CloudStack  
New Features Overview

For CloudStack Version 3.0

Revised February 17, 2012

**A note to our readers**

This document is a draft of work in progress for a future release of ClouStack. It is not ready for publication. It may have errors, omissions, and descriptions of features that will not appear in the released software. The draft is provided for those who want an early look at work in progress for the next upcoming release of CloudStack, with the understanding that the documentation is subject to change, including major revision or removal. Distribution is not recommended.

© 2011, 2012 Citrix Systems, Inc. All rights reserved. Specifications are subject to change without notice. Citrix Systems, Inc., the Citrix logo, Citrix XenServer, Citrix XenCenter, and CloudStack are trademarks or registered trademarks of Citrix Systems, Inc. All other brands or products are trademarks or registered trademarks of their respective holders.

Contents

[What's In This Guide 3](#_Toc317205026)

[NetScaler Load Balancer 4](#_Toc317205027)

[Sticky Session Policies for External Load Balancers 5](#_Toc317205028)

[Using an LDAP Server for User Authentication 5](#_Toc317205029)

[VM Storage Migration 6](#_Toc317205030)

[Swift for Secondary Storage 6](#_Toc317205031)

[Password and Key Encryption 7](#_Toc317205032)

[Security Group Egress Rules 7](#_Toc317205033)

[Using Projects to Organize Users and Resources 8](#_Toc317205034)

[Providing Network Services for Users 9](#_Toc317205035)

[About Physical Networks 9](#_Toc317205036)

[Configurable Characteristics of Physical Networks 10](#_Toc317205037)

[About Virtual Networks 10](#_Toc317205038)

[Isolated Networks 10](#_Toc317205039)

[Shared Networks 11](#_Toc317205040)

[Runtime Allocation of Virtual Network Resources 11](#_Toc317205041)

[Network Service Providers 11](#_Toc317205042)

[Supported Network Service Providers 11](#_Toc317205043)

[Network Offerings 12](#_Toc317205044)

# What's In This Guide

CloudStack 3.0 introduces several new features. This Beta document provides overviews and concepts for these new features. Detailed instructions for using the features will be provided in the final documentation with the CloudStack 3.0 release.

# NetScaler Load Balancer

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

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

The functional behavior of the NetScaler with CloudStack is the same as described in the CloudStack documentation for using an F5 external load balancer, which was the only supported type of external load balancer in previous CloudStack versions. The only exception is that the F5 supports routing domains, and NetScaler does not; however, the same effect can be achieved by using the NetScaler in-line with a Juniper SRX firewall. NetScaler can not yet be used as a firewall.

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

|  |  |  |
| --- | --- | --- |
| **NetScaler ADC Type** | **Description of Capabilities** | **CloudStack 3.0 Supported Features** |
| MPX | Physical appliance. Capable of deep packet inspection. Can act as application firewall and load balancer. | In advanced zones, load balancer functionality fully supported without limitation. In basic zones, static NAT, elastic IP (EIP), and elastic load balancing (ELB) are also provided. |
| VPX | Virtual appliance. Can run as VM on XenServer, ESXi, and Hyper-V hypervisors. Same functionality as MPX. | Supported only on ESXi. Same functional support as for MPX. CloudStack will treat VPX and MPX as the same device type. |
| SDX | Physical appliance. Can create multiple fully isolated VPX instances on a single appliance to support multi-tenant usage. | Cloudstack will dynamically provision, configure, and manage the lifecycle of VPX instances on the SDX. Provisioned instances are added into CloudStack automatically – no manual configuration by the administrator is required. Once a VPX instance is added into CloudStack, it is treated the same as a VPX on an ESXi host. |

# Sticky Session Policies for External Load Balancers

CloudStack 3.0 supports sticky session policies for NetScaler and F5 external load balancers.

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.

Citrix NetScaler supports sticky sessions by allowing you to direct all requests from a single user session to the same backend server, where the user’s persistent session data is stored. This overrides the typical load balancer behavior, which would assign each new request to any available server that best balances the load, without regard to which user made the request.

CloudStack integrates the NetScaler’s sticky session capability. 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, and they are the same parameters you will find in NetScaler documentation for stickiness policies. 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.

# Using an LDAP Server for User Authentication

In CloudStack 3.0, you can use an external LDAP server such as Microsoft Active Directory or ApacheDS for end-user authentication. Just map CloudStack accounts to the corresponding LDAP accounts using a query filter. The query filter is written using the query syntax of the particular LDAP server, and can include special wildcard characters provided by CloudStack for matching common values such as the user’s email address and name. CloudStack will search the external LDAP directory tree starting at a specified base directory and return the distinguished name (DN) and password of the matching user. This information along with the given password is used to authenticate the user.

To set up LDAP authentication in CloudStack, provide the following:

* Hostname or IP address and listening port of the LDAP server and whether SSL is used
* Search user DN credentials, which give CloudStack permission to search on the LDAP server
* Base directory and query filter

For more about query filter syntax, consult the documentation for your LDAP server. The CloudStack wildcards are:

|  |  |
| --- | --- |
| %u | Account name |
| %e | Email address |
| %n | First and last name |

# VM Storage Migration

The CloudStack administrator can move a virtual machine’s root disk volume or any additional data disk from one storage pool to another in the same zone. You can use the storage migration feature to achieve some commonly desired administration goals, such as balancing the load on storage pools and increasing the reliability of virtual machines by moving them away from any storage pool that is experiencing issues. This functionality is supported in XenServer, KVM, and VMware.

When migrating the root disk volume, the VM must first be stopped, and there must be no data disks attached. During storage migration, users can not access the VM. After migration is complete, the VM must be restarted.

When migrating a data disk, it must first be detached from the VM. After migration, the disk can be re-attached to any desired VM running in the same cluster as the new storage server.

# Swift for Secondary Storage

In previous versions of CloudStack, NFS storage is supported for secondary storage. In CloudStack 3.0, OpenStack Object Storage (Swift, <http://swift.openstack.org>) is also supported for secondary storage.

When using Swift, you still set up NFS secondary storage for each zone as usual, then configure Swift storage for the entire CloudStack. The NFS storage in each zone acts as a staging area through which all templates and other secondary storage data pass before being forwarded to Swift. The Swift storage acts as a cloud-wide resource, making templates and other data available to any zone in the cloud. There is no hierarchy in the Swift storage, just one Swift container per storage object. Any secondary storage in the whole cloud can pull a container from Swift at need – no more copying templates and snapshots from one zone to another. Everything is available everywhere.

# Password and Key Encryption

CloudStack stores several sensitive passwords and secret keys that are used to provide security. Starting in CloudStack 3.0, these values are always automatically encrypted:

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

CloudStack 3.0 uses the Java Simplified Encryption (JASYPT) library. The data values are encrypted and decrypted using a database secret key, which is stored in one of CloudStack’s internal properties files along with the database password. The other encrypted values listed above (SSH keys, etc.) are in the CloudStack internal database.

Of course, the database secret key itself can not be stored in the open – it must be encrypted. How then does CloudStack read it? A second secret key must be provided from an external source during Management Server startup. This key can be provided in one of two ways: loaded from a file or provided by the CloudStack administrator. The CloudStack database has a new configuration setting that lets it know which of these methods will be used. If the encryption type is set to “file,” the key must be in a file in a known location. If the encryption type is set to “web,” the administrator runs the utility com.cloud.utils.crypt.EncryptionSecretKeySender, which relays the key to the Management Server over a known port.

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

# Security Group Egress Rules

In a zone that uses basic networking, there is a single guest network for all guest VMs. Security groups can be used to control network traffic to and from the 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.

In addition to ingress rules that control incoming network traffic to VMs in a given security group, starting in CloudStack 3.0 you can also define egress rules to control outgoing network traffic .

Security groups must first be enabled for the zone. The administrator can do this with a single click through the CloudStack UI.

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.

You can set up egress rules through the CloudStack UI. Fill out the following fields to specify what type of traffic is allowed to be sent out of VM instances in this security group. If no egress rules are specified, then all traffic will be allowed out. Once egress rules are specified, the following types of traffic are allowed out: traffic specified in egress rules; queries to DNS servers; and responses to any traffic that has been allowed in through an ingress rule.

* Add by CIDR/Account. Indicate whether the destination of the traffic will be defined by IP address (CIDR) or an existing security group in a CloudStack account (Account). Choose Account if you want to allow outgoing traffic to all VMs in another security group.
* Protocol. The networking protocol that VMs will use to send outgoing traffic. TCP and UDP are typically used for data exchange and end-user communications. ICMP 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 will be sent.
* CIDR. (Add by CIDR only) To send traffic only to 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.
* Account, Security Group. (Add by Account only) To allow traffic to be sent to another security group, enter the CloudStack account and name of a security group that has already been defined in that account. To allow traffic between VMs within the security group you are editing now, enter its name.

# Using Projects to Organize Users and Resources

In CloudStack 3.0, users can group themselves into projects so they can collaborate and share virtual resources. CloudStack tracks usage per project as well as per user, so the usage can be billed to either a user account or a project. For example, a private cloud within a software company might have all members of the QA department assigned to one project, so the company can track the resources used in testing while the project members can more easily isolate their efforts from other users of the same cloud.

You can configure CloudStack to allow any user to create a new project, or you can restrict that ability to just CloudStack administrators. Once you have created a project, you become that project’s administrator, and you can add others within your domain to the project. CloudStack can be set up either so that you can add people directly to a project, or so that you have to send an invitation which the recipient must accept. Project members can view and manage all virtual resources created by anyone in the project (for example, share VMs). A user can be a member of any number of projects and can switch views in the CloudStack UI to show only project-related information, such as project VMs, fellow project members, project-related alerts, and so on.

The project administrator can pass on the role to another project member. The project administrator can also invite more users, remove users from the project, set new resource limits (as long as they are below the global defaults set by the CloudStack administrator), and delete the project. When the administrator removes a user from the project, resources created by that user, such as VM instances, remain with the project. This brings us to the subject of resource ownership and which resources can be used by a project.

Resources created within a project are owned by the project, not by any particular CloudStack account, and they can be used only within the project. A user who belongs to one or more projects can still create resources outside of those projects, and those resources belong to the user’s account; they will not be counted against the project’s usage or resource limits. You can create project-level networks to isolate traffic within the project and provide network services such as port forwarding, load balancing, VPN, and static NAT. A project can also make use of certain types of resources from outside the project, if those resources are shared. For example, a shared network or public template is available to any project in the domain. A project can get access to a private template if the template’s owner will grant permission. A project can use any service offering or disk offering available in its domain; however, you can not create private service and disk offerings at the project level.

# Providing Network Services for Users

People using cloud infrastructure have a variety of needs and preferences when it comes to the networking services provided by the cloud. Provisioning physical and virtual networks has always been supported in CloudStack. As a CloudStack 3.0 administrator, you can do the following additional things to set up networking for your users:

* Set up several different providers for the same service on a single physical network (for example, both Cisco and Juniper firewalls)
* Bundle different types of network services into network offerings, so users can choose the desired network services for any given virtual machine (see Network Offerings on page 12)
* Add new network offerings as time goes on so end users can upgrade to a better class of service on their network
* Provide more ways for a network to be accessed by a user, such as through a project of which the user is a member (see Using Projects to Organize Users and Resources on page 8)

## About Physical Networks

A physical network is the actual network hardware and wiring in a zone. A zone can have multiple physical networks. Before 3.0, the concept of a physical network was implied by a combination of zone configuration, global configuration parameters, and hypervisor configuration. In CloudStack 3.0, the physical network is more directly under the administrator’s control. An administrator can:

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

### Configurable Characteristics of Physical Networks

CloudStack provides configuration settings you can use to set up a physical network in a zone, including:

* What type of network traffic it carries (guest, public, management, storage)
* VLANs
* Unique name that the hypervisor can use to find that particular network
* Enabled or disabled. When a network is first set up, it is disabled – not in use yet. The administrator sets the physical network to enabled, and it begins to be used. The administrator can later disable the network again, which prevents any new virtual networks from being created on that physical network; the existing network traffic continues even though the state is disabled.
* Speed
* Tags, so network offerings can be matched to physical networks
* Isolation method

## About Virtual Networks

A virtual network is a logical construct that enables multi-tenancy on a single physical network. In CloudStack 3.0, a virtual network can be shared or isolated.

### Isolated Networks

An isolated network can be accessed only by virtual machines of a single account. Isolated networks have the following properties:

* Resources such as VLAN are allocated and garbage collected dynamically.
* There is one network offering for the entire network.
* The network offering can be upgraded or downgraded.

### Shared Networks

A shared network can be accessed by virtual machines that belong to many different accounts. Network isolation on shared networks is accomplished using techniques such as security groups. Shared networks have the following properties:

* Shared networks are created by the administrator
* Shared networks can be assigned to a certain domain
* The administrator can designate shared network resources, such as VLANs mapped to physical networks
* Shared networks can have multiple network offerings, from which end users can choose when deploying a virtual machine
* Shared networks are isolated by security groups

There is one special shared network, the public network, that is not displayed to end users. This network is used for Internet traffic.

### Runtime Allocation of Virtual Network Resources

When you define a new virtual network, all your settings for that network are stored in CloudStack. The actual network resources are activated only when the first virtual machine starts in the network. When all virtual machines have left the virtual network, the network resources are garbage collected so they can be allocated again. This helps to conserve network resources.

## Network Service Providers

A service provider (also called a network element) is hardware or virtual appliance that makes a network service possible; for example, a firewall appliance can be installed in the cloud to provide firewall service. On a single network, multiple providers can provide the same network service. For example, a firewall service may be provided by both Cisco and Juniper devices in the same physical network.

You can have multiple instances of the same service provider in a network; for example, more than one Juniper SRX device.

If different providers are set up to provide the same service on the network, the administrator can create *network offerings* so users can specify which network service provider they prefer (along with the other choices offered in network offerings). Otherwise, CloudStack will choose which provider to use whenever the service is called for.

### Supported Network Service Providers

Note: For the most up-to-date list of which network service providers CloudStack supports, see the CloudStack UI or call listNetworkServiceProviders.

CloudStack ships with an internal list of the supported service providers, and you’ll choose from this list when creating a network offering.

## Network Offerings

A network offering is a named set of network services, such as:

Note: For the most up-to-date list of which network services CloudStack supports, see the CloudStack UI or call listNetworkServices.

* DHCP
* Source NAT
* Gateway
* Load Balancing
* Firewall
* VPN
* Port Forwarding
* (Optional) Name one of several available providers to use for a given service, such as Juniper for the firewall
* (Optional) Network tag to specify which physical network to use

When creating a new VM, the user chooses one of the available network offerings, and that determines which network services the VM can use.

The CloudStack administrator can create any number of custom network offerings in addition to the default network offerings provided by CloudStack. By creating multiple custom network offerings, you can offer different classes of service on a single multi-tenant physical network. For example, while the underlying physical wiring may be the same for two tenants, tenant A may only need simple firewall protection for their website, while tenant B may be running a web server farm and require a scalable firewall solution, load balancing solution, and alternate networks for accessing the database backend.

When creating a new virtual network, the CloudStack administrator chooses which network offering to enable for that network. Each virtual network is associated with one network offering. A virtual network can be upgraded or downgraded by changing its associated network offering. If you do this, be sure to reprogram the physical network to match.

CloudStack also has internal network offerings for use by CloudStack system VMs. These network offerings are not visible to users but can be modified by administrators.