9. Additional Installation Options

## 9.1. Installing the Usage Server (Optional)

### 9.1.1. Requirements for Installing the Usage Server

### 9.1.2. Steps to Install the Usage Server

## 9.2. SSL (Optional)

## 9.3. Database Replication (Optional)

### 9.3.1. Failover

The next few sections describe CloudStack features above and beyond the basic deployment options.

## 9.1. Installing the Usage Server (Optional)

You can optionally install the Usage Server once the Management Server is configured properly. The Usage Server takes data from the events in the system and enables usage-based billing for accounts.

When multiple Management Servers are present, the Usage Server may be installed on any number of them. The Usage Servers will coordinate usage processing. A site that is concerned about availability should install Usage Servers on at least two Management Servers.

### 9.1.1. Requirements for Installing the Usage Server

- The Management Server must be running when the Usage Server is installed.
- The Usage Server must be installed on the same server as a Management Server.

### 9.1.2. Steps to Install the Usage Server

1. Run `./install.sh`.

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

Você deve ver algumas mensagens enquanto o instalador se prepara, seguidas de uma lista de opções.

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

```
> S
```

3. Once installed, start the Usage Server with the following command.

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

The Administration Guide discusses further configuration of the Usage Server.

## 9.2. SSL (Optional)

CloudStack provides HTTP access in its default installation. There are a number of technologies and sites which choose to implement SSL. As a result, we have left CloudStack to expose HTTP under the assumption that a site will implement its typical practice.

CloudStack uses Tomcat as its servlet container. For sites that would like CloudStack to terminate the SSL session, Tomcat's SSL access may be enabled. Tomcat SSL configuration is described at <http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html>.

## 9.3. Database Replication (Optional)

CloudStack supports database replication from one MySQL node to another. This is achieved using standard MySQL replication. You may want to do this as insurance against MySQL server or storage loss. MySQL replication is implemented using a master/slave model. The master is the node that the Management Servers are configured to use. The slave is a standby node that receives all write operations from the master and applies them to a local, redundant copy of the database. The following steps are a guide to implementing MySQL replication.



### Nota

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

1. Ensure that this is a fresh install with no data in the master.
2. Edit `my.cnf` on the master and add the following in the `[mysqld]` section below `datadir`.

```
log_bin=mysql-bin
```

```
server_id=1
```

The `server_id` must be unique with respect to other servers. The recommended way to achieve this is to give the master an ID of 1 and each slave a sequential number greater than 1, so that the servers are numbered 1, 2, 3, etc.

- Restart the MySQL service. On RHEL/CentOS systems, use:

```
# service mysqld restart
```

On Debian/Ubuntu systems, use:

```
# service mysql restart
```

- Create a replication account on the master and give it privileges. We will use the "cloud-repl" user with the password "password". This assumes that master and slave run on the 172.16.1.0/24 network.

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

- Leave the current MySQL session running.
- In a new shell start a second MySQL session.
- Retrieve the current position of the database.

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

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

```
mysql> unlock tables;
```

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

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

- Edit `my.cnf` and add the following lines in the `[mysqld]` section below `datadir`.

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

- Restart MySQL. Use "mysqld" on RHEL/CentOS systems:

```
# service mysqld restart
```

On Ubuntu/Debian systems use "mysql."

```
# service mysql restart
```

- Instruct the slave to connect to and replicate from the master. Replace the IP address, password, log file, and position with the values you have used in the previous steps.

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

- Then start replication on the slave.

```
mysql> start slave;
```

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

This is not required for replication to work. But if you choose not to do this, you will need to do it when failover to the replica occurs.

### 9.3.1. Failover

This will provide for a replicated database that can be used to implement manual failover for the Management Servers. CloudStack failover from one MySQL instance to another is performed by the administrator. In the event of a database failure you should:

- Stop the Management Servers (via `service cloudstack-management stop`).
- Change the replica's configuration to be a master and restart it.
- Ensure that the replica's port 3306 is open to the Management Servers.
- Make a change so that the Management Server uses the new database. The simplest process here is to put the IP address of the new database server into each Management Server's `/etc/cloudstack/management/db.properties`.
- Restart the Management Servers:



# Capítulo 10. Selecionando a arquitetura de implementação

## 10.1. Implementação em pequena escala

### 10.2. Configuração redundante em larga escala

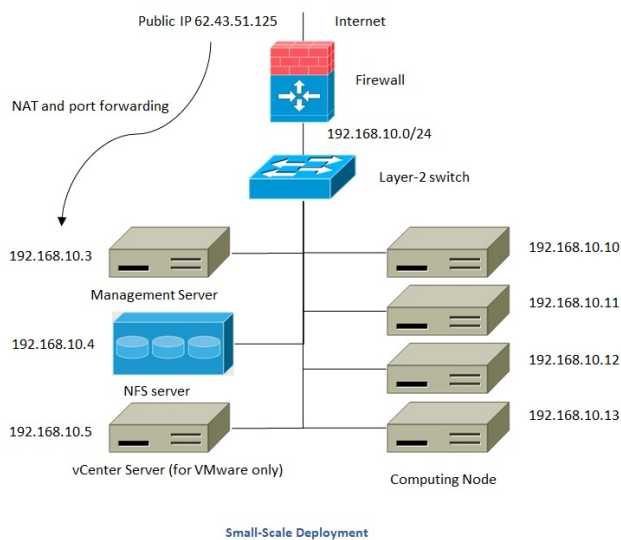
### 10.3. Rede dedicada de storage

### 10.4. Servidor multi-node de gerenciamento

### 10.5. Implementação multi-site

A arquitetura usada na implementação irá variar dependendo do tamanho e da finalidade da implementação. Esta seção contém exemplos de arquiteturas de implementação, incluindo uma implementação em pequena escala, útil para implementações de teste e avaliação, e uma configuração em larga escala totalmente redundante para implementações em ambiente de produção.

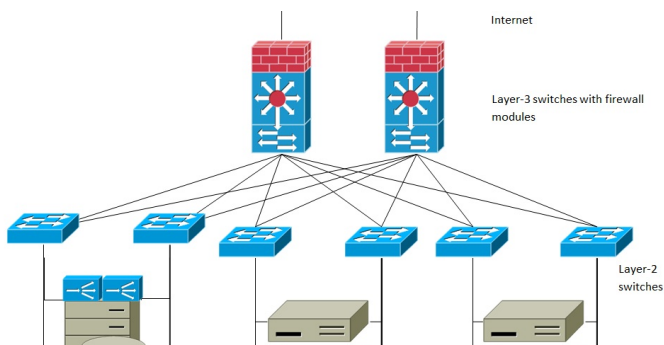
## 10.1. Implementação em pequena escala

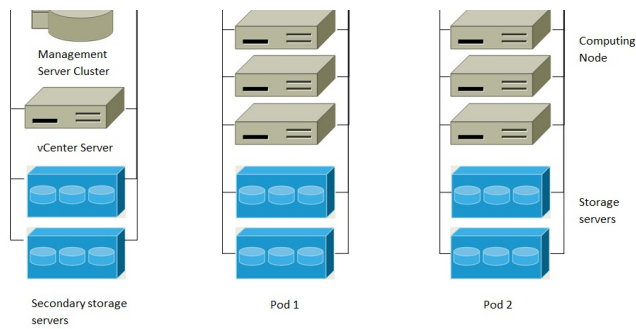


Este diagrama ilustra a arquitetura de rede de uma implementação em pequena escala do CloudStack.

- » Um firewall provê uma conexão à Internet. O firewall é configurado em modo NAT. O firewall encaminha requisições HTTP e chamadas API da Internet para o servidor de gerenciamento. O servidor de gerenciamento reside na rede de gerência.
- » Uma switch layer-2 conecta todos os servidores físicos e storage.
- » Um único servidor NFS provê tanto storage primária quanto storage secundária.
- » O servidor de gerenciamento é conectado à rede de gerência.

## 10.2. Configuração redundante em larga escala





Large-Scale Redundant Deployment

Este diagrama ilustra a arquitetura de rede de uma implementação redundante em larga escala do CloudStack.

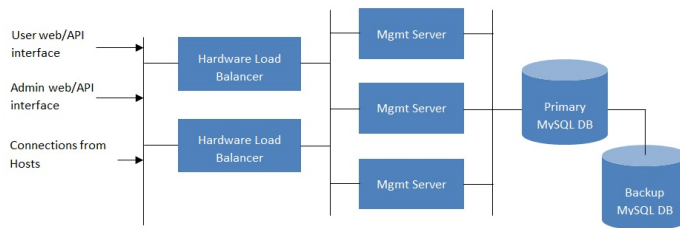
- ▶ Uma camada de comutação em layer-3 está no núcleo do data center. Um protocolo redundante de roteamento como VRRP deve ser implementado. Tipicamente, switches centrais de topo de linha também incluem módulos firewall. Aplicações de firewall distintas podem também ser usadas se a switches layer-3 não têm serviço de firewall integrado. Os firewalls são configurados em modo NAT. Os firewalls proveem as seguintes funções:
  - Encaminha requisições HTTP e chamadas API da Internet para o servidor de gerenciamento. O servidor de gerenciamento reside na rede de gerência.
  - Quando a nuvem se estende por múltiplas zonas, os firewalls devem habilitar VPNs entre sites, de forma que servidores em diferentes zonas possam conectar-se um ao outro diretamente.
- ▶ Um acesso em switch layer-2 é estabelecido para cada pod. Múltiplas switches podem ser empilhadas para aumentar o número de portas. Em qualquer caso, pares redundantes de switches layer-2 devem ser implementados.
- ▶ O cluster do servidor de gerenciamento (incluindo os balanceadores de carga front-end, nós servidores de gerenciamento, e o database MySQL) é conectado à rede de gerência através de um par de balanceadores de carga.
- ▶ Servidores de storage secundária são conectados à rede de gerência.
- ▶ Cada pod contém servidores de storage e de computação. Cada servidor de storage e computação deve ter NICs redundantes conectadas a switches layer-2 de acesso distintas.

### 10.3. Rede dedicada de storage

Na configuração redundante em larga escala descrita na seção anterior, tráfego de storage pode sobrecarregar a rede de gerência. Uma rede dedicada de storage é opcional para implementações. Protocolos de storage, tal como iSCSI, são sensíveis a atrasos na rede. Uma rede dedicada de storage garante que o tráfego de rede de hóspedes não comprometam a performance de storage.

### 10.4. Servidor multi-nó de gerenciamento

O servidor de gerenciamento do CloudStack é implementado em um mais servidores front-end conectados a um único database MySQL. Opcionalmente, um par de balanceadores de carga distribui requisições da web. Um servidor de gerenciamento backup pode ser implementado utilizando a replicação de MySQL em um site remoto para adicionar capacidade de recuperação de desastres.



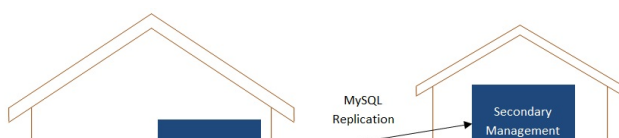
Multi-Node Management Server Deployment

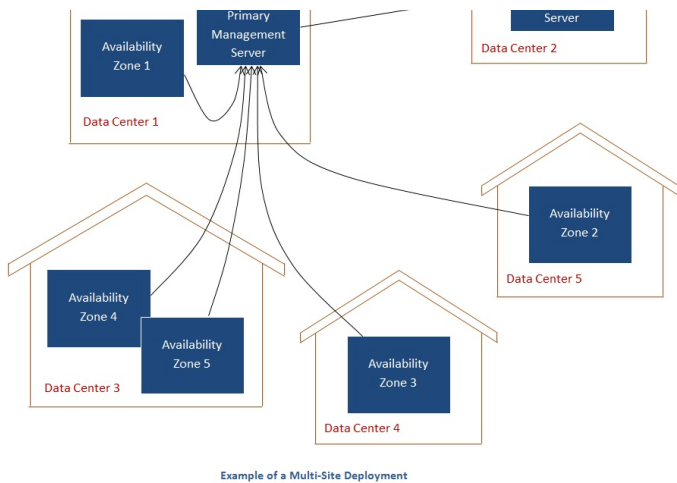
O administrador deve decidir o seguinte:

- ▶ Se balanceadores de carga serão utilizados ou não.
- ▶ Quantos servidores de gerenciamento serão implementados.
- ▶ Se replicação de MySQL será implementada para habilitar recuperação de desastres.

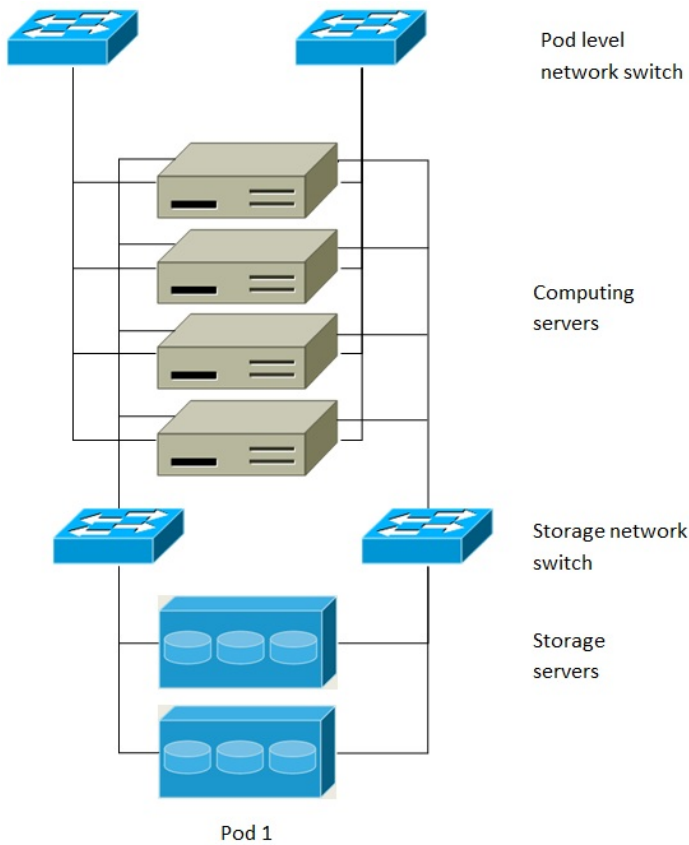
### 10.5. Implementação multi-site

A plataforma do CloudStack é bastante escalável em múltiplos sites através do uso de zonas. O diagrama a seguir mostra um exemplo de implementação multi-site.





Data Center 1 abriga o servidor primário de gerenciamento, assim como a zona 1. O database MySQL é replicado em tempo real no servidor secundário de gerenciamento no Data Center 2.



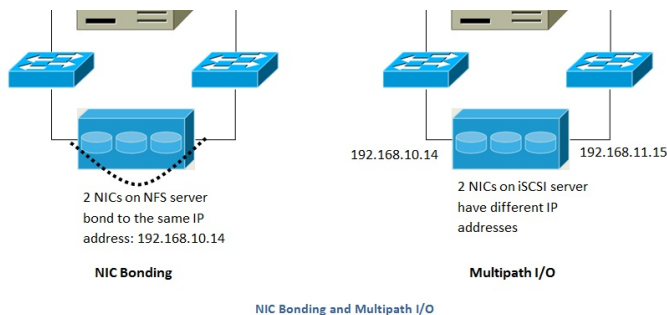
### Separate Storage Network

Este diagrama ilustra uma configuração com uma rede dedicada de storage. Cada servidor tem quatro NICs, dois conectados às switches da rede do pod e dois conectados às switches da rede de storage.

Há dois modos de configurar a rede de storage:

- » NICs acopladas e switches redundantes podem ser implementadas para NFS. Em implementações NFS, switches redundantes e NICs acopladas ainda resultam em uma rede (um bloco CIDR + endereço de default gateway).
- » iSCSI pode tirar vantagem de duas redes distintas de storage (dois blocos CIDR, cada um com seu próprio default gateway). Um cliente Multipath iSCSI chavear automaticamente e balancear a carga entre duas redes storage distintas.





Este diagrama ilustra as diferenças entre acoplamento de NICs e Multipath I/O (MPIO). A configuração de acoplamento de NICs envolve somente uma rede. MPIO envolve duas redes distintas.

# Capítulo 11. Amazon Web Services Compatible Interface

## 11.1. Amazon Web Services Compatible Interface

### 11.2. Supported API Version

### 11.3. Enabling the EC2 and S3 Compatible Interface

- 11.3.1. Enabling the Services
- 11.3.2. Creating EC2 Compatible Service Offerings
- 11.3.3. Modifying the AWS API Port

### 11.4. AWS API User Setup

- 11.4.1. AWS API User Registration
- 11.4.2. AWS API Command-Line Tools Setup

### 11.5. Using Timeouts to Ensure AWS API Command Completion

### 11.6. Supported AWS API Calls

### 11.7. Examples

- 11.7.1. Boto Examples
- 11.7.2. JClouds Examples

## 11.1. Amazon Web Services Compatible Interface

CloudStack can translate Amazon Web Services (AWS) API calls to native CloudStack API calls so that users can continue using existing AWS-compatible tools. This translation service runs as a separate web application in the same tomcat server as the management server of CloudStack, listening on a different port. The Amazon Web Services (AWS) compatible interface provides the EC2 SOAP and Query APIs as well as the S3 REST API.



### Nota

This service was previously enabled by separate software called CloudBridge. It is now fully integrated with the CloudStack management server.



### Atenção

The compatible interface for the EC2 Query API and the S3 API are Work In Progress. The S3 compatible API offers a way to store data on the management server file system, it is not an implementation of the S3 backend.

#### Limitations

- » Supported only in zones that use basic networking.
- » Available in fresh installations of CloudStack. Not available through upgrade of previous versions.
- » 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. Supported API Version

- ▶ The EC2 interface complies with Amazon's WDSL version dated November 15, 2010, available at <http://ec2.amazonaws.com/doc/2010-11-15/>.
- ▶ The interface is compatible with the EC2 command-line tools *EC2 tools* v. 1.3.6230, which can be downloaded at <http://s3.amazonaws.com/ec2-downloads/ec2-api-tools-1.3-62308.zip>.

**Nota**

Work is underway to support a more recent version of the EC2 API

## 11.3. Enabling the EC2 and S3 Compatible Interface

The software that provides AWS API compatibility is installed along with CloudStack. You must enable the services and perform some setup steps prior to using it.

1. Set the global configuration parameters for each service to true. See [Capítulo 7, Global Configuration Parameters](#).
2. Create a set of CloudStack service offerings with names that match the Amazon service offerings. You can do this through the CloudStack UI as described in the Administration Guide.



### Atenção

Be sure you have included the Amazon default service offering, `m1.small`. As well as any EC2 instance types that you will use.

3. If you did not already do so when you set the configuration parameter in step 1, restart the Management Server.

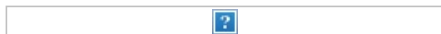
```
# service cloudstack-management restart
```

The following sections provides details to perform these steps

### 11.3.1. Enabling the Services

To enable the EC2 and S3 compatible services you need to set the configuration variables `enable.ec2.api` and `enable.s3.api` to true. You do not have to enable both at the same time. Enable the ones you need. This can be done via the CloudStack GUI by going in *Global Settings* or via the API.

The snapshot below shows you how to use the GUI to enable these services



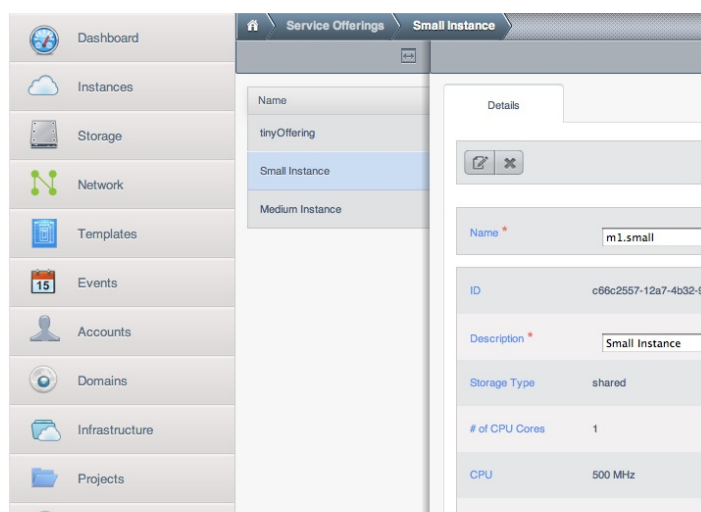
Using the CloudStack API, the easiest is to use the so-called integration port on which you can make unauthenticated calls. In *Global Settings* set the port to 8096 and subsequently call the `updateConfiguration` method. The following urls shows you how:

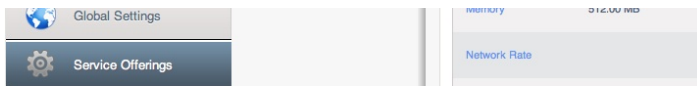
```
http://localhost:8096/client/api?
command=updateConfiguration&name=enable.ec2.api&value=true
http://localhost:8096/client/api?
command=updateConfiguration&name=enable.ec2.api&value=true
```

Once you have enabled the services, restart the server.

### 11.3.2. Creating EC2 Compatible Service Offerings

You will also need to define compute service offerings with names compatible with the [Amazon EC2 instance types](#) API names (e.g `m1.small`, `m1.large`). This can be done via the CloudStack GUI. Go under *Service Offerings* select *Compute offering* and either create a new compute offering or modify an existing one, ensuring that the name matches an EC2 instance type API name. The snapshot below shows you how:





### 11.3.3. Modifying the AWS API Port

#### Nota

(Optional) The AWS API listens for requests on port 7080. If you prefer AWS API to listen on another port, you can change it as follows:

- Edit the files `/etc/cloudstack/management/server.xml`, `/etc/cloudstack/management/server-nonssl.xml`, and `/etc/cloudstack/management/server-ssl.xml`.
- In each file, find the tag `<Service name="Catalina7080">`. Under this tag, locate `<Connector executor="tomcatThreadPool-internal" port= ....>`.
- Change the port to whatever port you want to use, then save the files.
- Reinicie o servidor de gerenciamento.

If you re-install CloudStack, you will have to re-enable the services and if need be update the port.

## 11.4. AWS API User Setup

In general, users need not be aware that they are using a translation service provided by CloudStack. They only need to send AWS API calls to CloudStack's endpoint, and it will translate the calls to the native CloudStack API. Users of the Amazon EC2 compatible interface will be able to keep their existing EC2 tools and scripts and use them with their CloudStack deployment, by specifying the endpoint of the management server and using the proper user credentials. In order to do this, each user must perform the following configuration steps:

- Generate user credentials.
- Register with the service.
- For convenience, set up environment variables for the EC2 SOAP command-line tools.

### 11.4.1. AWS API User Registration

Each user must perform a one-time registration. The user follows these steps:

- Obtain the following by looking in the CloudStack UI, using the API, or asking the cloud administrator:
  - The CloudStack server's publicly available DNS name or IP address
  - The user account's Access key and Secret key
- Generate a private key and a self-signed X.509 certificate. The user substitutes their own desired storage location for `/path/to/...` below.

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

- Register the user X.509 certificate and Access/Secret keys with the AWS compatible service. If you have the source code of CloudStack go to the `awsapi-setup/setup` directory and use the Python script `cloudstack-aws-api-register`. If you do not have the source then download the script using the following command.

```
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"
```

Then execute it, using the access and secret keys that were obtained in step 1. An example is shown below.

```
$ 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
```

#### Nota

A user with an existing AWS certificate could choose to use the same certificate with CloudStack, but note that the certificate would be uploaded to the CloudStack management server database.

### 11.4.2. AWS API Command-Line Tools Setup

To use the EC2 command-line tools, the user must perform these steps:

- Be sure you have the right version of EC2 Tools. The supported version is available at <http://s3.amazonaws.com/ec2-downloads/ec2-api-tools-1.3-62308.zip>.
- Set up the EC2 environment variables. This can be done every time you use the service or you can set them up in the proper shell profile. Replace the endpoint (i.e EC2\_URL) with the proper address of your CloudStack management server and port. In a bash shell do the following.

```
$ 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. Using Timeouts to Ensure AWS API Command Completion

The Amazon EC2 command-line tools have a default connection timeout. When used with CloudStack, a longer timeout might be needed for some commands. If you find that commands are not completing due to timeouts, you can specify a custom timeout. You can add the following optional command-line parameters to any CloudStack-supported EC2 command:

<code>--connection-timeout <i>TIMEOUT</i></code>	Specifies a connection timeout (in seconds). Example: <code>--connection-timeout 30</code>
<code>--request-timeout <i>TIMEOUT</i></code>	Specifies a request timeout (in seconds). Example: <code>--request-timeout 45</code>

Example:

```
ec2-run-instances 2 -z us-test1 -n 1-3 --connection-timeout 120 --request-timeout 120
```



### Nota

The timeouts optional arguments are not specific to CloudStack.

## 11.6. Supported AWS API Calls

The following Amazon EC2 commands are supported by CloudStack when the AWS API compatible interface is enabled. For a few commands, there are differences between the CloudStack and Amazon EC2 versions, and these differences are noted. The underlying SOAP call for each command is also given, for those who have built tools using those calls.

Tabela 11.1. Elastic IP API mapping

EC2 command	SOAP call	CloudStack API call
ec2-allocate-address	AllocateAddress	associateIpAddress
ec2-associate-address	AssociateAddress	enableStaticNat
ec2-describe-addresses	DescribeAddresses	listPublicIpAddresses
ec2-disassociate-address	DisassociateAddress	disableStaticNat
ec2-release-address	ReleaseAddress	disassociateIpAddress

Tabela 11.2. Availability Zone API mapping

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

Tabela 11.3. Images API mapping

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

Tabela 11.4. Image Attributes API mapping

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

Tabela 11.5. Instances API mapping

EC2 command	SOAP call	CloudStack API call
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

Tabela 11.6. Instance Attributes Mapping

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

Tabela 11.7. Keys Pairs Mapping

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

Tabela 11.8. Passwords API Mapping

EC2 command	SOAP call	CloudStack API call
ec2-get-password	GetPasswordData	getVMPasswd

Tabela 11.9. Security Groups API Mapping

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

Tabela 11.10. Snapshots API Mapping

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

Tabela 11.11. Volumes API Mapping

EC2 command	SOAP call	CloudStack API call
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. Examples

There are many tools available to interface with a AWS compatible API. In this section we provide a few examples that users of CloudStack can build upon.

### 11.7.1. Boto Examples

Boto is one of them. It is a Python package available at <https://github.com/boto/boto>. In this section we provide two examples of Python scripts that use Boto and have been tested with the CloudStack AWS API Interface.

First is an EC2 example. Replace the Access and Secret Keys with your own and update the endpoint.

Exemplo 11.1. An EC2 Boto example

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

import sys
import os
import boto
import boto.ec2

region = boto.ec2.regioninfo.RegionInfo(name="R00T", endpoint="localhost")
apikey='GwNnpUPr06KgIdZu01z_ZhhZnKjtSdRwuYd4DvpzvFpyxGMvrzno2q05MB0ViBoFYtdqKd'
secretkey='t4eXLEYWw7chBhd1aKf38adCMShx_wlds6JfSx3z9fSpS0m0AbP9Moj0oGIzy2LSC8iw'

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()
```

Second is an S3 example. Replace the Access and Secret keys with your own, as well as the endpoint of the service. Be sure to also update the file paths to something that exists on your machine.

Exemplo 11.2. An S3 Boto Example

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

import svs
```



```

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

apikey='Ch0w-pwdcCFy6fpeyv6kUaR0NnhzmG3tE7HLN2z30B_s-ogF5HjZtN4rnzKnq2UjtnHeg_yLA5g0w'
secretkey='IMY8R7CJQisGFk4cHwfXXN3DUFXz07cCiU80eM3McmfLs7kusgy0fm0g9qzXRXhoAPCH-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 Examples

# Capítulo 12. Configuração de rede

## 12.1. Rede básica e avançada

## 12.2. VLAN Allocation Example

## 12.3. Example Hardware Configuration

### 12.3.1. Dell 62xx

### 12.3.2. Cisco 3750

## 12.4. Layer-2 Switch

### 12.4.1. Dell 62xx

### 12.4.2. Cisco 3750

## 12.5. Hardware Firewall

### 12.5.1. Generic Firewall Provisions

### 12.5.2. External Guest Firewall Integration for Juniper SRX (Optional)

### 12.5.3. External Guest Load Balancer Integration (Optional)

## 12.6. Management Server Load Balancing

## 12.7. Topology Requirements

### 12.7.1. Security Requirements

### 12.7.2. Runtime Internal Communications Requirements

### 12.7.3. Storage Network Topology Requirements

- [12.7.4. External Firewall Topology Requirements](#)
- [12.7.5. Advanced Zone Topology Requirements](#)
- [12.7.6. XenServer Topology Requirements](#)
- [12.7.7. VMware Topology Requirements](#)
- [12.7.8. KVM Topology Requirements](#)

## 12.8. Guest Network Usage Integration for Traffic Sentinel

## 12.9. Setting Zone VLAN and Running VM Maximums

Alcançar a correta configuração de rede é crucial para uma instalação do CloudStack com sucesso. Esta seção contém informações para ajudá-lo a tomar decisões e adotar os procedimentos corretos para configurar corretamente sua rede.

## 12.1. Rede básica e avançada

O CloudStack provê dois estilos de rede:

### Básico

Para redes no estilo AWS. Provê uma única rede onde o isolamento de hóspedes pode ser implantado através de métodos da camada 3 tais como grupos de segurança (filtragem do endereço IP de origem).

### Avançado

Para topologias de rede mais sofisticadas. Este modelo de rede provê a maior flexibilidade ao definir redes hóspedes, mas requer mais passos de configuração que a rede básica.

Cada zona tem ou rede básica ou rede avançada. Uma vez que a escolha do modelo de rede para uma zona foi feita e configurada no CloudStack, ela não pode ser alterada. Uma zona ou é básica ou avançada por toda sua vida.

A tabela seguinte compara os recursos de rede dos dois modelos de rede.

Recurso de rede	Rede básica	Rede avançada
Número de redes	Rede única	Redes múltiplas
Tipo de firewall	Físico	Físico e virtual
Balanceador de carga	Físico	Físico e virtual
Tipo de isolamento	Camada 3	Camada 2 e camada 3
Suporte a VPN	Não	Sim
Encaminhamento de porta	Físico	Físico e virtual
NAT 1:1	Físico	Físico e virtual
NAT de origem	Não	Físico e virtual
Userdata	Sim	Sim
Monitoração da utilização de rede	sFlow / netFlow no roteador físico	Hipervisor e roteador virtual
DNS e DHCP	Sim	Sim

Os dois tipos de rede podem estar em uso na mesma nuvem. Entretanto, uma determinada zona deve usar ou rede básica ou rede avançada.

Diferentes tipos de tráfego de rede podem ser segmentados na mesma rede física. Tráfego hóspede pode também ser segmentado por conta. Para isolar tráfego, você pode usar VLANs separadas. Se você está usando VLANs separadas em uma única rede física, certifique-se de que as tags VLAN estão em intervalos numéricos distintos.

## 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.
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. Example Hardware Configuration

This section contains an example configuration of specific switch models for zone-level layer-3 switching. It assumes VLAN management protocols, such as VTP or GVRP, have been disabled. The example scripts must be changed appropriately if you choose to use VTP or GVRP.

### 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. Configure all the VLANs in the database.

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

2. Configure Ethernet port 1/g1.

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

The statements configure Ethernet port 1/g1 as follows:

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

### 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. Setting VTP mode to transparent allows us to utilize VLAN IDs above 1000. Since we only use VLANs up to 999, vtp transparent mode is not strictly required.

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

2. Configure GigabitEthernet1/0/1.

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

The statements configure GigabitEthernet1/0/1 as follows:

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

## 12.4. Layer-2 Switch

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

- ▶ It should trunk all VLANs into every computing host.
- ▶ It should switch traffic for the management network containing computing and storage hosts. The layer-3 switch will serve as the gateway for the management network.

### Example Configurations

This section contains example configurations for specific switch models for pod-level layer-2 switching. It assumes VLAN management protocols such as VTP or GVRP have been disabled. The scripts must be changed appropriately if you choose to use VTP or GVRP.

#### 12.4.1. Dell 62xx

The following steps show how a Dell 62xx is configured for pod-level layer-2 switching.

1. Configure all the VLANs in the database.

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

2. VLAN 201 is used to route untagged private IP addresses for pod 1, and pod 1 is connected to this layer-2 switch.

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

The statements configure all Ethernet ports to function as follows:

- ▶ All ports are configured the same way.
- ▶ All VLANs (300-999) are passed through all the ports of the layer-2 switch.

#### 12.4.2. Cisco 3750

The following steps show how a Cisco 3750 is configured for pod-level layer-2 switching.

1. Setting VTP mode to transparent allows us to utilize VLAN IDs above 1000. Since we only use VLANs up to 999

1. Setting vtp mode to transparent allows us to utilize VLAN IDs above 1000. Since we only use VLANs up to 999, vtp transparent mode is not strictly required.

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

2. Configure all ports to dot1q and set 201 as the native VLAN.

```
interface range GigabitEthernet 1/0/1-24
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 201
exit
```

By default, Cisco passes all VLANs. Cisco switches complain if the native VLAN IDs are different when 2 ports are connected together. That's why you must specify VLAN 201 as the native VLAN on the layer-2 switch.

## 12.5. Hardware Firewall

All deployments should have a firewall protecting the management server; see Generic Firewall Provisions. Optionally, some deployments may also have a Juniper SRX firewall that will be the default gateway for the guest networks; see [Seção 12.5.2, "External Guest Firewall Integration for Juniper SRX \(Optional\)"](#).

### 12.5.1. Generic Firewall Provisions

The hardware firewall is required to serve two purposes:

- » Protect the Management Servers. NAT and port forwarding should be configured to direct traffic from the public Internet to the Management Servers.
- » Route management network traffic between multiple zones. Site-to-site VPN should be configured between multiple zones.

To achieve the above purposes you must set up fixed configurations for the firewall. Firewall rules and policies need not change as users are provisioned into the cloud. Any brand of hardware firewall that supports NAT and site-to-site VPN can be used.

### 12.5.2. External Guest Firewall Integration for Juniper SRX (Optional)

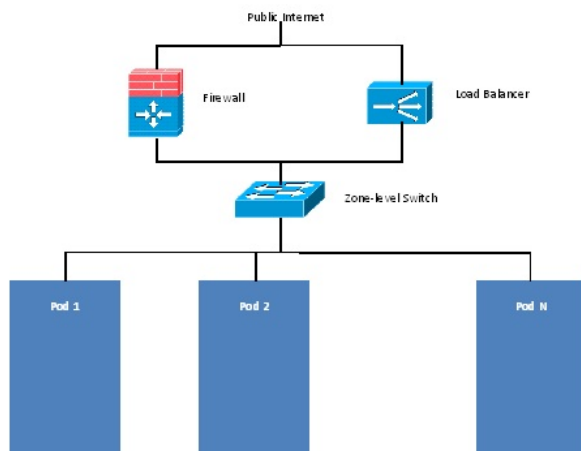


#### Nota

Available only for guests using advanced networking.

CloudStack provides for direct management of the Juniper SRX series of firewalls. This enables CloudStack to establish static NAT mappings from public IPs to guest VMs, and to use the Juniper device in place of the virtual router for firewall services. You can have one or more Juniper SRX per zone. This feature is optional. If Juniper integration is not provisioned, CloudStack will use the virtual router for these services.

The Juniper SRX can optionally be used in conjunction with an external load balancer. External Network elements can be deployed in a side-by-side or inline configuration.



CloudStack requires the Juniper to be configured as follows:



#### Nota

Supported SRX software version is 10.3 or higher.

1. Install your SRX appliance according to the vendor's instructions.
2. Connect one interface to the management network and one interface to the public network. Alternatively, you can connect the same interface to both networks and use a VLAN for the public network.
3. Make sure "vlan-tagging" is enabled on the private interface.
4. Record the public and private interface names. If you used a VLAN for the public interface, add a "[VLAN TAG]" after the interface name. For example, if you are using ge-0/0/3 for your public interface and VLAN tag 301, your public interface name would be "ge-0/0/3.301". Your private interface name should always be untagged because the CloudStack software automatically creates tagged logical interfaces.
5. Create a public security zone and a private security zone. By default, these will already exist and will be called "untrust" and "trust". Add the public interface to the public zone and the private interface to the private zone. Note down the security zone names.
6. Make sure there is a security policy from the private zone to the public zone that allows all traffic.
7. Note the username and password of the account you want the CloudStack software to log in to when it is programming rules.
8. Make sure the "ssh" and "xnm-clear-text" system services are enabled.
9. If traffic metering is desired:
  - a. Create an incoming firewall filter and an outgoing firewall filter. These filters should be the same names as your public security zone name and private security zone name respectively. The filters should be set to be "interface-specific". For example, here is the configuration where the public zone is "untrust" and the private zone is "trust":

```

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

```

- b. Add the firewall filters to your public interface. For example, a sample configuration output (for public interface ge-0/0/3.0, public security zone untrust, and private security zone trust) is:

```

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

```

10. Make sure all VLANs are brought to the private interface of the SRX.
11. After the CloudStack Management Server is installed, log in to the CloudStack UI as administrator.
12. In the left navigation bar, click Infrastructure.
13. In Zones, click View More.
14. Choose the zone you want to work with.
15. Clique na aba Network.
16. In the Network Service Providers node of the diagram, click Configure. (You might have to scroll down to see this.)
17. Click SRX.
18. Click the Add New SRX button (+) and provide the following:
  - IP Address: The IP address of the SRX.
  - Username: The user name of the account on the SRX that CloudStack should use.
  - Password: The password of the account.
  - Public Interface: The name of the public interface on the SRX. For example, ge-0/0/2. A ".x" at the end of the interface indicates the VLAN that is in use.
  - Private Interface: The name of the private interface on the SRX. For example, ge-0/0/1.
  - Usage Interface: (Optional) Typically, the public interface is used to meter traffic. If you want to use a different interface, specify its name here
  - Number of Retries: The number of times to attempt a command on the SRX before failing. The default value is 2.
  - Timeout (seconds): The time to wait for a command on the SRX before considering it failed. Default is 300 seconds.
  - Public Network: The name of the public network on the SRX. For example, trust.
  - Private Network: The name of the private network on the SRX. For example, untrust.
  - Capacity: The number of networks the device can handle
  - Dedicated: When marked as dedicated, this device will be dedicated to a single account. When Dedicated is checked, the value in the Capacity field has no significance implicitly, its value is 1
19. Clique em OK.
20. Click Global Settings. Set the parameter external.network.stats.interval to indicate how often you want CloudStack to fetch network usage statistics from the Juniper SRX. If you are not using the SRX to gather network usage statistics, set to 0.

### 12.5.3. External Guest Load Balancer Integration (Optional)

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

To install and enable an external load balancer for CloudStack management:

1. Set up the appliance according to the vendor's directions.
2. Connect it to the networks carrying public traffic and management traffic (these could be the same network).
3. Record the IP address, username, password, public interface name, and private interface name. The interface names will be something like "1.1" or "1.2".
4. Make sure that the VLANs are trunked to the management network interface.
5. After the CloudStack Management Server is installed, log in as administrator to the CloudStack UI.
6. In the left navigation bar, click Infrastructure.
7. In Zones, click View More.
8. Choose the zone you want to work with.
9. Clique na aba Network.
10. In the Network Service Providers node of the diagram, click Configure. (You might have to scroll down to see this.)
11. Click NetScaler or F5.
12. Click the Add button (+) and provide the following:  
For NetScaler:
  - IP Address: The IP address of the SRX.
  - Username/Password: The authentication credentials to access the device. CloudStack uses these credentials to access the device.
  - Type: The type of device that is being added. It could be F5 Big Ip Load Balancer, NetScaler VPX, NetScaler MPX, or NetScaler SDX. For a comparison of the NetScaler types, see the CloudStack Administration Guide.
  - Public interface: Interface of device that is configured to be part of the public network.
  - Private interface: Interface of device that is configured to be part of the private network.
  - Number of retries. Number of times to attempt a command on the device before considering the operation failed. Default is 2.
  - Capacity: The number of networks the device can handle.
  - Dedicated: When marked as dedicated, this device will be dedicated to a single account. When Dedicated is checked, the value in the Capacity field has no significance implicitly, its value is 1.
13. Clique em OK.

The installation and provisioning of the external load balancer is finished. You can proceed to add VMs and NAT or load balancing rules.

## 12.6. Management Server Load Balancing

CloudStack can use a load balancer to provide a virtual IP for multiple Management Servers. The administrator is responsible for creating the load balancer rules for the Management Servers. The application requires persistence or stickiness across multiple sessions. The following chart lists the ports that should be load balanced and whether or not persistence is required.

Even if persistence is not required, enabling it is permitted.

Source Port	Destination Port	Protocolo	Persistence Required?
80 or 443	8080 (or 20400 with AJP)	HTTP (or AJP)	Sim
8250	8250	TCP	Sim
8096	8096	HTTP	Não

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. Topology Requirements

### 12.7.1. Security Requirements

The public Internet must not be able to access port 8096 or port 8250 on the Management Server.

### 12.7.2. Runtime Internal Communications Requirements

- The Management Servers communicate with each other to coordinate tasks. This communication uses TCP on ports 8250 and 9090.
- The console proxy VMs connect to all hosts in the zone over the management traffic network. Therefore the management traffic network of any given pod in the zone must have connectivity to the management traffic network of all other pods in the zone.
- The secondary storage VMs and console proxy VMs connect to the Management Server on port 8250. If you are using multiple Management Servers, the load balanced IP address of the Management Servers on port 8250 must be reachable.

### 12.7.3. Storage Network Topology Requirements

The secondary storage NFS export is mounted by the secondary storage VM. Secondary storage traffic goes over the management traffic network, even if there is a separate storage network. Primary storage traffic goes over the storage network, if available. If you choose to place secondary storage NFS servers on the storage network, you must make sure there is a route from the management traffic network to the storage network.

#### 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. Advanced Zone Topology Requirements

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

#### 12.7.6. XenServer Topology Requirements

The Management Servers communicate with XenServer hosts on ports 22 (ssh), 80 (HTTP), and 443 (HTTPS).

#### 12.7.7. VMware Topology Requirements

- ▶ The Management Server and secondary storage VMs must be able to access vCenter and all ESXi hosts in the zone. To allow the necessary access through the firewall, keep port 443 open.
- ▶ The Management Servers communicate with VMware vCenter servers on port 443 (HTTPS).
- ▶ The Management Servers communicate with the System VMs on port 3922 (ssh) on the management traffic network.

#### 12.7.8. KVM Topology Requirements

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

### 12.8. Guest Network Usage Integration for Traffic Sentinel

To collect usage data for a guest network, CloudStack needs to pull the data from an external network statistics collector installed on the network. Metering statistics for guest networks are available through CloudStack's integration with inMon Traffic Sentinel.

Traffic Sentinel is a network traffic usage data collection package. CloudStack can feed statistics from Traffic Sentinel into its own usage records, providing a basis for billing users of cloud infrastructure. Traffic Sentinel uses the traffic monitoring protocol sFlow. Routers and switches generate sFlow records and provide them for collection by Traffic Sentinel, then CloudStack queries the Traffic Sentinel database to obtain this information.

To construct the query, CloudStack determines what guest IPs were in use during the current query interval. This includes both newly assigned IPs and IPs that were assigned in a previous time period and continued to be in use. CloudStack queries Traffic Sentinel for network statistics that apply to these IPs during the time period they remained allocated in CloudStack. The returned data is correlated with the customer account that owned each IP and the timestamps when IPs were assigned and released in order to create billable metering records in CloudStack. When the Usage Server runs, it collects this data.

To set up the integration between CloudStack and Traffic Sentinel:

1. On your network infrastructure, install Traffic Sentinel and configure it to gather traffic data. For installation and configuration steps, see inMon documentation at [Traffic Sentinel Documentation](#).
2. In the Traffic Sentinel UI, configure Traffic Sentinel to accept script querying from guest users. CloudStack will be the guest user performing the remote queries to gather network usage for one or more IP addresses. Click File > Users > Access Control > Reports Query, then select Guest from the drop-down list.
3. On CloudStack, add the Traffic Sentinel host by calling the CloudStack API command addTrafficMonitor. Pass in the URL of the Traffic Sentinel as protocol + host + port (optional); for example, http://10.147.28.100:8080. For the addTrafficMonitor command syntax, see the API Reference at [API Documentation](#). For information about how to call the CloudStack API, see the Developer's Guide at [CloudStack API Developer's Guide](#).
4. Faça login na interface de usuário do CloudStack como administrador.
5. Select Configuration from the Global Settings page, and set the following:  
direct.network.stats.interval: How often you want CloudStack to query Traffic Sentinel.

### 12.9. Setting Zone VLAN and Running VM Maximums

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

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

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

## Capítulo 13. Gerenciando redes e

# tráfego

## 13.1. Tráfego de hóspedes

## 13.2. Rede em um pod

## 13.3. Rede em uma zona

## 13.4. Configuração de rede física de zona básica

## 13.5. Configuração de rede física de zona avançada

### 13.5.1. Configure o tráfego hóspede na zona avançada

### 13.5.2. Configure o tráfego público na zona avançada

## 13.6. Usando múltiplas redes hóspedes

### 13.6.1. Adicionando uma rede hóspede adicional

### 13.6.2. Alterando a oferta de rede em uma rede hóspede

## 13.7. Grupos de segurança

### 13.7.1. About Security Groups

### 13.7.2. Adicionando um grupo de segurança

### 13.7.3. Security Groups in Advanced Zones (KVM Only)

### 13.7.4. Habilitando grupos de segurança

### 13.7.5. Adicionando regras de ingresso e egresso a um grupo de segurança

## 13.8. Firewalls e balanceadores de carga externos

### 13.8.1. Sobre a utilização do balanceador de carga NetScaler

### 13.8.2. Configuring SNMP Community String on a RHEL Server

### 13.8.3. Configuração inicial de firewalls e balanceadores de carga externos

### 13.8.4. Configuração continuada de firewalls e balanceadores de carga externos

### 13.8.5. Configuring AutoScale

## 13.9. Regras de balanceamento de carga

### 13.9.1. Adding a Load Balancer Rule

### 13.9.2. Sticky Session Policies for Load Balancer Rules

## 13.10. Guest IP Ranges

## 13.11. Obtendo um novo endereço IP

## 13.12. Liberando um endereço IP

## 13.13. NAT estática

### 13.13.1. Habilitando ou desabilitando NAT estática

## 13.14. Encaminhamento de IP e firewall

### 13.14.1. Creating Egress Firewall Rules in an Advanced Zone

### 13.14.2. Regras de firewall

### 13.14.3. Encaminhamento de Porta

## 13.15. Balanceamento de carga de IP

## 13.16. DNS e DHCP

## 13.17. VPN

### 13.17.1. Configurando VPN

### 13.17.2. Usando VPN com Windows

### 13.17.3. Using VPN with Mac OS X

### 13.17.4. Configurando uma conexão VPN Site-to-Site

## 13.18. About Inter-VLAN Routing

## 13.19. Configuring a Virtual Private Cloud

### 13.19.1. About Virtual Private Clouds

### 13.19.2. Adding a Virtual Private Cloud

### 13.19.3. Adding Tiers

### 13.19.4. Configuring Access Control List

### 13.19.5. Adicionando um gateway privado a uma VPC

### 13.19.6. Implantando máquinas virtuais na camada

### 13.19.7. Obtendo um novo endereço IP para uma VPC

### 13.19.8. Liberando um endereço IP atribuído a uma VPC

### 13.19.9. Habilitando ou desabilitando NAT estática em uma VPC

### 13.19.10. Adicionando regras de balanceamento de carga em uma VPC

### 13.19.11. Adicionando uma regra de encaminhamento de porta em uma VPC

### 13.19.12. Removing Tiers

### 13.19.13. Editing, Restarting, and Removing a Virtual Private Cloud



## 13.20. Persistent Networks

### 13.20.1. Persistent Network Considerations

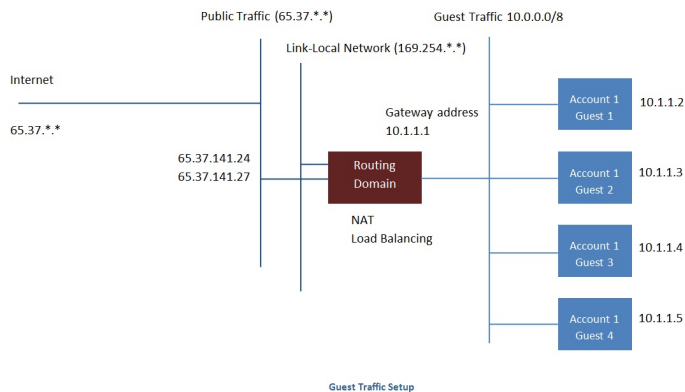
### 13.20.2. Creating a Persistent Guest Network

Em um ambiente CloudStack, máquinas virtuais hóspedes podem comunicar-se entre si usando uma infraestrutura compartilhada com segurança e com a percepção do usuário que os hóspedes têm uma rede privada. O roteador virtual do CloudStack é o principal componente a fornecer recursos de rede para o tráfego de hóspedes.

## 13.1. Tráfego de hóspedes

Uma rede pode transportar tráfego de hóspedes somente entre máquinas virtuais em uma zona. Máquinas virtuais em diferentes zonas não podem se comunicar usando seus endereços IP; elas devem se comunicar através de roteamento em uma rede IP pública.

This figure illustrates a typical guest traffic setup:



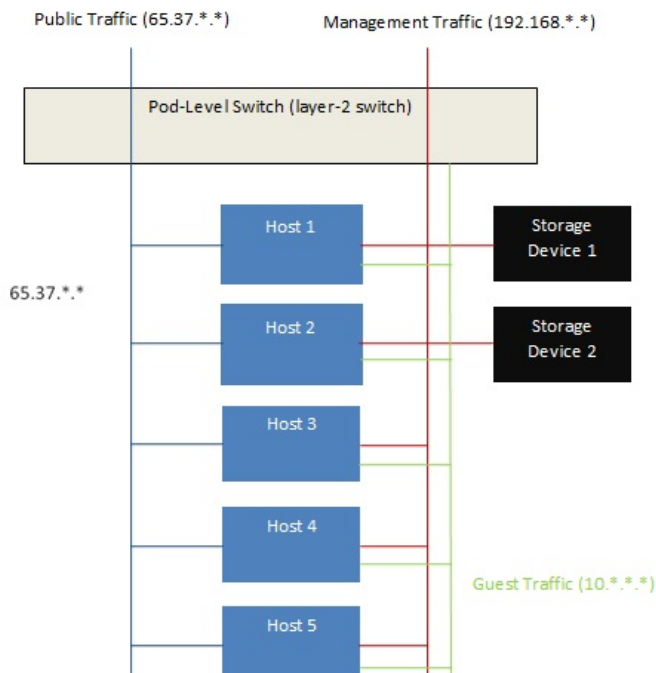
O servidor de gerenciamento automaticamente cria um roteador virtual para cada rede. Um roteador virtual é uma máquina virtual especial que executa nos hosts. Cada roteador virtual tem três interfaces de rede. Seu interface eth0 serve como o gateway para o tráfego hóspede e tem o endereço IP 10.1.1.1. Seu interface eth1 é usado pelo sistema para configurar o roteador virtual. A seu interface eth2 é assinalado um endereço IP público para tráfego público.

O roteador virtual provê DHCP e automaticamente irá assinalar um endereço IP para cada máquina virtual no intervalo de IPs assinalado para a rede. O usuário pode manualmente reconfigurar máquinas virtuais hóspedes para utilizarem diferentes endereços IP.

NAT da origem é automaticamente configurado no roteador virtual para encaminhar tráfego de saída para todas as máquinas virtuais hóspedes

## 13.2. Rede em um 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.





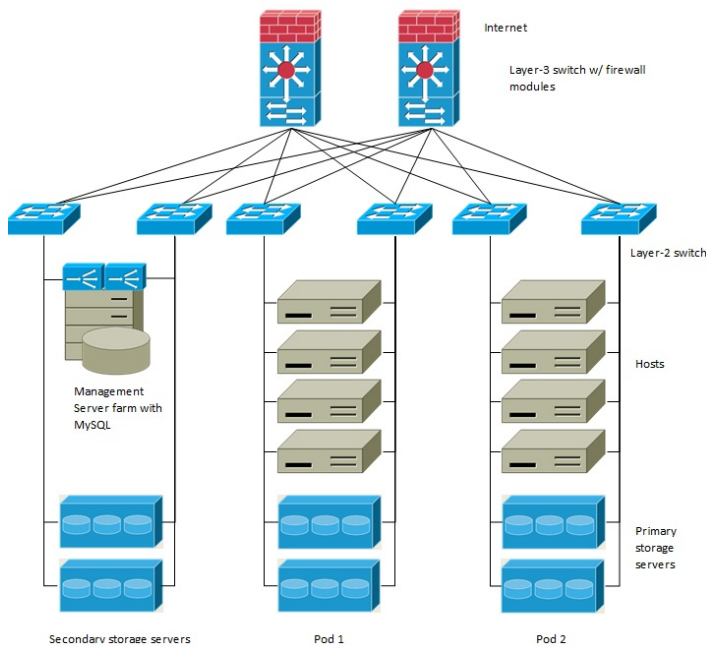
Servidores são conectados como se segue:

- » Equipamentos de storage são conectados somente à rede que transporta tráfego de gerenciamento.
- » Hosts são conectados a redes tanto para tráfego de gerência quanto para tráfego público.
- » Hosts também são conectados a uma ou mais redes que transportam tráfego de hóspedes.

Recomendamos o uso de múltiplas placas Ethernet físicas para implementar cada interface de rede, assim como switch fabrics redundantes, para maximizar o throughput e aumentar a confiabilidade.

### 13.3. Rede em uma zona

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



Um firewall para tráfego de gerência opera em modo NAT. Tipicamente à rede é assinalado um endereço IP do espaço de endereços classe B 192.168.0.0/16. A cada pod é assinalado um endereço IP no espaço de endereços classe C privado 192.168.\*.0/24.

Cada zona tem seu próprio conjunto de endereços IP públicos. Endereços IP públicos de diferentes zonas não se sobrepõem.

### 13.4. Configuração de rede física de zona básica

Em uma rede básica, a configuração da rede física é bastante simples. Na maioria dos casos, você precisa somente configurar uma rede hóspede para transportar tráfego que é gerado pelas máquinas virtuais hóspedes. Quando você adiciona a primeira zona ao CloudStack, você configura a rede hóspede através das telas Add Zone.

### 13.5. Configuração de rede física de zona avançada

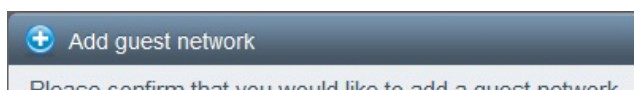
Em uma zona que usa rede avançada, você precisa informar ao servidor de gerenciamento como a rede física é configurada para transportar diferentes tipos de tráfego com isolamento.

#### 13.5.1. Configure o tráfego hóspede na zona avançada

Nestes passos se supõe que você já está logado na interface de usuário do CloudStack. Para configurar a base da rede hóspede:

1. No painel de navegação à esquerda, selecione Infrastructure. Em Zones, clique View More, então clique a zona à qual você deseja adicionar uma rede.
2. Clique na aba Network.
3. Clique em Add guest network.

A janela Add guest network é apresentada:



Please confirm that you would like to add a guest network

\* Name:

\* Display Text:

\* Zone:

\* Network Offering:

Guest Gateway:

Guest Netmask:

Cancel OK

4. Forneça as seguintes informações:

- » **Name.** O nome da rede. Isto será visível pelo usuário
- » **Display Text:** A descrição da rede. Isto será visível pelo usuário
- » **Zone:** A zona na qual você está configurando a rede hóspede.
- » **Network offering:** Se o administrador configurou múltiplas ofertas de rede, selecione a que você deseja usar para esta rede
- » **Guest Gateway:** O gateway que os hóspedes devem usar
- » **Guest Netmask:** A máscara de rede em uso na subnet que os hóspedes utilizarão

5. Clique em OK.

### 13.5.2. Configure o tráfego público na zona avançada

Em uma zona que usa rede avançada, você precisa configurar pelo menos um intervalo de endereços IP para tráfego de Internet.

## 13.6. Usando múltiplas redes hóspedes

Em zonas que usam rede avançada, redes adicionais para tráfego hóspede podem ser adicionadas a qualquer tempo após a instalação inicial. Você pode também customizar o nome de domínio associado com a rede especificando um sufixo DNS para cada rede.

As redes de uma máquina virtual são definidas em tempo de criação da máquina virtual. Uma máquina virtual não pode adicionar ou remover redes após ter sido criada, embora o usuário possa remover no hóspede o endereço IP da NIC de uma rede específica.

Cada máquina virtual tem somente uma rede default. A resposta do DHCP do roteador virtual irá determinar o default gateway do hóspede como aquele da rede default. Múltiplas redes non-default podem ser adicionadas a um hóspede em adição à rede default, única, requerida. O administrador pode controlar quais redes são disponíveis como rede default.

Redes adicionais podem estar disponíveis para todas as contas ou serem assinaladas a uma conta específica. Redes que estão disponíveis para todas as contas são zone-wide. Qualquer usuário com acesso à zona pode criar uma máquina virtual com acesso àquela rede. Estas redes zone-wide proveem pequeno ou nenhum isolamento entre hóspedes. Redes que são assinaladas a contas específicas proveem isolamento robusto.

### 13.6.1. Adicionando uma rede hóspede adicional


1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Clique em Add guest network. Forneça as seguintes informações:
  - » **Name.** O nome da rede. Isto será visível pelo usuário.
  - » **Display Text:** A descrição da rede. Isto será visível pelo usuário.
  - » **Zone.** O nome da zona a qual esta rede se aplica. Cada zona é um domínio de broadcast, e portanto cada zona tem um diferente intervalo de IP para a rede hóspede. O administrador deve configurar o intervalo de IP para cada zona.
  - » **Network offering:** Se o administrador configurou múltiplas ofertas de rede, selecione a que você deseja usar para esta rede.
  - » **Guest Gateway:** O gateway que os hóspedes devem usar.
  - » **Guest Netmask:** A máscara de rede em uso na subnet que os hóspedes utilizarão.
4. Clique em Create.

### 13.6.2. Alterando a oferta de rede em uma rede hóspede

Um usuário ou administrador pode alterar a oferta de rede associada com uma rede hóspede associada.

- » Faça login na interface de usuário do CloudStack como administrador ou usuário final.
- » If you are changing from a network offering that uses the CloudStack virtual router to one that uses external devices as

network service providers, you must first stop all the VMs on the network. See "Stopping and Starting Virtual Machines" in the Administrator's Guide.

- » Na barra de navegação à esquerda, selecione Network.
- » Click the name of the network you want to modify.
- » In the Details tab, click Edit. 
- » Em Network Offering, escolha a nova oferta de rede, então clique em Apply.
- » A prompt is displayed asking whether you want to keep the existing CIDR. This is to let you know that if you change the network offering, the CIDR will be affected. Choose No to proceed with the change.
- » Wait for the update to complete. Don't try to restart VMs until the network change is complete.
- » If you stopped any VMs, restart them.

## 13.7. Grupos de segurança

### 13.7.1. About Security Groups

Security groups provide a way to isolate traffic to VMs. A security group is a group of VMs that filter their incoming and outgoing traffic according to a set of rules, called ingress and egress rules. These rules filter network traffic according to the IP address that is attempting to communicate with the VM. Security groups are particularly useful in zones that use basic networking, because there is a single guest network for all guest VMs. In advanced zones, security groups are supported only on the KVM hypervisor.



#### Nota

In a zone that uses advanced networking, you can instead define multiple guest networks to isolate traffic to VMs.

Each CloudStack account comes with a default security group that denies all inbound traffic and allows all outbound traffic. The default security group can be modified so that all new VMs inherit some other desired set of rules.

Any CloudStack user can set up any number of additional security groups. When a new VM is launched, it is assigned to the default security group unless another user-defined security group is specified. A VM can be a member of any number of security groups. Once a VM is assigned to a security group, it remains in that group for its entire lifetime; you can not move a running VM from one security group to another.

You can modify a security group by deleting or adding any number of ingress and egress rules. When you do, the new rules apply to all VMs in the group, whether running or stopped.

If no ingress rules are specified, then no traffic will be allowed in, except for responses to any traffic that has been allowed out through an egress rule.

### 13.7.2. Adicionando um grupo de segurança

Um usuário ou administrador pode definir um novo grupo de segurança.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Em Select view, selecione Security Groups.
4. Clique em Add Security Group.
5. Forneça um nome e descrição.
6. Clique em OK.  
O novo grupo de segurança aparece na aba Security Groups Details.
7. Para tornar útil o grupo de segurança, continue em Adicionando regras de ingresso e egresso a um grupo de segurança.

### 13.7.3. Security Groups in Advanced Zones (KVM Only)

CloudStack provides the ability to use security groups to provide isolation between guests on a single shared, zone-wide network in an advanced zone where KVM is the hypervisor. Using security groups in advanced zones rather than multiple VLANs allows a greater range of options for setting up guest isolation in a cloud.

#### Limitations

The following are not supported for this feature:

- » Two IP ranges with the same VLAN and different gateway or netmask in security group-enabled shared network.
- » Two IP ranges with the same VLAN and different gateway or netmask in account-specific shared networks.
- » Multiple VLAN ranges in security group-enabled shared network.
- » Multiple VLAN ranges in account-specific shared networks.

Security groups must be enabled in the zone in order for this feature to be used.

### 13.7.4. Habilitando grupos de segurança

In order for security groups to function in a zone, the security groups feature must first be enabled for the zone. The administrator can do this when creating a new zone, by selecting a network offering that includes security groups. The procedure is described in Basic Zone Configuration in the Advanced Installation Guide. The administrator can not enable security groups for an existing zone, only when creating a new zone.

## 13.7.5. Adicionando regras de ingresso e egresso a um grupo de segurança

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Em Select view, selecione Security Groups, então clique no grupo de segurança que você deseja.
4. Para adicionar uma regra de ingresso, clique na aba Ingress Rules e preencha os campos seguintes para especificar qual tráfego de rede é permitido em instâncias de máquinas virtuais neste grupo de segurança. Se nenhuma regra de ingresso é especificada, então nenhum tráfego será permitido entrar, exceto respostas a qualquer tráfego que tenha sido permitido sair por uma regra de egresso.
  - **Add by CIDR/Account.** Indica se a fonte do tráfego será definida pelo endereço IP (CIDR) ou por um grupo de segurança existente em uma conta do CloudStack (Account). Selecione Account se você deseja permitir tráfego de entrada oriundo de todas as máquinas virtuais em outro grupo de segurança
  - **Protocol.** O protocolo de rede que as fontes utilizarão para enviar tráfego ao grupo de segurança. TCP e UDP são usados tipicamente para intercâmbio de dados e comunicações de usuários finais. ICMP é usado tipicamente para enviar mensagens de erro e dados de monitoração de rede.
  - **Start Port, End Port.** (somente para TCP e UDP) Um intervalo de listening ports que são os destinos do tráfego entrante. Se você está abrindo uma única porta, use o mesmo número em ambos os campos.
  - **ICMP Type, ICMP Code.** (somente ICMP) O tipo de mensagem e o código de erro que serão aceitos.
  - **CIDR.** (Adição somente por CIDR) Para aceitar tráfego somente de endereços IP em um bloco de endereços específico, informe um CIDR ou uma lista de CIDRs separados por vírgulas. O CIDR é o endereço IP base do tráfego entrante. Por exemplo, 192.168.0.0/22. Para permitir todos os CIDRs, especifique 0.0.0.0/0.
  - **Account, Security Group.** (Adição somente por conta) Para aceitar somente tráfego de outro grupo de segurança, informe a conta do CloudStack e nome de um grupo de segurança que já esteja definido naquela conta. Para permitir tráfego entre máquinas virtuais no grupo de segurança que você está editando, informe o mesmo nome que você usou no passo 7.

Um exemplo a seguir permite acesso HTTP entrante de qualquer lugar:

Protocol	Start Port	End Port	CIDR	Add
TCP	80	80	0.0.0.0/0	Add

5. Para adicionar uma regra de egresso, clique na aba Egress Rules e preencha os campos seguintes para especificar qual tipo de tráfego de rede é permitido ser enviado de instâncias de máquinas virtuais neste grupo de segurança. Se nenhuma regra de egresso é especificada, então todo tráfego será permitido sair. Uma vez que regras de egresso são especificadas, os seguintes tipos de tráfego são permitidos sair: tráfego especificado regras de egresso; queries a servidores DNS e DHCP; e respostas a qualquer tráfego que tenha sido permitido entrar através de uma regra de ingresso
  - **Add by CIDR/Account.** Indica se o destino do tráfego será definido pelo endereço IP (CIDR) ou por um grupo de segurança existente em uma conta do CloudStack (Account). Selecione Account se você deseja permitir tráfego de saída destinado a todas as máquinas virtuais em outro grupo de segurança.
  - **Protocol.** O protocolo de rede que máquinas virtuais usarão para enviar tráfego de saída. TCP e UDP são usados tipicamente para intercâmbio de dados e comunicações de usuários finais. ICMP é usado tipicamente para enviar mensagens de erro e dados de monitoração de rede.
  - **Start Port, End Port.** (somente para TCP e UDP) Um intervalo de listening ports que são os destinos do tráfego saindo. Se você está abrindo uma única porta, use o mesmo número em ambos os campos.
  - **ICMP Type, ICMP Code.** (somente ICMP) O tipo de mensagem e o código de erro que serão enviados.
  - **CIDR.** (Adição somente por CIDR) Para enviar tráfego somente a endereços IP em um bloco de endereços específico, informe um CIDR ou uma lista de CIDRs separados por vírgulas. O CIDR é o endereço IP base do tráfego entrante. Por exemplo, 192.168.0.0/22. Para permitir todos os CIDRs, especifique 0.0.0.0/0.
  - **Account, Security Group.** (Adição somente por conta) Para permitir o envio de tráfego a outro grupo de segurança, informe a conta do CloudStack e nome de um grupo de segurança que já esteja definido naquela conta. Para permitir tráfego entre máquinas virtuais no grupo de segurança que você está editando, informe o nome do grupo.
6. Clique em Add.

## 13.8. Firewalls e balanceadores de carga externos

O CloudStack é capaz de substituir seu roteador virtual por um equipamento Juniper SRX externo e um balanceador de carga externo NetScaler ou F5 para serviços de gateway e balanceamento de carga. Neste caso, as máquinas virtuais usam o SRX como seu gateway.

### 13.8.1. Sobre a utilização do balanceador de carga NetScaler

O Citrix NetScaler é suportado como um elemento externo de rede para balanceamento de carga em zonas que usam rede avançada (também chamadas zonas avançadas). Configure um balanceador de carga externo quando você quiser prover balanceamento de carga por outros meios que o roteador virtual provido pelo CloudStack.

O NetScaler pode ser configurado em modo direto (fora do firewall). Ele deve ser adicionado antes que qualquer regra de balanceamento de carga seja implementada em máquinas virtuais da zona.

O comportamento funcional do NetScaler com o CloudStack é o mesmo que é descrito na documentação do CloudStack para o uso de um balanceador de carga externo F5. A seguir, você verá como configurar o NetScaler para ser usado com o CloudStack.

CloudStack para uso de um balanceador de carga externo F5. A única exceção é que o F5 suporta domínios de roteamento, e o NetScaler não. O NetScaler ainda não pode ser usado como um firewall.

O Citrix NetScaler é oferecido em três variantes. A tabela a seguir resume como estas variantes são tratadas no CloudStack.

Tipo de NetScaler ADC	Descrição das capacidades	Recursos suportados no CloudStack
MPX	Dispositivo físico. Capaz de inspeção profunda de pacotes. Pode atuar como application firewall e balanceador de carga	Em zonas avançadas, a funcionalidade de balanceador de carga é suportada sem limitações. Em zonas básicas, NAT estática, elastic IP (EIP), e elastic load balancing (ELB) também são providos
VPX	Dispositivo virtual. Pode ser executado como máquina virtual nos hipervisores XenServer, ESXi, e Hyper-V. Mesma funcionalidade que MPX	Suportado somente no ESXi. Mesmo suporte funcional que MPX. O CloudStack tratará VPX e MPX como o mesmo tipo de dispositivo
SDX	Dispositivo físico. Pode criar múltiplas instâncias VPX completamente isoladas em um único dispositivo para suportar uso por múltiplos hóspedes	O CloudStack irá dinamicamente aprovisionar, configurar, e gerenciar o ciclo de vida de instâncias VPX no SDX. Instâncias fornecidas são automaticamente adicionadas ao CloudStack – nenhuma configuração manual pelo administrador é requerida. Uma vez que uma instância VPX é adicionada ao CloudStack, ela é tratada da mesma forma que uma VPX em um host ESXi.

### 13.8.2. Configuring SNMP Community String on a RHEL Server

The SNMP Community string is similar to a user id or password that provides access to a network device, such as router. This string is sent along with all SNMP requests. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device discards the request and does not respond.

The NetScaler device uses SNMP to communicate with the VMs. You must install SNMP and configure SNMP Community string for a secure communication between the NetScaler device and the RHEL machine.

1. Ensure that you installed SNMP on RedHat. If not, run the following command:

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

2. Edit the `/etc/snmp/snmpd.conf` file to allow the SNMP polling from the NetScaler device.
  - a. Map the community name into a security name (local and mynetwork, depending on where the request is coming from):



#### Nota

Use a strong password instead of public when you edit the following table.

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



#### Nota

Setting to 0.0.0.0 allows all IPs to poll the NetScaler server.

- b. Map the security names into group names:

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

- c. Create a view to allow the groups to have the permission to:

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

- d. Grant access with different write permissions to the two groups to the view you created.

```
# 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. Unblock SNMP in iptables.

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

4. Start the SNMP service:

```
service snmpd start
```

5. Ensure that the SNMP service is started automatically during the system startup:

```
chkconfig snmpd on
```

### 13.8.3. Configuração inicial de firewalls e balanceadores de carga externos

Quando a primeira máquina virtual é criada para uma nova conta, o CloudStack programa o firewall e o balanceador de carga externos para trabalhar com a máquina virtual. Os seguintes objetos são criados no firewall:

- » Uma nova interface lógica para conectar à VLAN privada da conta. O IP da interface é sempre o primeiro IP da subnet privada da conta (e.g. 10.1.1.1).
- » Uma regra NAT de origem que encaminha todo o tráfego sainte da VLAN privada da conta para a Internet pública, usando o endereço IP público da conta como o endereço de origem
- » Um contador de filtro de firewall que registra o número de bytes do tráfego sainte da conta

Os seguintes objetos são criados no balanceador de carga:

- » Uma nova VLAN que corresponde à VLAN na zona fornecida para a conta
- » Um IP para a VLAN. Este é sempre o segundo IP da subnet privada da conta (e.g. 10.1.1.2).

### 13.8.4. Configuração continuada de firewalls e balanceadores de carga externos

Ações adicionais de usuários (e.g. configuração de um encaminhamento de porta) causará programação adicional do firewall e balanceador de carga. Um usuário pode requisitar endereços IP públicos adicionais e encaminhamento de tráfego recebido nestes IPs para máquinas virtuais específicas. Isto é executado através da habilitação de NAT estático para um endereço IP público, assinalando o IP a uma máquina virtual, e especificando um conjunto de protocolos e intervalos de portas a liberar. Quando uma regra NAT estática é criada, o CloudStack programa o firewall externo da zona com os seguintes objetos:

- » Uma regra NAT estática que mapeia o endereço IP público ao endereço IP privado de uma máquina virtual.
- » Uma política de segurança que permite tráfego no conjunto de protocolos e intervalos de porta que são especificados.
- » Um contador de filtro de firewall que registra o número de bytes do tráfego entrante no IP público.

O número de bytes entrantes e saintes através de NAT de origem, NAT estático, e regras de balanceamento de carga é medido e salvo em cada elemento externo. Este dado é coletado regularmente e armazenado no database do CloudStack.

### 13.8.5. Configuring 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 is designed to seamlessly launch or terminate VMs based on user-defined conditions. Conditions for triggering a scaleup or scaledown action can vary from a simple use case like monitoring the CPU usage of a server to a complex use case of monitoring a combination of server's responsiveness and its CPU usage. For example, you can configure AutoScaling to launch an additional VM whenever CPU usage exceeds 80 percent for 15 minutes, or to remove a VM whenever CPU usage is less than 20 percent for 30 minutes.

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.



#### Nota

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

#### Prerequisites

Before you configure an AutoScale rule, consider the following:

- » Ensure that the necessary template is prepared before configuring AutoScale. When a VM is deployed by using a template and when it comes up, the application should be up and running.



#### Nota

If the application is not running, the NetScaler device considers the VM as ineffective and continues provisioning the VMs unconditionally until the resource limit is exhausted.

- » Deploy the templates you prepared. Ensure that the applications come up on the first boot and is ready to take the traffic. Observe the time requires to deploy the template. Consider this time when you specify the quiet time while configuring AutoScale.
- » The AutoScale feature supports the SNMP counters that can be used to define conditions for taking scale up or scale down actions. To monitor the SNMP-based counter, ensure that the SNMP agent is installed in the template used for creating the AutoScale VMs and the SNMP operations work with the configured SNMP community and port by using

creating the AutoScale VMs, and the SNMP operations with that are configured SNMP community and port by using standard SNMP managers. For example, see [Seção 13.8.2, “Configuring SNMP Community String on a RHEL Server”](#) to configure SNMP on a RHEL machine.

- ▶ Ensure that the `endpoint.url` parameter present in the Global Settings is set to the Management Server API URL. For example, `http://10.102.102.22:8080/client/api`. In a multi-node Management Server deployment, use the virtual IP address configured in the load balancer for the management server’s cluster. Additionally, ensure that the NetScaler device has access to this IP address to provide AutoScale support.

If you update the `endpoint.url`, disable the AutoScale functionality of the load balancer rules in the system, then enable them back to reflect the changes. For more information see [Updating an AutoScale Configuration](#)

- ▶ If the API Key and Secret Key are regenerated for an AutoScale user, ensure that the AutoScale functionality of the load balancers that the user participates in are disabled and then enabled to reflect the configuration changes in the NetScaler.
- ▶ In an advanced Zone, ensure that at least one VM should be present before configuring a load balancer rule with AutoScale. Having one VM in the network ensures that the network is in implemented state for configuring AutoScale.

## Configuração

Especifique o seguinte:

- ▶ **Template:** A template consists of a base OS image and application. A template is used to provision the new instance of an application on a scaleup action. When a VM is deployed from a template, the VM can start taking the traffic from the load balancer without any admin intervention. For example, if the VM is deployed for a Web service, it should have the Web server running, the database connected, and so on.
- ▶ **Compute offering:** A predefined set of virtual hardware attributes, including CPU speed, number of CPUs, and RAM size, that the user can select when creating a new virtual machine instance. Choose one of the compute offerings to be used while provisioning a VM instance as part of scaleup action.
- ▶ **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 available to serve the traffic.

### Nota

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.

### Nota

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. Regras de balanceamento de carga

Um usuário ou administrador do CloudStack pode criar regras de balanceamento de carga que distribuem o tráfego recebido em um endereço IP público por uma ou mais máquinas virtuais. Um usuário cria uma regra, especifica um algoritmo e assinala a regra a um conjunto de máquinas virtuais.



### Nota

Se você cria regras de balanceamento de carga enquanto usando um oferta de serviço de rede que inclui um equipamento externo de balanceamento de carga, como o NetScaler, e depois altera a oferta de serviço para um que usa o roteador virtual do CloudStack, você deve criar uma regra no firewall do roteador virtual para cada uma

das regras de balanceamento de carga existentes, de forma que elas possam continuar funcionando.

### 13.9.1. Adding a Load Balancer Rule

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Click the name of the network where you want to load balance the traffic.
4. Clique em View IP Addresses.
5. Clique no endereço IP para o qual você deseja criar a regra, então clique na aba Configuration.
6. No nó Load Balancing do diagrama, clique em View All.  
In a Basic zone, you can also create a load balancing rule without acquiring or selecting an IP address. CloudStack internally assign an IP when you create the load balancing rule, which is listed in the IP Addresses page when the rule is created.  
To do that, select the name of the network, then click Add Load Balancer tab. Continue with [7](#).
7. Fill in the following:
  - ▶ **Name:** Um nome para a regra de balanceamento de carga.
  - ▶ **Public Port:** The port receiving incoming traffic to be balanced.
  - ▶ **Private Port:** A porta que as máquinas virtuais usarão para receber o tráfego.
  - ▶ **Algorithm:** Choose the load balancing algorithm you want CloudStack to use. CloudStack supports a variety of well-known algorithms. If you are not familiar with these choices, you will find plenty of information about them on the Internet.
  - ▶ **Stickiness:** (Optional) Click Configure and choose the algorithm for the stickiness policy. See Sticky Session Policies for Load Balancer Rules.
  - ▶ **AutoScale:** Click Configure and complete the AutoScale configuration as explained in [Seção 13.8.5, "Configuring AutoScale"](#).
8. Click Add VMs, then select two or more VMs that will divide the load of incoming traffic, and click Apply.  
The new load balancer rule appears in the list. You can repeat these steps to add more load balancer rules for this IP address.

### 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. Guest IP Ranges


The IP ranges for guest network traffic are set on a per-account basis by the user. This allows the users to configure their network in a fashion that will enable VPN linking between their guest network and their clients.

## 13.11. Obtendo um novo endereço IP

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Clique no nome da rede com a qual você quer trabalhar.
4. Clique em View IP Addresses.
5. Clique em Acquire New IP, e clique Yes no diálogo de confirmação.  
Você deve confirmar porque, tipicamente, endereços IP são um recurso limitado. Em alguns momentos, o novo endereço IP deve aparecer no estado Allocated. Agora você pode usar o endereço IP no encaminhamento de porta ou regras NAT estáticas.

## 13.12. Liberando um endereço IP

When the last rule for an IP address is removed, you can release that IP address. The IP address still belongs to the VPC; however, it can be picked up for any guest network again.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Clique no nome da rede com a qual você quer trabalhar.
4. Clique em View IP Addresses.
5. Clique no endereço IP que você deseja liberar.
6. Click the Release IP button. 

## 13.13. NAT estática


A static NAT rule maps a public IP address to the private IP address of a VM in order to allow Internet traffic into the VM. The public IP address always remains the same, which is why it is called "static" NAT. This section tells how to enable or disable static NAT for a particular IP address.

### 13.13.1. Habilitando ou desabilitando NAT estática

Se regras de encaminhamento de portas já estão em efeito para um endereço IP, você não pode habilitar NAT estática para este IP.

Se uma máquina virtual hóspede faz parte de mais de uma rede, regras de NAT estática funcionarão somente se elas estão definidas na rede default.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Clique no nome da rede com a qual você quer trabalhar.
4. Clique em View IP Addresses.
5. Clique no endereço IP com o qual você deseja trabalhar.

6. Click the Static NAT  button.

The button toggles between Enable and Disable, depending on whether static NAT is currently enabled for the IP address.

7. If you are enabling static NAT, a dialog appears where you can choose the destination VM and click Apply.

## 13.14. Encaminhamento de IP e firewall

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 [Seção 13.14.1, "Creating Egress Firewall Rules in an Advanced Zone"](#).

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 [Seção 13.14.2, "Regras de firewall"](#) and [Seção 13.14.3, "Encaminhamento de Porta"](#).

### 13.14.1. Creating Egress Firewall Rules in an Advanced Zone



#### Nota

The egress firewall rules are supported only on virtual routers.

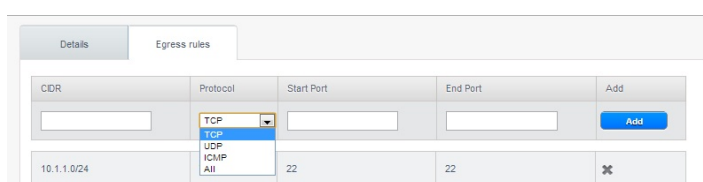
The egress traffic originates from a private network to a public network, such as the Internet. By default, the egress traffic is blocked, so no outgoing traffic is allowed from a guest network to the Internet. However, you can control the egress traffic in an Advanced zone by creating egress firewall rules. When an egress firewall rule is applied, the traffic specific to the rule is allowed and the remaining traffic is blocked. When all the firewall rules are removed the default policy, Block, is applied.

Consider the following scenarios to apply egress firewall rules:

- » Allow the egress traffic from specified source CIDR. The Source CIDR is part of guest network CIDR.
- » Allow the egress traffic with destination protocol TCP,UDP,ICMP, or ALL.
- » Allow the egress traffic with destination protocol and port range. The port range is specified for TCP, UDP or for ICMP type and code.

To configure an egress firewall rule:

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. In Select view, choose Guest networks, then click the Guest network you want.
4. To add an egress rule, click the Egress rules tab and fill out the following fields to specify what type of traffic is allowed to be sent out of VM instances in this guest network:



CIDR	Protocol	Start Port	End Port	Add
10.1.1.0/24	TCP	22	22	

- » **CIDR:** (Add by CIDR only) To send traffic only to the IP addresses within a particular address block, enter a CIDR or a comma-separated list of CIDRs. The CIDR is the base IP address of the destination. For example, 192.168.0.0/22. To allow all CIDRs, set to 0.0.0.0/0.
- » **Protocol:** The networking protocol that VMs uses to send outgoing traffic. The TCP and UDP protocols are typically used for data exchange and end-user communications. The ICMP protocol is typically used to send

error messages or network monitoring data.

- ▶ **Start Port, End Port:** (TCP, UDP only) A range of listening ports that are the destination for the outgoing traffic. If you are opening a single port, use the same number in both fields.
- ▶ **ICMP Type, ICMP Code:** (ICMP only) The type of message and error code that are sent.

5. Clique em Add.

### 13.14.2. Regras de firewall

Por default, todo o tráfego entrante no endereço IP público é rejeitado pelo firewall. Para permitir tráfego externo, você pode abrir portas no firewall especificando regras de firewall. Opcionalmente, você pode especificar um ou mais CIDRs para filtrar os IPs de origem. Isto é útil quando você deseja permitir tráfego entrante somente de certos endereços IP.

Você não pode usar regras de firewall para abrir portas para um endereço IP elástico. Quando um IP elástico é usado, acesso externo é controlado pelo uso de grupos de segurança. Veja [Seção 13.7.2, "Adicionando um grupo de segurança"](#).

In an advanced zone, you can also create egress firewall rules by using the virtual router. For more information, see [Seção 13.14.1, "Creating Egress Firewall Rules in an Advanced Zone"](#).

Regras de firewall podem ser criadas usando a aba Firewall no interface de usuário do Servidor de gerenciamento. Por default, esta aba não é apresentada quando o CloudStack é instalado. Para exibir a aba Firewall, o administrador do CloudStack deve configurar o parâmetro global `firewall.rule.ui.enabled` como "true."

Para criar uma regra de firewall:

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Clique no nome da rede com a qual você quer trabalhar.
4. Clique em View IP Addresses.
5. Clique no endereço IP com o qual você deseja trabalhar.
6. Clique na aba Configuration e preencha os seguintes valores.
  - ▶ **Source CIDR.** (Opcional) Para aceitar tráfego somente de endereços IP em um bloco de endereços específico, informe um CIDR ou uma lista de CIDRs separados por vírgulas.. Exemplo: 192.168.0.0/22. Deixe vazio para permitir todos os CIDRs.
  - ▶ **Protocol.** O protocolo de comunicação em uso na(s) porta(s) aberta(s).
  - ▶ **Start Port e End Port.** A(s) porta(s) que você deseja abrir no firewall. Se você está abrindo um única porta, use o mesmo número em ambos os campos
  - ▶ **ICMP Type e ICMP Code.** Usados somente se Protocol é configurado como ICMP. Proveem o tipo e o código requeridos pelo protocolo ICMP para preencher o cabeçalho ICMP. Consulte a documentação do ICMP para mais detalhes se você não tem certeza do que informar
7. Clique em Add.

### 13.14.3. Encaminhamento de Porta

A port forward service is a set of port forwarding rules that define a policy. A port forward service is then applied to one or more guest VMs. The guest VM then has its inbound network access managed according to the policy defined by the port forwarding service. You can optionally specify one or more CIDRs to filter the source IPs. This is useful when you want to allow only incoming requests from certain IP addresses to be forwarded.

A guest VM can be in any number of port forward services. Port forward services can be defined but have no members. If a guest VM is part of more than one network, port forwarding rules will function only if they are defined on the default network

You cannot use port forwarding to open ports for an elastic IP address. When elastic IP is used, outside access is instead controlled through the use of security groups. See Security Groups.

To set up port forwarding:

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. If you have not already done so, add a public IP address range to a zone in CloudStack. See Adding a Zone and Pod in the Installation Guide.
3. Add one or more VM instances to CloudStack.
4. In the left navigation bar, click Network.
5. Click the name of the guest network where the VMs are running.
6. Choose an existing IP address or acquire a new IP address. See [Seção 13.11, "Obtendo um novo endereço IP"](#). Click the name of the IP address in the list.
7. Click the Configuration tab.
8. No nó Port Forwarding do diagrama, clique em View All.
9. Fill in the following:
  - ▶ **Public Port.** The port to which public traffic will be addressed on the IP address you acquired in the previous step.
  - ▶ **Private Port.** The port on which the instance is listening for forwarded public traffic.
  - ▶ **Protocol.** The communication protocol in use between the two ports
10. Clique em Add.

### 13.15. Balanceamento de carga de IP

O usuário pode escolher associar o mesmo IP público para vários hóspedes. O CloudStack implementa um balanceador de carga em nível de TCP com as seguintes políticas.

- ▶ Round-robin
- ▶ Menor quantidade de conexões
- ▶ IP de origem

Isto é similar a encaminhamento de porta, mas o destino pode ser múltiplos endereços IP.

## 13.16. DNS e DHCP

O roteador virtual provê serviços DNS e DHCP aos hóspedes. Ele faz proxy de requisições DNS ao servidor DNS configurado na Availability Zone.

## 13.17. VPN

Donos de contas no CloudStack podem criar redes privadas virtuais (VPN) para acessar suas máquinas virtuais. Se a rede hóspede é instanciada de uma oferta de rede que oferece o serviço de acesso remoto por VPN, o roteador virtual (baseado na máquina virtual de sistema) é usado para prover o serviço. O CloudStack provê um serviço de acesso remoto por VPN baseado em L2TP-over-IPsec para redes virtuais hóspedes. Como cada rede obtém seu próprio roteador virtual, as VPNs não são compartilhadas pelas redes. Clientes VPN nativos em Windows, Mac OS X e iOS podem ser usados para conectar às redes hóspedes. O dono da conta pode criar e gerenciar usuários para suas VPNs. O CloudStack não usa seu database de contas com este propósito, mas usa uma tabela distinta. O database de usuários de VPN é compartilhado por todas as VPNs criadas pelo dono da conta. Todos os usuários de VPN obtêm acesso a todas as VPNs criadas pelo dono da conta.



### Nota

Certifique-se de que nem todo tráfego passa pela VPN. Isto é, a rota estabelecida pela VPN deve ser apenas para a rede hóspede e não para todo o tráfego.

- ▶ **Road Warrior / Remote Access.** Usuários desejam ser capazes de se conectar com segurança de casa ou do escritório a uma rede privada na nuvem. Tipicamente, o endereço IP do cliente que se conecta é dinâmico e não pode ser pré-configurado no servidor VPN.
- ▶ **Site to Site.** In this scenario, two private subnets (for example, an office network) is connected through a gateway to the network in the cloud. The address of the user's gateway must be preconfigured on the VPN server in the cloud. Note that although L2TP-over-IPsec can be used to set up Site-to-Site VPNs, this is not the primary intent of this feature. For more information, see [Seção 13.17.4, "Configurando uma conexão VPN Site-to-Site"](#)


### 13.17.1. Configurando VPN

Para configurar VPN para a nuvem:

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, clique em Global Settings.
3. Configure os seguintes parâmetros de configuração global.
  - ▶ 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 – Tamanho da chave IPsec.
  - ▶ remote.access.vpn.user.limit – Número máximo de usuários VPN por conta.

Para habilitar VPN para uma rede em particular:

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, clique em Network.
3. Clique no nome da rede com a qual você quer trabalhar.
4. Clique em View IP Addresses.
5. Clique em um dos endereços IP apresentados.

6. Click the Enable VPN button. 

A chave IPsec é apresentada em uma janela popup.

### 13.17.2. Usando VPN com Windows

O procedimento para usar VPN varia de acordo com a versão do Windows. Geralmente, o usuário deve editar as propriedades da VPN e certificar-se de que a rota default não é a VPN. Os passos seguintes são para clientes Windows L2TP no Windows Vista. Os comandos devem ser similares para outras versões do Windows.

1. Faça login na interface de usuário do CloudStack e clique no IP NAT de origem para a conta. A aba VPN deve exibir a chave IPsec pré-compartilhada. Tome nota disto e do IP NAT de origem. A interface de usuário também lista um ou mais usuários e suas senhas. Escolha um destes usuários ou, se nenhum existe, adicione um usuário e uma senha.
2. No Windows, vá para o Painel de Controle, selecione Centro de Rede e Compartilhamento. Clique em Configurar uma conexão ou uma rede.
3. No próximo diálogo, selecione Conectar a um local de trabalho.
4. No próximo diálogo, selecione Use minha conexão com a Internet (VPN).
5. In the next dialog, enter the source NAT IP from step [1](#) and give the connection a name. Check Don't connect now.
6. In the next dialog, enter the user name and password selected in step [1](#).
7. Clique em Create.

8. Volte ao painel de Controle e clique em Conexões de Rede para ver a nova conexão. A conexão ainda não está ativa.
9. Clique com o botão da direita na nova conexão e selecione Propriedades. No diálogo de Propriedades, selecione a aba Rede.
10. In Type of VPN, choose L2TP IPsec VPN, then click IPsec settings. Select Use preshared key. Enter the preshared key from Step [1](#).
11. A conexão está pronta para ser ativada. Volte a Painel de Controle -> Conexões de Rede e dê dois cliques na conexão criada.
12. Enter the user name and password from Step [1](#).

### 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. Configurando uma conexão VPN Site-to-Site

Uma conexão VPN Site-to-Site o ajuda a estabelecer uma conexão segura de um centro de dados empresarial à infraestrutura de nuvem. Isto permite o acesso de usuários a máquinas virtuais hóspedes estabelecendo uma conexão VPN de um equipamento no centro de dados da empresa ao roteador virtual da conta . Possuindo este recurso é eliminada a necessidade de estabelecer conexões VPN a máquinas virtuais individuais.

Os terminais suportados nos centros de dados remotos são:

- » Cisco ISR com IOS 12.4 ou posterior
- » Roteadores Juniper J-Series com JunOS 9.5 ou posterior



#### Nota

Adicionalmente aos equipamentos Cisco e Juniper específicos listados acima, a expectativa é que qualquer equipamento Cisco ou Juniper executando os sistemas operacionais suportados sejam capazes de estabelecer conexões VPN.

Para configurar uma conexão VPN Site-to-Site, execute o seguinte:

1. Crie uma Virtual Private Cloud (VPC).  
Veja [Seção 13.19, "Configuring a Virtual Private Cloud"](#).
2. Crie um VPN Customer Gateway.
3. Crie um VPN gateway para a VPC que você criou.
4. Crie uma conexão VPN do VPN gateway da VPC para o customer VPN gateway.



#### Nota

Appropriate events are generated on the CloudStack UI when status of a Site-to-Site VPN connection changes from connected to disconnected, or vice versa. Currently no events are generated when establishing a VPN connection fails or pending.

#### 13.17.4.1. Creating and Updating a VPN Customer Gateway



#### Nota

A VPN customer gateway can be connected to only one VPN gateway at a time.

To add a VPN Customer Gateway:

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.

3. In the Select view, select VPN Customer Gateway.
4. Click Add site-to-site VPN.

Forneça as seguintes informações:

- **Name:** A unique name for the VPN customer gateway you create.
- **Gateway:** The IP address for the remote gateway.
- **CIDR list:** The guest CIDR list of the remote subnets. Enter a CIDR or a comma-separated list of CIDRs. Ensure that a guest CIDR list is not overlapped with the VPC's CIDR, or another guest CIDR. The CIDR must be RFC1918-compliant.
- **IPsec Preshared Key:** Preshared keying is a method where the endpoints of the VPN share a secret key. This key value is used to authenticate the customer gateway and the VPC VPN gateway to each other.

#### Nota

The IKE peers (VPN end points) authenticate each other by computing and sending a keyed hash of data that includes the Preshared key. If the receiving peer is able to create the same hash independently by using its Preshared key, it knows that both peers must share the same secret, thus authenticating the customer gateway.

- **IKE Encryption:** The Internet Key Exchange (IKE) policy for phase-1. The supported encryption algorithms are AES128, AES192, AES256, and 3DES. Authentication is accomplished through the Preshared Keys.

#### Nota

The phase-1 is the first phase in the IKE process. In this initial negotiation phase, the two VPN endpoints agree on the methods to be used to provide security for the underlying IP traffic. The phase-1 authenticates the two VPN gateways to each other, by confirming that the remote gateway has a matching Preshared Key.

- **IKE Hash:** The IKE hash for phase-1. The supported hash algorithms are SHA1 and MD5.
- **IKE DH:** A public-key cryptography protocol which allows two parties to establish a shared secret over an insecure communications channel. The 1536-bit Diffie-Hellman group is used within IKE to establish session keys. The supported options are None, Group-5 (1536-bit) and Group-2 (1024-bit).
- **ESP Encryption:** Encapsulating Security Payload (ESP) algorithm within phase-2. The supported encryption algorithms are AES128, AES192, AES256, and 3DES.

## Nota

The phase-2 is the second phase in the IKE process. The purpose of IKE phase-2 is to negotiate IPSec security associations (SA) to set up the IPSec tunnel. In phase-2, new keying material is extracted from the Diffie-Hellman key exchange in phase-1, to provide session keys to use in protecting the VPN data flow.

- ▶ **ESP Hash:** Encapsulating Security Payload (ESP) hash for phase-2. Supported hash algorithms are SHA1 and MD5.
- ▶ **Perfect Forward Secrecy:** Perfect Forward Secrecy (or PFS) is the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised. This property enforces a new Diffie-Hellman key exchange. It provides the keying material that has greater key material life and thereby greater resistance to cryptographic attacks. The available options are None, Group-5 (1536-bit) and Group-2 (1024-bit). The security of the key exchanges increase as the DH groups grow larger, as does the time of the exchanges.

## Nota

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. Clique em 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. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. In the Select view, select VPN 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. Clique em OK.

### 13.17.4.2. Criando um gateway VPN para o VPC

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.  
Todas as VPCs que você criou para a conta são listadas na página.
4. Clique no botão Configure da VPC na qual você deseja implementar as máquinas virtuais.  
Na página VPC apresentada, todas as camadas que você criou são listadas em um diagrama.
5. Clique no ícone Settings.

As seguintes opções são apresentadas.

- ▶ Endereços IP
- ▶ Gateways
- ▶ Site-to-Site VPN
- ▶ Network ACLs

6. Selecione Site-to-Site VPN.

Se você está criando o gateway VPN pela primeira vez, selecionando Site-to-Site VPN requer de você criar um gateway VPN.

7. No diálogo de confirmação, clique Yes para confirmar.

Em poucos momentos, o gateway VPN é criado. Você será solicitado ver os detalhes do gateway VPN que você criou. Clique Yes para confirmar.

Os seguintes detalhes são apresentados na página VPN Gateway:

- ▶ Endereço IP
- ▶ Conta
- ▶ Domínio

### 13.17.4.3. Criando uma conexão VPN





1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.  
Todas as VPCs que você cria para a conta são listadas na página.
4. Clique no botão Configure da VPC na qual você deseja implementar as máquinas virtuais.  
Na página VPC apresentada, todas as camadas que você criou são listadas em um diagrama.
5. Clique no ícone Settings.  
As seguintes opções são apresentadas.
  - » IP Addresses
  - » Gateways
  - » Site-to-Site VPN
  - » Network ACLs
6. Selecione Site-to-Site VPN.  
Apágina Site-to-Site VPN é apresentada.
7. Na lista suspensa Select View, certifique-se de que VPN Connection é selecionada.
8. Clique em Create VPN Connection.  
O diálogo Create VPN Connection é apresentado:



9. Selecione o gateway desejado, então clique OK para confirmar.  
Em poucos momentos, a conexão VPN é apresentada.  
A seguinte informação sobre a conexão VPN é apresentada:
  - » Endereço IP
  - » Gateway
  - » Estado
  - » Chave IPsec pré compartilhada
  - » Política IKE
  - » Política ESP

#### 13.17.4.4. Reiniciando e removendo uma conexão VPN

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
  2. Na barra de navegação à esquerda, selecione Network.
  3. Na view Select, selecione VPC.  
Todas as VPCs que você criou para a conta são listadas na página.
  4. Clique no botão Configure da VPC na qual você deseja implementar as máquinas virtuais.  
Na página VPC apresentada, todas as camadas que você criou são listadas em um diagrama.
  5. Clique no ícone Settings.  
As seguintes opções são apresentadas.
    - » Endereços IP
    - » Gateways
    - » Site-to-Site VPN
    - » Network ACLs
  6. Selecione Site-to-Site VPN.  
Apágina Site-to-Site VPN é apresentada.
  7. Na lista suspensa Select View, certifique-se de que VPN Connection é selecionada.  
Todas as conexões VPN que você criou são apresentadas.
  8. Selecione a conexão VPN com a qual você quer trabalhar.  
Aba Details é apresentada.
  9. Para remover uma conexão VPN, clique no botão Delete VPN connection 
- Para reiniciar uma conexão VPN, clique no botão Reset VPN connection presente na aba Details. 

## 13.18. About Inter-VLAN Routing

Inter-VLAN Routing is the capability to route network traffic between VLANs. This feature enables you to build Virtual Private Clouds (VPC), an isolated segment of your cloud, that can hold multi-tier applications. These tiers are deployed on different VLANs that can communicate with each other. You provision VLANs to the tiers you create, and VMs can be deployed on different tiers. The VLANs are connected to a virtual router, which facilitates communication between the VMs. In effect, you can segment VMs by means of VLANs into different networks that can host multi-tier applications. such

as Web, Application, or Database. Such segmentation by means of VLANs logically separate application VMs for higher security and lower broadcasts, while remaining physically connected to the same device.

This feature is supported on XenServer and VMware hypervisors.

The major advantages are:

- ▶ The administrator can deploy a set of VLANs and allow users to deploy VMs on these VLANs. A guest VLAN is randomly allotted to an account from a pre-specified set of guest VLANs. All the VMs of a certain tier of an account reside on the guest VLAN allotted to that account.

**Nota**

A VLAN allocated for an account cannot be shared between multiple accounts.

- ▶ The administrator can allow users to create their own VPC and deploy the application. In this scenario, the VMs that belong to the account are deployed on the VLANs allotted to that account.
- ▶ Both administrators and users can create multiple VPCs. The guest network NIC is plugged to the VPC virtual router when the first VM is deployed in a tier.
- ▶ The administrator can create the following gateways to send to or receive traffic from the VMs:
  - VPN Gateway:** For more information, see [Seção 13.17.4.2, "Criando um gateway VPN para o VPC"](#).
  - Public Gateway:** The public gateway for a VPC is added to the virtual router when the virtual router is created for VPC. The public gateway is not exposed to the end users. You are not allowed to list it, nor allowed to create any static routes.
  - Private Gateway:** For more information, see [Seção 13.19.5, "Adicionando um gateway privado a uma VPC"](#).
- ▶ Both administrators and users can create various possible destinations-gateway combinations. However, only one gateway of each type can be used in a deployment.

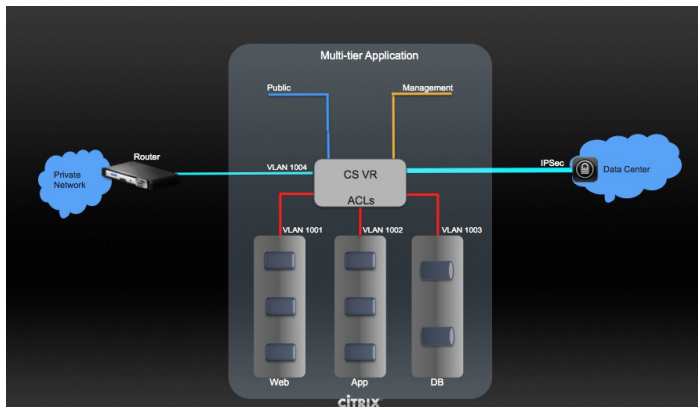
For example:

**VLANs and Public Gateway:** For example, an application is deployed in the cloud, and the Web application VMs communicate with the Internet.

**VLANs, VPN Gateway, and Public Gateway:** For example, an application is deployed in the cloud; the Web application VMs communicate with the Internet; and the database VMs communicate with the on-premise devices.

- ▶ The administrator can define Access Control List (ACL) on the virtual router to filter the traffic among the VLANs or between the Internet and a VLAN. You can define ACL based on CIDR, port range, protocol, type code (if ICMP protocol is selected) and Ingress/Egress type.

The following figure shows the possible deployment scenarios of a Inter-VLAN setup:



To set up a multi-tier Inter-VLAN deployment, see [Seção 13.19, "Configuring a Virtual Private Cloud"](#).

## 13.19. Configuring a Virtual Private Cloud

### 13.19.1. About Virtual Private Clouds

CloudStack Virtual Private Cloud is a private, isolated part of CloudStack. A VPC can have its own virtual network topology that resembles a traditional physical network. You can launch VMs in the virtual network that can have private addresses in the range of your choice, for example: 10.0.0.0/16. You can define network tiers within your VPC network range, which in turn enables you to group similar kinds of instances based on IP address range.

For example, if a VPC has the private range 10.0.0.0/16, its guest networks can have the network ranges 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, and so on.

#### Major Components of a VPC:

A VPC is comprised of the following network components:

- ▶ **VPC:** A VPC acts as a container for multiple isolated networks that can communicate with each other via its virtual router.
- ▶ **Network Tiers:** Each tier acts as an isolated network with its own VLANs and CIDR list, where you can place groups of resources, such as VMs. The tiers are segmented by means of VLANs. The NIC of each tier acts as its gateway.
- ▶ **Virtual Router:** A virtual router is automatically created and started when you create a VPC. The virtual router connect

- **Virtual Router:** A virtual router is automatically created and started when you create a VPC. The virtual router connects the tiers and directs traffic among the public gateway, the VPN gateways, and the NAT instances. For each tier, a corresponding NIC and IP exist in the virtual router. The virtual router provides DNS and DHCP services through its IP.
- **Public Gateway:** The traffic to and from the Internet routed to the VPC through the public gateway. In a VPC, the public gateway is not exposed to the end user; therefore, static routes are not supported for the public gateway.
- **Private Gateway:** All the traffic to and from a private network routed to the VPC through the private gateway. For more information, see [Seção 13.19.5, "Adicionando um gateway privado a uma VPC"](#).
- **VPN Gateway:** The VPC side of a VPN connection.
- **Site-to-Site VPN Connection:** A hardware-based VPN connection between your VPC and your datacenter, home network, or co-location facility. For more information, see [Seção 13.17.4, "Configurando uma conexão VPN Site-to-Site"](#).
- **Customer Gateway:** The customer side of a VPN Connection. For more information, see [Seção 13.17.4.1, "Creating and Updating a VPN Customer Gateway"](#).
- **NAT Instance:** An instance that provides Port Address Translation for instances to access the Internet via the public gateway. For more information, see [Seção 13.19.9, "Habilitando ou desabilitando NAT estática em uma VPC"](#).

### Network Architecture in a VPC

In a VPC, the following four basic options of network architectures are present:

- VPC with a public gateway only
- VPC with public and private gateways
- VPC with public and private gateways and site-to-site VPN access
- VPC with a private gateway only and site-to-site VPN access

### Connectivity Options for a VPC

You can connect your VPC to:

- The Internet through the public gateway.
- The corporate datacenter by using a site-to-site VPN connection through the VPN gateway.
- Both the Internet and your corporate datacenter by using both the public gateway and a VPN gateway.

### VPC Network Considerations

Consider the following before you create a VPC:

- A VPC, by default, is created in the enabled state.
- A VPC can be created in Advance zone only, and can't belong to more than one zone at a time.
- The default number of VPCs an account can create is 20. However, you can change it by using the `max.account.vpcs` global parameter, which controls the maximum number of VPCs an account is allowed to create.
- The default number of tiers an account can create within a VPC is 3. You can configure this number by using the `vpc.max.networks` parameter.
- Each tier should have a unique CIDR in the VPC. Ensure that the tier's CIDR should be within the VPC CIDR range.
- A tier belongs to only one VPC.
- All network tiers inside the VPC should belong to the same account.
- When a VPC is created, by default, a SourceNAT IP is allocated to it. The Source NAT IP is released only when the VPC is removed.
- A public IP can be used for only one purpose at a time. If the IP is a sourceNAT, it cannot be used for StaticNAT or port forwarding.
- The instances only have a private IP address that you provision. To communicate with the Internet, enable NAT to an instance that you launch in your VPC.
- Only new networks can be added to a VPC. The maximum number of networks per VPC is limited by the value you specify in the `vpc.max.networks` parameter. The default value is three.
- The load balancing service can be supported by only one tier inside the VPC.
- If an IP address is assigned to a tier:
  - That IP can't be used by more than one tier at a time in the VPC. For example, if you have tiers A and B, and a public IP1, you can create a port forwarding rule by using the IP either for A or B, but not for both.
  - That IP can't be used for StaticNAT, load balancing, or port forwarding rules for another guest network inside the VPC.
- Remote access VPN is not supported in VPC networks.

## 13.19.2. Adding a Virtual Private Cloud

When creating the VPC, you simply provide the zone and a set of IP addresses for the VPC network address space. You specify this set of addresses in the form of a Classless Inter-Domain Routing (CIDR) block.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.
4. Click Add VPC. The Add VPC page is displayed as follows:



Forneça as seguintes informações:

- ▶ **Name:** A short name for the VPC that you are creating.
- ▶ **Description:** A brief description of the VPC.
- ▶ **Zone:** Choose the zone where you want the VPC to be available.
- ▶ **Super CIDR for Guest Networks:** Defines the CIDR range for all the tiers (guest networks) within a VPC. When you create a tier, ensure that its CIDR is within the Super CIDR value you enter. The CIDR must be RFC1918 compliant.
- ▶ **DNS domain for Guest Networks:** If you want to assign a special domain name, specify the DNS suffix. This parameter is applied to all the tiers within the VPC. That implies, all the tiers you create in the VPC belong to the same DNS domain. If the parameter is not specified, a DNS domain name is generated automatically.

### 13.19.3. Adding Tiers

Tiers are distinct locations within a VPC that act as isolated networks, which do not have access to other tiers by default. Tiers are set up on different VLANs that can communicate with each other by using a virtual router. Tiers provide inexpensive, low latency network connectivity to other tiers within the VPC.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.

All the VPC that you have created for the account is listed in the page.



#### Nota

The end users can see their own VPCs, while root and domain admin can see any VPC they are authorized to see.

4. Click the Configure button of the VPC for which you want to set up tiers.  
The Add new tier dialog is displayed, as follows:

If you have already created tiers, the VPC diagram is displayed. Click Create Tier to add a new tier.

5. Especifique o seguinte:

All the fields are mandatory.

- ▶ **Name:** A unique name for the tier you create.
- ▶ **Network Offering:** The following default network offerings are listed: DefaultIsolatedNetworkOfferingForVpcNetworksNoLB, DefaultIsolatedNetworkOfferingForVpcNetworks. In a VPC, only one tier can be created by using LB-enabled network offering.
- ▶ **Gateway:** The gateway for the tier you create. Ensure that the gateway is within the Super CIDR range that you specified while creating the VPC, and is not overlapped with the CIDR of any existing tier within the VPC.
- ▶ **Netmask:** The netmask for the tier you create.  
For example, if the VPC CIDR is 10.0.0.0/16 and the network tier CIDR is 10.0.1.0/24, the gateway of the tier is

For example, if the VPC CIDR is 10.0.0.0/16 and the network tier CIDR is 10.0.1.0/24, the gateway of the tier is 10.0.1.1, and the netmask of the tier is 255.255.255.0.

6. Clique em OK.
7. Continue with configuring access control list for the tier.

### 13.19.4. Configuring Access Control List

Define Network Access Control List (ACL) on the VPC virtual router to control incoming (ingress) and outgoing (egress) traffic between the VPC tiers, and the tiers and Internet. By default, all incoming and outgoing traffic to the guest networks is blocked. To open the ports, you must create a new network ACL. The network ACLs can be created for the tiers only if the NetworkACL service is supported.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.

Todas as VPCs que você criou para a conta são listadas na página.

4. Clique no ícone Settings.

As seguintes opções são apresentadas.

- » Endereços IP
- » Gateways
- » Site-to-Site VPN
- » Network ACLs

5. Select Network ACLs.

The Network ACLs page is displayed.

6. Click Add Network ACLs.

To add an ACL rule, fill in the following fields to specify what kind of network traffic is allowed in this tier.

- » **CIDR:** The CIDR acts as the Source CIDR for the Ingress rules, and Destination CIDR for the Egress rules. To accept traffic only from or to the IP addresses within a particular address block, enter a CIDR or a comma-separated list of CIDRs. The CIDR is the base IP address of the incoming traffic. For example, 192.168.0.0/22. To allow all CIDRs, set to 0.0.0.0/0.
- » **Protocol:** The networking protocol that sources use to send traffic to the tier. The TCP and UDP protocols are typically used for data exchange and end-user communications. The ICMP protocol is typically used to send error messages or network monitoring data.
- » **Start Port, End Port** (TCP, UDP only): A range of listening ports that are the destination for the incoming traffic. If you are opening a single port, use the same number in both fields.
- » **Select Tier:** Select the tier for which you want to add this ACL rule.
- » **ICMP Type, ICMP Code** (ICMP only): The type of message and error code that will be sent.
- » **Traffic Type:** Select the traffic type you want to apply.

**Egress:** To add an egress rule, select Egress from the Traffic type drop-down box and click Add. This specifies what type of traffic is allowed to be sent out of VM instances in this tier. If no egress rules are specified, all traffic from the tier is allowed out at the VPC virtual router. Once egress rules are specified, only the traffic specified in egress rules and the responses to any traffic that has been allowed in through an ingress rule are allowed out. No egress rule is required for the VMs in a tier to communicate with each other.

**Ingress:** To add an ingress rule, select Ingress from the Traffic type drop-down box and click Add. This specifies what network traffic is allowed into the VM instances in this tier. If no ingress rules are specified, then no traffic will be allowed in, except for responses to any traffic that has been allowed out through an egress rule.

Nota

By default, all incoming and outgoing traffic to the guest networks is blocked. To open the ports, create a new network ACL.

7. Click Add. The ACL rule is added.

To view the list of ACL rules you have added, click the desired tier from the Network ACLs page, then select the Network ACL tab.

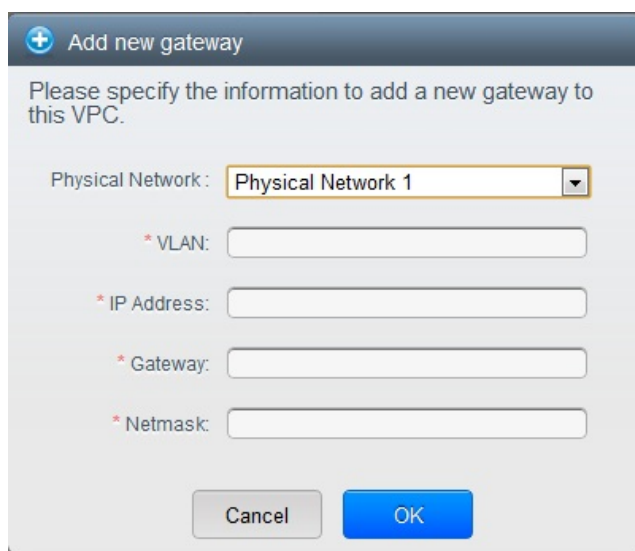
Network Details		Network ACL				IP Addresses			
CIDR	Protocol	Start Port	End Port	ICMP Type	ICMP Code	Traffic type	Add rule	Actions	
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>			Ingress	Add		
0.0.0.0/0	TCP	1	65535			Ingress			
0.0.0.0/0	TCP	1	65535			Egress			
0.0.0.0/0	ICMP			-1	-1	Egress			
0.0.0.0/0	ICMP			-1	-1	Ingress			

You can edit the tags assigned to the ACL rules and delete the ACL rules you have created. Click the appropriate button in the Actions column.

### 13.19.5. Adicionando um gateway privado a uma VPC

Um gateway privado somente pode ser adicionado pelo administrador root. A rede privada da VPC tem uma relação 1:1 com a NIC da rede física. Nenhum gateway com VLAN e IP duplicado é permitido no mesmo centro de dados.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.  
Todas as VPCs que você criou para a conta são listadas na página.
4. Clique no botão Configure da VPC na qual você deseja configurar regras de balanceamento de carga.  
Na página VPC apresentada, todas as camadas que você criou são listadas em um diagrama.
5. Clique no ícone Settings.  
As seguintes opções são apresentadas.
  - » Endereços IP
  - » Private Gateways
  - » Site-to-Site VPN
  - » Network ACLs
6. Selecione Private Gateways.  
A página Gateways é apresentada.
7. Clique em Add new gateway:



The screenshot shows a dialog box titled "Add new gateway". The main text says "Please specify the information to add a new gateway to this VPC." Below this, there are four input fields: "Physical Network:" with a dropdown menu showing "Physical Network 1"; "\* VLAN:"; "\* IP Address:"; "\* Gateway:"; and "\* Netmask:". At the bottom, there are two buttons: "Cancel" and "OK".

8. Especifique o seguinte:
    - » **Physical Network:** A rede física que você criou na zona.
    - » **IP Address:** O endereço IP associado com o gateway VPC.
    - » **Gateway:** O gateway através do qual o tráfego é roteado de e para a VPC.
    - » **Netmask:** A máscara de rede associada com o gateway VPC.
    - » **VLAN:** A VLAN associada com o gateway VPC.
- O novo gateway aparece na lista. Você pode repetir estes passo para adicionar mais gateways para esta VPC.

### 13.19.6. Implantando máquinas virtuais na camada

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.  
Todas as VPCs que você criou para a conta são listadas na página.
4. Clique no botão Configure da VPC na qual você deseja implementar as máquinas virtuais.  
Na página VPC apresentada, todas as camadas que você criou são listadas.
5. Clique no botão Add VM da camada a qual você deseja adicionar uma máquina virtual.  
A página Add Instance é apresentada.  
Siga as instruções na tela para adicionar uma instância. Para informações sobre adição de uma instância, veja a seção Adicionando instâncias no Guia de Instalação.

### 13.19.7. Obtendo um novo endereço IP para uma VPC

Quando você obtém um endereço IP, todos os endereços IP são alocados à VPC, não às redes hóspedes na VPC. Os IPs são associados à rede hóspede somente quando a primeira regra de port-forwarding, balanceamento de carga ou NAT estática é criada para o IP ou para a rede. Um IP não pode ser associado a mais de uma rede de cada vez.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.  
Todas as VPCs que você criou para a conta são listadas na página.
4. Clique no botão Configure da VPC na qual você deseja implementar as máquinas virtuais.

Na página VPC apresentada, todas as camadas que você criou são listadas em um diagrama.

5. Clique no ícone Settings.

As seguintes opções são apresentadas.

- » Endereços IP
- » Gateways
- » Site-to-Site VPN
- » Network ACLs

6. Selecione IP Addresses.

A página IP Addresses é apresentada.

7. Clique em Acquire New IP, e clique Yes no diálogo de confirmação.

Você deve confirmar porque, tipicamente, endereços IP são um recurso limitado. Em alguns momentos, o novo endereço IP deve aparecer no estado Allocated. Agora você pode usar o endereço IP no encaminhamento de porta, balanceamento de carga, ou regras NAT estáticas.

### 13.19.8. Liberando um endereço IP atribuído a uma VPC

O endereço IP é um recurso limitado. Se você não precisa mais de um IP particular, você pode desassociá-lo de sua VPC e retorná-lo ao pool de endereços disponíveis. Um endereço IP pode ser liberado de sua camada somente quando todas as rede de rede (port forwarding, balanceamento de carga, ou NAT estática) são removidas para este endereço IP. O endereço IP liberado ainda irá pertencer à mesma VPC.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.

2. Na barra de navegação à esquerda, selecione Network.

3. Na view Select, selecione VPC.

Todas as VPCs que você criou para a conta são listadas na página.

4. Clique no botão Configure da VPC da qual você deseja liberar o IP.

Na página VPC apresentada, todas as camadas que você criou são listadas em um diagrama.

5. Clique no ícone Settings.


As seguintes opções são apresentadas.

- » Endereços IP
- » Gateways
- » Site-to-Site VPN
- » Network ACLs

6. Selecione IP Addresses.

A página IP Addresses é apresentada.

7. Clique no IP que você deseja liberar.

8. Na aba Details, clique no botão Release IP 

### 13.19.9. Habilitando ou desabilitando NAT estática em uma VPC

Uma regra NAT estática mapeia um endereço IP público para o endereço IP privado de uma máquina virtual em uma VPC para permitir tráfego da Internet para ela. Esta seção informa como habilitar ou desabilitar NAT estática para um endereço IP em particular em uma VPC.

Se regras de encaminhamento de portas já estão em efeito para um endereço IP, você não pode habilitar NAT estática para este IP.

Se uma máquina virtual hóspede faz parte de mais de uma rede, regras de NAT estática funcionarão somente se elas estão definidas na rede default.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.

2. Na barra de navegação à esquerda, selecione Network.

3. Na view Select, selecione VPC.

Todas as VPCs que você criou para a conta são listadas na página.

4. Clique no botão Configure da VPC na qual você deseja implementar as máquinas virtuais.

Na página VPC apresentada, todas as camadas que você criou são listadas em um diagrama.

5. Clique no ícone Settings.


As seguintes opções são apresentadas.

- » Endereços IP
- » Gateways
- » Site-to-Site VPN
- » Network ACLs

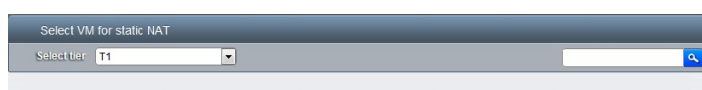
6. Selecione IP Addresses.

A página IP Addresses é apresentada.

7. Clique no IP com o qual você deseja trabalhar.

8. Na aba Details, clique no botão Static NAT.  O botão alterna entre Enable e Disable, dependendo se NAT estática está habilitada ou não para o endereço IP.

9. Se você está habilitando NAT estática, um diálogo é apresentado como se segue:



Display name	Internal name	Zone name	State	Select
T1-VM1	i2-4-VM	zone1	 Running	<input type="radio"/>

Cancel

10. Selecione a camada e a máquina virtual de destino, e então clique em Apply.

### 13.19.10. Adicionando regras de balanceamento de carga em uma VPC

Um usuário ou administrador do CloudStack pode criar regras de balanceamento de carga que distribuem o tráfego recebido em um endereço IP público por uma ou mais máquinas virtuais que pertencem a uma camada de rede que provê serviço de balanceamento de carga em uma VPC. Um usuário cria uma regra, especifica um algoritmo e assinala a regra a um conjunto de máquinas virtuais em uma VPC.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.  
Todas as VPCs que você criou para a conta são listadas na página.
4. Clique no botão Configure da VPC na qual você deseja configurar regras de balanceamento de carga.  
Na página VPC apresentada, todas as camadas que você criou são listadas em um diagrama.
5. Clique no ícone Settings.  
As seguintes opções são apresentadas.
  - » IP Addresses
  - » Gateways
  - » Site-to-Site VPN
  - » Network ACLs
6. Selecione IP Addresses.  
A página IP Addresses é apresentada.
7. Clique no endereço IP para o qual você deseja criar a regra, então clique na aba Configuration.
8. No nó Load Balancing do diagrama, clique em View All.
9. Selecione a camada para a qual você deseja aplicar a regra.



#### Nota

Em uma VPC, o serviço de balanceamento de carga é suportado somente em uma única camada.

10. Especifique o seguinte:
  - » **Name:** Um nome para a regra de balanceamento de carga.
  - » **Public Port:** A porta que recebe o tráfego entrante a ser balanceado.
  - » **Private Port:** A porta que as máquinas virtuais usarão para receber o tráfego.
  - » **Algorithm.** Escolha o algoritmo de balanceamento de carga que você deseja que o CloudStack use. O CloudStack suporta os seguintes algoritmos bem conhecidos:
    - Round-robin
    - Menos conexões
    - Origem
  - » **Stickiness.** (Opcional) Clique Configure e escolha o algoritmo para a política de afinidade. Veja Sticky Session Policies for Load Balancer Rules.
  - » **Add VMs:** Clique em Add VMs, então selecione duas ou mais máquinas virtuais que irão dividir a carga do tráfego entrante, e clique em Apply.

A nova regra de balanceamento de carga aparece na lista. Você pode repetir estes passos para adicionar mais regras de balanceamento de carga para este endereço IP.

### 13.19.11. Adicionando uma regra de encaminhamento de porta em uma VPC

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.  
Todas as VPCs que você criou para a conta são listadas na página.
4. Clique no botão Configure da VPC na qual você deseja implementar as máquinas virtuais.  
Na página VPC apresentada, todas as camadas que você criou são listadas em um diagrama.
5. Clique no ícone Settings.  
As seguintes opções são apresentadas.
  - » Endereços IP
  - » Gateways
  - » Site-to-Site VPN
  - » Network ACLs
6. Escolha um endereço IP existente ou obtenha um novo endereço IP. Clique no nome do endereço IP na lista.  
A página IP Addresses é apresentada.
7. Clique no endereço IP para o qual você deseja criar a regra, então clique na aba Configuration.
8. No nó Port Forwarding do diagrama, clique em View All.
9. Selecione a camada para a qual você deseja aplicar a regra.



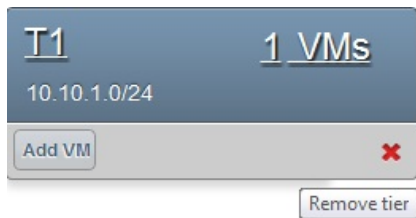
10. Especifique o seguinte:

- ▶ **Public Port:** A porta para a qual tráfego público será encaminhado no endereço IP que você obteve no passo anterior.
- ▶ **Private Port:** A porta na qual a instância está ouvindo por tráfego público encaminhado.
- ▶ **Protocol:** O protocolo de comunicações em uso entre as duas portas.
  - TCP
  - UDP
- ▶ **Add VM:** Clique em Add VM. Selecione o nome da instância a qual esta regra se aplica, e clique Apply. Você pode testar a regra abrindo uma sessão ssh com a instância.

### 13.19.12. Removing Tiers

You can remove a tier from a VPC. A removed tier cannot be revoked. When a tier is removed, only the resources of the tier are expunged. All the network rules (port forwarding, load balancing and staticNAT) and the IP addresses associated to the tier are removed. The IP address still be belonging to the same VPC.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.
  - All the VPC that you have created for the account is listed in the page.
4. Click the Configure button of the VPC for which you want to set up tiers.
  - The Configure VPC page is displayed. Locate the tier you want to work with.
5. Click the Remove VPC button:



Wait for some time for the tier to be removed.

### 13.19.13. Editing, Restarting, and Removing a Virtual Private Cloud



#### Nota

Ensure that all the tiers are removed before you remove a VPC.

1. Faça login na interface de usuário do CloudStack como administrador ou usuário final.
2. Na barra de navegação à esquerda, selecione Network.
3. Na view Select, selecione VPC.
  - Todas as VPCs que você criou para a conta são listadas na página.
4. Select the VPC you want to work with.
5. To remove, click the Remove VPC button

You can edit the name and description of a VPC. To do that, select the VPC, then click the Edit button.

To restart a VPC, select the VPC, then click the Restart button.

## 13.20. Persistent Networks

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.  
See the *Administration Guide*.
2. Select Network from the left navigation pane.
3. Select the guest network that you want to offer this network service to.
4. Click the Edit button.
5. From the Network Offering drop-down, select the persistent network offering you have just created.
6. Click on OK.

## Revision History

**Revisão 1-0**      **October 5 2012**      **Jessica Tomechak, Radhika PC, Wido den Hollander**  
Initial publication