



CloudStack 3.0.0 Release Notes

For CloudStack Version 3.0.0

Revised March 22, 2012 2:19 PM Pacific

© 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

Overview	4
Submitting Feedback and Getting Help	4
Overview of Major New Features in 3.0.0	4
Redesigned User Interface	4
NetScaler Load Balancer	5
Sticky Session Policies for Load Balancer Rules	5
Using an LDAP Server for User Authentication	5
VM Storage Migration	5
Swift for Secondary Storage	5
Password and Key Encryption	6
Security Group Egress Rules	6
Using Projects to Organize Users and Resources	6
Providing Network Services for Users	6
New Features in 3.0.0	7
Issues Fixed in 3.0.0	9
Known Issues in 3.0.0	12
API Changes from 2.2.14 to 3.0	14

Overview

These Release Notes provide a brief description of new features and known issues for the 3.0.0 release of CloudStack.

NOT FOR UPGRADING CUSTOMERS

This release is intended for use in fresh installations of CloudStack. The capability to upgrade from 2.2.x versions of CloudStack is not provided in this release.

Submitting Feedback and Getting Help

We would like to hear your feedback, and we are available to help you use CloudStack 3.0.0.

Open-source community

A variety of channels are available for getting help with CloudStack, from forums to IRC chat and more. For details, see <http://cloudstack.org/discuss/>.

Commercial customers

The CloudStack support team is available to help commercial customers plan and execute their installations. To contact the support team, log in to the support portal at <https://na6.salesforce.com/sserv/login.jsp?orgId=00D80000000LWom> using the account credentials you received when you purchased your support contract.

Overview of Major New Features in 3.0.0

CloudStack 3.0.0 is a major new release. It provides several new features compared to CloudStack 2.2.x. This section provides overviews of the new features. If you just want a quick list by bug number, see [New Features in 3.0.0](#) on page 7.

Redesigned User Interface

The user interface of CloudStack has been redesigned to provide easier navigation as well as a more intuitive workflow. Graphical displays of the infrastructure topology have replaced drill-down lists as the main way to access the various CloudStack components such as zones, hosts, and networks. The main Dashboard now provides a more clear display of key information for managing the cloud. The end-user UI also benefits from this redesign, making it easier for users to manage their VMs and other resources. The new Project View lets users switch context from one set of resources to another, enabling a more efficient focus on the task at hand.

NetScaler Load Balancer

Citrix NetScaler is now supported as an external network element for load balancing. Set up an external load balancer when you want to provide load balancing through means other than CloudStack's provided virtual router.

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

Limitations: NetScaler can not yet be used as a firewall. It can not currently be set up in in-line mode (behind the firewall).

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 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. A variety of options are provided to control the exact behavior of cookies, such as how they are generated and whether they are cached.

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.

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.

Swift for Secondary Storage

In CloudStack 3.0, OpenStack Object Storage (Swift, <http://swift.openstack.org>) is supported for secondary storage. When using Swift, you configure Swift storage for the entire CloudStack, then set up NFS secondary storage for each zone. 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. These include the database secret key, database password, SSH keys, compute node root password, VPN password, user API secret key, and VNC password.

CloudStack 3.0 uses the Java Simplified Encryption (JASYPT) library. The data values are encrypted and decrypted using a database secret key. Of course, the database secret key itself can not be stored in the open – it must be encrypted. To 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 encryption type, database secret key, and Management Server secret key are set by the administrator during CloudStack installation.

Security Group Egress Rules

Security groups can be used to control network traffic to and from 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. 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. An egress rule can be specified either by CIDR to specify IP addresses, or by account to allow traffic from another security group.

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. Per-project resource limits can be set.

You can configure CloudStack to allow any user to create a new project, or you can restrict that ability to just CloudStack administrators. 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.

A user can be a member of any number of projects and can switch to a new Project View in the CloudStack UI to show only project-related information, such as project VMs, fellow project members, project-related alerts, and so on.

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 (also known as network elements) for the same service on a single physical network. For example, you can provide both Cisco and Juniper firewalls. You can have multiple instances of the same service provider in a network; for example, more than one Juniper SRX device.
- Bundle different types of network services into network offerings. When creating a new VM, the user chooses one of the available network offerings, and that determines which network services the VM can use. A network offering is a named set of network services, such as DHCP, source NAT, load balancing, firewall, VPN, port forwarding, and specific network service providers, such as Juniper SRX for the firewall. You can 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.
- Set up two types of virtual networks: shared and isolated. An isolated network can be accessed only by virtual machines of a single account. 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.
- More directly control the physical network, such as add/remove/update physical networks in a zone, configure VLANs on the physical network, specify properties like network speed, configure a name so the network can be recognized by hypervisors, configure the IP addresses trunked to a physical network, and specify what type of traffic is carried on the physical network (such as guest VM traffic vs. internal management traffic).

New Features in 3.0.0

4282	Added nonce support in API.
5510	Openstack Swift can now be used as an alternative to NFS storage for templates, ISO, and snapshots.
5822	All sensitive passwords are now properly encrypted in the database and any configuration files.
6745	UUIDs are now used in place of regular DB IDs. 3.0 API will support both.
6876	Netscaler MPX, VPX, and SDX is now supported.
7883	Templates, ISOs, Disk, and Service offerings can now be sorted to allow admins to more easily view them in the UI.
<Many>	Network as a Service feature.

8313	Basic LDAP authentication is now built in as an optional AUTH adapter.
8620	Projects feature.
8791	User dispersing allocator has now been added as an alternative algorithm for VM placement.
8962	Admins can now re-assign VM from one account to another.
9128	Network throttling is now controlled via network offerings.
9154	Redundant Router support has been added.
<Many>	Brand new 3.0 User Interface
9949	Users can now revert a VM to the original template it was created from.
<Many>	State management now included to pod and cluster level from the original host and zone level support.
10405	API Version annotation supported.
10588	XenServer 6.0 is now supported.
10617	Egress rules for security groups now supported.
10657	Capacity now has two levels of threshold support. One threshold is used to alert. The other is to disable resource allocation.
10792	Added ability for admins to set ingress rules that cannot be removed by user.
10796	Sticky session now supported for load balancers.
11303	Added support in login API call to take in a map of parameters that can be passed into the authenticators.
11173	VPN usage is now added as a new usage record.

11598	MTU for secondary storage is now configurable via Global configuration.
11689	Templates now have a SSH enabled flag similar to password enabled flag.
<Many>	vSphere 5.0 now has Beta support.
<Many>	RHEL/Centos 6.2 (KVM) is now supported.

Issues Fixed in 3.0.0

<Many>	VM Sync has been improved so that VM state should be better reflected between Management Server and Hypervisor.
8150	Template delete events are now recorded after being expunged.
8870	IPs from "Direct-Tagged" networks (shared guest networks) are no longer counted as part of the total number of public IPs.
9036	Migrated VMs will now have their consumed resources reflected properly in the capacity reports.
9842	Network Usage time range aggregation has been improved.
10043	Restarting the Management Server will no longer change a host status from Maintenance to Up.
10067	Extractable attribute can now be edited by administrators.
10195	Added a new VM state of "Unknown" if the host state is in "Alert".
10217	Management Server install will now check for FQDN hostname instead of stopping with an error condition.
10292	UI will no longer allow attaching volumes from one hypervisor to another.

10307	Network Usage will now account for more than one virtual interface.
10354	VMware ISO attach and detach events are now correctly registered.
10362	Disabling VPN will now work correctly even if the virtual router is in a STOPPED state.
10674	Management Server will now alert if it hits a snapshot limit quota.
10779	Port Ranges now work in the UI.
10831	Adding Secondary Storage URL with double slashes will now work.
11056	DHCP issues with Debian/Ubuntu guest OS have been resolved.
11131	VM scheduler will no longer retry in the same zone if that zone has been declared as non-allocable.
11193	Management Server will now alert a link-local IP capacity issue.
<Many>	Added new Global configurations to set limits for the number of guest VMs per hypervisor.
11273	Management Server will no longer attempt to program security group rules for non-reachable hypervisors.
11284	Administrators can now add a Basic Zone without security group support.
11311	Improved listVirtualMachine API call performance.
11387	Public IP of the secondary storage VM will now be correctly returned to the pool after being expunged.
11492	Volume limits are now checked when deploying a new VM.
11542	Management Server will no longer allow same public IP ranged across zones.
11585	Multiple public VLANs are now correctly supported in VMware.

11616	Manual live migration of VMs for KVM is now supported.
11814	General guest VM options for VMware are now supported.
11838	Deleted VM template names can now be re-used.
11902	Added global configuration to allow different NIC drivers for VMware system VM.
11926	Installation of system template will now do some mount point validation before proceeding.
<Many>	Many passwords are no longer logged in the Management Server logs.
<Many>	Secondary storage VM has been hardened.
12139	Added a way for Administrators to specify the default system template to use on a global or per zone basis.
12113	Improved re-try algorithm when attempting to copy a template from secondary to primary during failure scenarios.
12162	CreateLoadBalancer public ID was incorrectly published as optional. It is now required.
12192	State NFS handle are now correctly handled for KVM.
12290	Security Groups improvements.
12476	DHCP anti-spoofing fixes.
12481	Account ID is now returned as part of listAccount API.
12705	Source NAT is no longer configured on additional IP of a different network interface.
12782	Capacity now reflects hosts in maintenance mode.
12820	KVM: Attached disks are no longer removed after a VM reboot.

12877	Pagesize = -1 now works correctly.
12848	Removed notion of setting a default network when adding a shared network. Default networks are now specified during VM deployment.
12929	Added domain ID to all events.
13201	Added global configuration to allow administrator to specify default network device drivers for system VMs.
13315	Added BASIC auth http proxy for secondary storage VM.
13396	Escaped double-quotes in JSON responses.
13537	Templates created from snapshots now work with NFSv4.
13777	VMware snapshot errors are now handled better.

Known Issues in 3.0.0

11535	In-line mode for load balancer is not supported for all external devices.
12741	vSphere: maintenance mode will not live migrate system VM to another host.
12840	Capacity view is not available for pods or clusters.
13518	Security Groups are not supported in Advanced Networking.

<Many>	<p>F5 Known Issues:</p> <ul style="list-style-type: none"> • Unable to create load balancer rule for port 22. • No support for changing algorithm once rule has been created. • Source algorithm is not supported. Setting a rule to source will prevent other rules from being created properly. • Virtual router upgrades do not migrate all sticky session parameters correctly.
<Many>	<p>NetScaler Known Issues:</p> <ul style="list-style-type: none"> • When a VM from a load balancer rules is removed, it will also get removed for other load balancer rules of the same port. • Sticky session method “lbCookie” and “appCookie” do not work for any port other than 80. • Virtual router upgrades do not migrate all sticky session parameters correctly. • Once the public port 80 has been mapped to any private port, “A”, no other public port can be mapped to that private port, “A”.
13336	vSphere: cross cluster volume migration does not work properly.
13359	Programming F5/NetScaler rules can be better optimized.
<Many>	Network restart can fail under certain circumstances.
13883	Multiple NetScalers are not supported in Basic Networking.
13935	vSphere: detaching an ISO from a restored VM instance fails.
13963	vSphere: template download from templates created off of the root volume does not work properly.
<Many>	Disabling a pod or cluster does not prevent resource creation. Only zone level is supported right now.
14024	KVM: clustered LVM is not working properly.
<Many>	Bare metal host provisioning is not working properly.

API Changes from 2.2.14 to 3.0

Change to Behavior of List Commands

There was a major change in how our List* API commands work in CloudStack 3.0 compared to 2.2.x. The rules below apply only for managed resources – those that belong to an account/domain/project. They are irrelevant for the List* commands displaying unmanaged (system) resources, such as hosts, clusters, and external network resources.

When no parameters are passed in to the call, the caller sees only resources owned by the caller (even when the caller is the administrator). Previously, the administrator saw everyone else's resources by default.

When accountName/domainId are passed in:

- The caller sees the resources dedicated to the account specified.
- If the call is executed by a regular user, the user is authorized to specify only the user's own account/domainId.
- If the caller is a domain administrator, CloudStack performs an authorization check to see whether the caller is permitted to view resources for the given account/domainId.

When projectId is passed in, only resources belonging to that project are listed.

When domainId is passed in, the call returns only resources belonging to the domain specified. To see the resources of subdomains, use the parameter isRecursive=true. Again, the regular user can see only resources owned by that user, the root administrator can list anything, and a domain administrator is authorized to see only resources of the administrator's own domain and subdomains.

To see all resources the caller is authorized to see, except for Project resources, use the parameter listAll=true.

To see all Project resources the caller is authorized to see, use the parameter projectId=-1.

There is one API command that doesn't fall under the rules above completely: the listTemplates command. This command has its own flags defining the list rules:

listTemplates Flag	Description
featured	Returns templates that have been marked as featured and public
self	Returns templates that have been registered or created by the calling user
selfexecutable	Same as self, but only returns templates that are ready to be deployed with
sharedexecutable	Ready templates that have been granted to the calling user by another user
executable	Templates that are owned by the calling user, or public templates, that can be used to deploy a

	new VM
community	Returns templates that have been marked as public but not featured
all	Returns all templates (only usable by admins)

The CloudStack UI on a general view will display all resources that the logged-in user is authorized to see, except for project resources. To see the project resources, select the project view.

Removed API commands

- createConfiguration (Adds configuration value)
- configureSimulator (Configures simulator)

Added API commands

- assignVirtualMachine (Move a user VM to another user under same domain.)
- restoreVirtualMachine (Restore a VM to original template or specific snapshot)
- createLBStickinessPolicy (Creates a Load Balancer stickiness policy)
- deleteLBStickinessPolicy (Deletes a LB stickiness policy.)
- listLBStickinessPolicies (Lists LBStickiness policies.)
- ldapConfig (Configure the LDAP context for this site.)
- addSwift (Adds Swift.)
- listSwifts (List Swift.)
- migrateVolume (Migrate volume)
- updateStoragePool (Updates a storage pool.)
- authorizeSecurityGroupEgress (Authorizes a particular egress rule for this security group)
- revokeSecurityGroupEgress (Deletes a particular egress rule from this security group)
- createNetworkOffering (Creates a network offering.)
- deleteNetworkOffering (Deletes a network offering.)
- createProject (Creates a project)
- deleteProject (Deletes a project)
- updateProject (Updates a project)

- activateProject (Activates a project)
- suspendProject (Suspends a project)
- listProjects (Lists projects and provides detailed information for listed projects)
- addAccountToProject (Adds account to a project)
- deleteAccountFromProject (Deletes account from the project)
- listProjectAccounts (Lists project's accounts)
- listProjectInvitations (Lists projects and provides detailed information for listed projects)
- updateProjectInvitation (Accepts or declines project invitation)
- deleteProjectInvitation (Accepts or declines project invitation)
- updateHypervisorCapabilities (Updates a hypervisor capabilities.)
- listHypervisorCapabilities (Lists all hypervisor capabilities.)
- createPhysicalNetwork (Creates a physical network)
- deletePhysicalNetwork (Deletes a Physical Network.)
- listPhysicalNetworks (Lists physical networks)
- updatePhysicalNetwork (Updates a physical network)
- listSupportedNetworkServices (Lists all network services provided by CloudStack or for the given Provider.)
- addNetworkServiceProvider (Adds a network serviceProvider to a physical network)
- deleteNetworkServiceProvider (Deletes a Network Service Provider.)
- listNetworkServiceProviders (Lists network serviceproviders for a given physical network.)
- updateNetworkServiceProvider (Updates a network serviceProvider of a physical network)
- addTrafficType (Adds traffic type to a physical network)
- deleteTrafficType (Deletes traffic type of a physical network)
- listTrafficTypes (Lists traffic types of a given physical network.)
- updateTrafficType (Updates traffic type of a physical network)
- listTrafficTypeImplementors (Lists implementors of implementor of a network traffic type or implementors of all network traffic types)
- createStorageNetworkIpRange (Creates a Storage network IP range.)

- deleteStorageNetworkIpRange (Deletes a storage network IP Range.)
- listStorageNetworkIpRange (List a storage network IP range.)
- updateStorageNetworkIpRange (Update a Storage network IP range, only allowed when no IPs in this range have been allocated.)
- listUsageTypes (List Usage Types)
- addF5LoadBalancer (Adds a F5 BigIP load balancer device)
- configureF5LoadBalancer (configures a F5 load balancer device)
- deleteF5LoadBalancer (delete a F5 load balancer device)
- listF5LoadBalancers (lists F5 load balancer devices)
- listF5LoadBalancerNetworks (lists network that are using a F5 load balancer device)
- addSrxFirewall (Adds a SRX firewall device)
- deleteSrxFirewall (delete a SRX firewall device)
- configureSrxFirewall (Configures a SRX firewall device)
- listSrxFirewalls (lists SRX firewall devices in a physical network)
- listSrxFirewallNetworks (lists network that are using SRX firewall device)
- addNetscalerLoadBalancer (Adds a netscaler load balancer device)
- deleteNetscalerLoadBalancer (delete a netscaler load balancer device)
- configureNetscalerLoadBalancer (configures a netscaler load balancer device)
- listNetscalerLoadBalancers (lists netscaler load balancer devices)
- listNetscalerLoadBalancerNetworks (lists network that are using a netscaler load balancer device)
- createVirtualRouterElement (Create a virtual router element.)
- configureVirtualRouterElement (Configures a virtual router element.)
- listVirtualRouterElements (Lists all available virtual router elements.)