cloudstack DOCUMENTATION

Apache CloudStack 4.2.1

Version 4.2.1 Release Notes

Edition 1

cloudstack™
open source cloud computing

Apache CloudStack

Legal Notice

Abstract

Release notes for the Apache CloudStack 4.2.1 release.

Preface

1. Document Conventions

This manual uses several conventions to highlight certain words and phrases and draw attention to specific pieces of information.

In PDF and paper editions, this manual uses typefaces drawn from the Liberation Fonts set. The Liberation Fonts set is also used in HTML editions if the set is installed on your system. If not, alternative but equivalent typefaces are displayed. Note: Red Hat Enterprise Linux 5 and later includes the Liberation Fonts set by default.

1.1. Typographic Conventions

Four typographic conventions are used to call attention to specific words and phrases. These conventions, and the circumstances they apply to, are as follows.

`Mono-spaced Bold`

Used to highlight system input, including shell commands, file names and paths. Also used to highlight keycaps and key combinations. For example:

> To see the contents of the file **`my_next_bestselling_novel`** in your current working directory, enter the **`cat my_next_bestselling_novel`** command at the shell prompt and press **`Enter`** to execute the command.

The above includes a file name, a shell command and a keycap, all presented in mono-spaced bold and all distinguishable thanks to context.

Key combinations can be distinguished from keycaps by the hyphen connecting each part of a key combination. For example:

> Press **`Enter`** to execute the command.
>
> Press **`Ctrl`**+**`Alt`**+**`F2`** to switch to the first virtual terminal. Press **`Ctrl`**+**`Alt`**+**`F1`** to return to your X-Windows session.

The first paragraph highlights the particular keycap to press. The second highlights two key combinations (each a set of three keycaps with each set pressed simultaneously).

If source code is discussed, class names, methods, functions, variable names and returned values mentioned within a paragraph will be presented as above, in **`mono-spaced bold`**. For example:

> File-related classes include **`filesystem`** for file systems, **`file`** for files, and **`dir`** for directories. Each class has its own associated set of permissions.

Proportional Bold

This denotes words or phrases encountered on a system, including application names; dialog box text; labeled buttons; check-box and radio button labels; menu titles and sub-menu titles. For example:

> Choose **System** → **Preferences** → **Mouse** from the main menu bar to launch **Mouse Preferences**. In the **`Buttons`** tab, click the **`Left-handed mouse`** check box and click **`Close`** to switch the primary mouse button from the left to the right (making the mouse suitable for use in the left hand).
>
> To insert a special character into a **gedit** file, choose **Applications** → **Accessories** → **Character Map** from the main menu bar. Next, choose **Search** → **Find…** from the **Character Map** menu bar, type the name of the character in the **`Search`** field and click **`Next`**. The character you sought will be highlighted in the **`Character Table`**. Double-click this highlighted character to place it in the **`Text to copy`** field and then click the **`Copy`** button. Now switch back to your document and choose **Edit** → **Paste** from the **gedit** menu bar.

The above text includes application names; system-wide menu names and items; application-specific menu names; and buttons and text found within a GUI interface, all presented in proportional bold and all distinguishable by context.

`Mono-spaced Bold Italic` or ***`Proportional Bold Italic`***

Whether mono-spaced bold or proportional bold, the addition of italics indicates replaceable or variable text. Italics denotes text you do not input literally or displayed text that changes depending on circumstance. For example:

> To connect to a remote machine using ssh, type **`ssh`** ***`username@domain.name`*** at a shell prompt. If the remote machine is **`example.com`** and your username on that machine is john, type **`ssh john@example.com`**.
>
> The **`mount -o remount`** ***`file-system`*** command remounts the named file system. For example, to

remount the **/home** file system, the command is **mount -o remount /home**.

To see the version of a currently installed package, use the **rpm -q *package*** command. It will return a result as follows: ***package-version-release***.

Note the words in bold italics above — username, domain.name, file-system, package, version and release. Each word is a placeholder, either for text you enter when issuing a command or for text displayed by the system.

Aside from standard usage for presenting the title of a work, italics denotes the first use of a new and important term. For example:

Publican is a *DocBook* publishing system.

1.2. Pull-quote Conventions

Terminal output and source code listings are set off visually from the surrounding text.

Output sent to a terminal is set in **mono-spaced roman** and presented thus:

```
books        Desktop   documentation  drafts  mss    photos   stuff  svn
books_tests  Desktop1  downloads      images  notes  scripts  svgs
```

Source-code listings are also set in **mono-spaced roman** but add syntax highlighting as follows:

```
package org.jboss.book.jca.ex1;

import javax.naming.InitialContext;

public class ExClient
{
   public static void main(String args[])
       throws Exception
   {
      InitialContext iniCtx = new InitialContext();
      Object         ref    = iniCtx.lookup("EchoBean");
      EchoHome       home   = (EchoHome) ref;
      Echo           echo   = home.create();

      System.out.println("Created Echo");

      System.out.println("Echo.echo('Hello') = " + echo.echo("Hello"));
   }
}
```

1.3. Notes and Warnings

Finally, we use three visual styles to draw attention to information that might otherwise be overlooked.

Note

Notes are tips, shortcuts or alternative approaches to the task at hand. Ignoring a note should have no negative consequences, but you might miss out on a trick that makes your life easier.

Important

Important boxes detail things that are easily missed: configuration changes that only apply to the current session, or services that need restarting before an update will apply. Ignoring a box labeled 'Important' will not cause data loss but may cause irritation and frustration.

Warning

Warnings should not be ignored. Ignoring warnings will most likely cause data loss.

2. Feedback

to-do

Chapter 1. Welcome to CloudStack 4.2.1

Welcome to the 4.2.1 release of CloudStack. This version is the first defect fix release of CloudStack in the 4.2.x line.

This document contains information specific to this release of CloudStack, including upgrade instructions from prior releases, new features added to CloudStack, API changes, and issues fixed in the release. For installation instructions, please see the Installation Guide. For usage and administration instructions, please see the CloudStack Administrator's Guide. Developers and users who wish to work with the API will find instruction in the CloudStack API Developer's Guide

If you find any errors or problems in this guide, please see Section 2, “Feedback”. We hope you enjoy working with CloudStack!

Chapter 2. Compatibility Matrix

This section describes the operating systems, browsers, and hypervisors that have been newly tested and certified compatible with CloudStack 4.2.1. Most earlier OS and hypervisor versions are also still supported for use with 4.2.1 It might work well on other platforms, but the platforms listed below are the ones that are specifically tested against and are more likely to be able to help troubleshoot if you run into any issues.

2.1. Supported OS Versions for Management Server

This section lists the operating systems that are supported for running CloudStack Management Server. Note that specific versions of the operating systems are tested, so compatibility with CentOS 6.3 may not indicate compatibility with CentOS 6.2, 6.1 and so on.

- RHEL versions 5.5, 6.2, 6.3, and 6.4
- CentOS versions 6.3, and 6.4
- Ubuntu 12.04 LTS

2.2. Supported Hypervisor Versions

CloudStack supports three hypervisor families, XenServer with XAPI, KVM, and VMware with vSphere.

- CentOS 6.2 with KVM
- Red Hat Enterprise Linux 6.2 with KVM
- XenServer 6.0.2 (with Hotfix)
- XenServer 6.1
- VMware vSphere/vCenter 5.1
- Bare metal hosts are supported, which have no hypervisor. These hosts can run the following operating systems:

  RHEL or CentOS, v6.2 or 6.3

  

  Note

  Use libvirt version 0.9.10 for CentOS 6.3

  Fedora 17

  Ubuntu 12.04

For more information, see the Hypervisor Compatibility Matrix in the CloudStack Installation Guide.

2.3. Supported External Devices

- Netscaler VPX and MPX versions 9.3 and 10.e
- Netscaler SDX version 9.3
- SRX (Model srx100b) versions 10.3 or higher
- F5 10.1.0 (Build 3341.1084)

2.4. Supported Browsers

The CloudStack Web-based UI should be compatible with any modern browser, but it's possible that some browsers will not render portions of the UI reliably, depending on their support of Web standards. For best results, one of the following browsers recommended:

- Internet Explorer versions 8 and 9
- Firefox version 10 and beyond
- Google Chrome versions 17 and 20.0.1132.47m
- Safari 5

Chapter 3. About This New Release

3.1. What's New in 4.2.1

CloudStack 4.2.1 includes the following new features.

3.1.1. Optional XenServer 64-Bit Template Support

CloudStack now provides XenServer 64-bit templates for System VMs. With this support, you will be able to upgrade virtual routers in a zone. The following parameters have been introduced for the same purpose:

- XenServer: ***router.template.xen***
- KVM: ***router.template.kvm***

3.1.2. XenServer VM Snapshots

VM Snapshots are now supported on both VMware and XenServer hosts. Previously, they were suported only on VMware.

In addition to the existing CloudStack ability to snapshot individual VM volumes, you can now take a VM snapshot to preserve all the VM's data volumes as well as (optionally) its CPU/memory state. This is useful for quick restore of a VM. For example, you can snapshot a VM, then make changes such as software upgrades. If anything goes wrong, simply restore the VM to its previous state using the previously saved VM snapshot. The VM snapshot includes not only the data volumes, but optionally also whether the VM is running or turned off (CPU state) and the memory contents. The snapshot is stored in CloudStack's primary storage.

VM snapshots can have a parent/child relationship. Each successive snapshot of the same VM is the child of the snapshot that came before it. Each time you take an additional snapshot of the same VM, it saves only the differences between the current state of the VM and the state stored in the most recent previous snapshot. The previous snapshot becomes a parent, and the new snapshot is its child. It is possible to create a long chain of these parent/child snapshots, which amount to a "redo" record leading from the current state of the VM back to the original.

3.1.3. Cisco UCS Enhancements

Several modifications have been made to improve the user experience when working with Cisco UCS blades and the UCS Manager.

- The internal procedure for associating a profile to a blade has been modified. When a user wants to associate a profile to a blade in CloudStack 4.2.1, the user chooses a profile template. CloudStack instantiates a profile from that template. In the previous version, CloudStack would instead create a clone of a profile chosen by the user.
- As a consequence of this change, the user now views a list of profile templates rather than a list of profiles when associating a blade.
- A new mechanism is provided for making CloudStack aware of any changes that are made manually on the Cisco UCS Manager. For example, at any time, CloudStack users might directly associate or dissociate blades on the UCS Manager, and CloudStack would not be aware of these changes. In order to synchronize the state of CloudStack with UCS Manager, the user can click a new Refresh Blades button in the CloudStack UI. This button is located in the Blades tab, above the list of associated blades.
- To support the UCS enhancements, several changes have been made to the CloudStack API. See Chapter 5, *API Changes from 4.2 to 4.2.1*.

3.1.4. Choose Single-part or Multi-part Upload to Object Storage

CloudStack 4.2.1 supports both multi-part and single-part upload for registering templates, uploading volumes, and backing up snapshots to object storage in secondary storage. Previously, only multi-part upload was supported for registering templates and uploading volumes, and only single-part upload was supported for backing up snapshots.

The type of upload CloudStack will use depends on the value of the new global configuration setting s3.singleupload.max.size. You can use this setting to set up three different upload scenarios:

- Choose the upload technique dynamically depending on the size of the object to be uploaded. Smaller objects will be uploaded as a single unit, and larger objects will be split into multiple parts for upload. To set the threshold for switching to multi-part upload, set s3.singleupload.max.size to the desired object size in GB (default: 5GB).
- To use multi-part upload for all objects regardless of size, set s3.singleupload.max.size to 0.
- To use single-part upload for all objects, set s3.singleupload.max.size to -1.

Multi-part upload is useful to make the transfer of templates and volumes to remote storage more resilient to network failure and to optimize throughput. Single-part upload may be preferable when using storage that is local to the data center.

3.1.5. Device ID Changes for XenServer

In XenServer 6.1 version and above, a new parameter, **`device_id: 0002`**, is introduced for Windows VM with PV drivers. Due to this change, Windows VMs deployed with PV drivers on XenServer 6.0.2 or earlier hosts are not able to successfully boot after stopping and starting once the hosts have been upgraded to XenServer version 6.1 or 6.2. In order to address this issue, a new Global Parameter, **`xen.pvdriver.version`**, is introduced to reflect the default PV driver version that is used when registering templates as regular users. Default value for this Global parameter on fresh install will be set to **`xenserver61`**, which implies that the new deployments will have only XenServer 6.1 or XenServer 6.2 hosts. Default value for this Global parameter on upgrades would be set to **`xenserver61`** only if all the hosts in the deployment are XenServer 6.1 or above. Even if a host is below XenServer 6.1 version, this value will be set to **`xenserver56`**. The administrators are provided with following abilities with respect to setting or altering PV driver version:

- Ability to set the PV driver version 6.1+ option for a template when registering templates.

  Regular and Domain admin users will not have the ability to set the PV driver version when registering templates. In this case the PV driver version is defaulted to the Global parameter, **`xen.pvdriver.version`**. The PV driver version of the template is stored in **`vm_template_details`**.
- Ability to update the PV driver version 6.1 + option for an existing template.
- Ability to update the PV driver version 6.1 + option for a VM when it is in stopped state.

3.1.6. Acquiring IP Without Enabling SourceNAT Service

The SourceNAT dependency for acquiring IPs has been removed. Therefore, an IP can now be acquired and LB rules can be created on it without enabling the SourceNAT service in a network. In both shared and isolated networks, DNS, DHCP and LB services provided by CloudStack is a valid service combination. In this case gateway is defined externally on the configured LB device and CloudStack does not provide any NAT service.

3.2. Issues Fixed in 4.2.1

Apache CloudStack uses Jira to track its issues. All new features and bugs for 4.2.1 have been tracked in Jira, and have a standard naming convention of "CLOUDSTACK-NNNN" where "NNNN" is the issue number.

This section includes a summary of known issues were fixed in 4.2.1. Approximately 150 bugs were resolved or closed in the 4.2.1 cycle.

Defect	Description
CLOUDSTACK-5154	CVE-2014-0031 CloudStack ListNetworkACL API discloses ACLs for other users
CLOUDSTACK-5263	CVE-2013-2136 CloudStack Virtual Router stop/start modifies firewall rules allowing additional access
CLOUDSTACK-3237	[VMware] Migrate volume is failing when snapshots exist for that volume.
CLOUDSTACK-4300	[KVM] [Upgrade][2.2.14 to 4.2] System VMs are not coming up after upgrade.
CLOUDSTACK-4405	[Upgrade] Migration failed between existing hosts and new hosts.
CLOUDSTACK-4436	Virtual Router fails to start on RHEL6.2.
CLOUDSTACK-4446	AWSAPI server fails to start due to an error in bean creation.
CLOUDSTACK-4464	[VMware] When deploying 30 parallel VMs, a VM fails to get deployed due to the "StartCommand failed due to Exception: javax.xml.ws.soap.SOAPFaultException" error.
CLOUDSTACK-4479	VPC Network Tier creation fails.
CLOUDSTACK-4516	[VMware][Upgrade] MySQLIntegrityConstraintViolationException while performing any task by using local storage after upgrade from 3.0.7 to 4.2.
CLOUDSTACK-4522	[VMware][Upgrade] Creation of VM from ISO fails.
CLOUDSTACK-4554	[VMware][Upgrade from 3.0.6 to 4.2] System VM agent doesn't come up after adding a zone on an upgraded setup.
CLOUDSTACK-4555	[VMware][Upgrade from 3.0.6 to 4.2] After upgrade the system VMs fail to come up because the Secondary Storage mount point is pointing to a wrong location.
CLOUDSTACK-4561	Deploying a VM fails after upgrading to 4.2 from earlier version having a private zone.
CLOUDSTACK-4579	[KVM] [Upgrade 2.2.14 to 4.2] After upgrade, deploying VMs with existing templates does not work.
CLOUDSTACK-4580	[KVM] [Upgrade 2.2.14 - 4.2] After upgrade, existing VMs cannot be started after stopping them.
CLOUDSTACK-4618	Storage refactoring has broken CLVM.
CLOUDSTACK-4671	ListZone API failed with Assertion error if assertion is turned on for Management Server.
CLOUDSTACK-4864	[VMware] 64-bit system VM template does not exist.
CLOUDSTACK-5065	[KVM] Snapshot doesn't take VM snapshot if the VM is running.
CLOUDSTACK-532	Cleaning up Storage template corrupts templates.
CLOUDSTACK-732	[KVM] No Snapshot support.
CLOUDSTACK-1670	When a VM is part of two networks, the IP address from the first network is being assigned to eth1.
CLOUDSTACK-1775	Events related to User/Domain/Account are not generated, instead USER-DISABLE, DOMAIN-DELETE and ACCOUNT.DISABLE event are generated.
CLOUDSTACK-1819	In AWS Regions, various issues persist when moving a zone from one region to another.
CLOUDSTACK-2792	In a Redundant router, password is reset again after a fail-over.
CLOUDSTACK-3010	[VMware] Router VM deployment fails with a "Message: Invalid configuration for device '2' error in Shared networks.

CLOUDSTACK-3285	No support for HTTP redirects and HTTPS certificate handling in UCS.
CLOUDSTACK-3424	[IPv6] When a VM is expunged and a new VM is deployed with the same name, **`/etc/dhchosts.txt`** has two entries with the same name.
CLOUDSTACK-3583	Stopping Management Server does not remove PID.
CLOUDSTACK-3715	Live Migration of virtual instances operation is getting timed out.
CLOUDSTACK-3737	Uploaded volume is not getting deleted from Secondary storage after attaching it to guest VM.
CLOUDSTACK-3765	[Packaging] Unable to upgrade 4.2 build on Centos 5.5.
CLOUDSTACK-3808	Attaching a volume does not work when root is at zone-level primary store and data at cluster-level or host-level store.
CLOUDSTACK-3911	[Portable IP] No mechanism to check while adding a zone-level public range to check whether the same VLAN exists in portable IP range.
CLOUDSTACK-4095	Region ID appears within the Database Transaction code.
CLOUDSTACK-4128	Starting a System VMs does not check for existence of staging Secondary Storage in a zone.
CLOUDSTACK-4137	[KVM]After unmanaging a cluster, managing another cluster does not bring hosts to UP state. To work around manually restart cloud-agent on KVM hosts.
CLOUDSTACK-4190	Volume is not deleted from staging storage after a successful volume migration.
CLOUDSTACK-4199	In Redundant Virtual Router,no failover occurs.
CLOUDSTACK-4239	[VMware] Snapshot creation on ESX 4.1 host fails with a ""BackupSnapshotCommand exception: javax.xml.ws.soap.SOAPFaultException" error.
CLOUDSTACK-4327	SSVM, CPVM and router VMs are running even after storage entered into maintenance.
CLOUDSTACK-4350	[Performance Testing] Adding hosts take much longer time than baselines.
CLOUDSTACK-4432	[VMware] Null Pointer exception is thrown during VM deployment.
CLOUDSTACK-4433	[VMware] Registration of template by using the downloaded template URL is failing.
CLOUDSTACK-4434	[Ubuntu] Direct input ""- _ "", ""? /"", ""keyboard /"" ,""keyboard -"" keys are not working well for the US keyboard.
CLOUDSTACK-4454	Not able to delete secondary storage when existing snapshots are deleted.
CLOUDSTACK-4455	Template sync results in private templates being synced to all the secondary stores.
CLOUDSTACK-4458	[VMware] Failed to create Snapshot on data disk because of backup snapshot exception.
CLOUDSTACK-4465	Resource count is not decremented for domain if user VM is being destroyed as a part of account removal.
CLOUDSTACK-4485	[VMware] [3.0.6 to ASF 4.2 Upgrade] System VMs is not created in the cluster due to invalid path information of the template on the Primary Storage in the cluster.
CLOUDSTACK-4495	System VM template URL is pointing to old template location in the Upgrade file.
CLOUDSTACK-4499	[XenServer v 6.1 and 6.2] Hosts initially transition to 'Alert' state and then to 'Up' after adding a host.
CLOUDSTACK-4513	[VMware] In a new mapping between a datacenter and a zone, when hosts in the second cluster in data center put in maintenance mode, CPVM and guest VMs that are migrated failed to come up.
CLOUDSTACK-4520	[VMware][Upgrade] ExtractVolumeCmd fails with NPE while attempting to download a volume.
CLOUDSTACK-4530	Creating template from a Snapshot fails with having not able to find any ova/ovf snapshot when multiple secondary storage exist for a zone.
CLOUDSTACK-4539	[VMware] If ***`vmware.create.full.clone`*** is set to true in an upgraded setup, default nature of VMs are full clone.
CLOUDSTACK-4551	Migrating the data volume from NFS to local storage does not change the underlying disk offering.
CLOUDSTACK-4573	Acquiring IP addresses above domain limit is possible in VPC.
CLOUDSTACK-4596	Same IP range is allowed to be defined in different VLANs across public and portable ranges.
CLOUDSTACK-4600	Registered cross-zone template does not populate

	template_zone_ref for later added zones using S3.
CLOUDSTACK-4624	VM Migration fails in Security Group-enabled Advanced Zone with 'CloudRuntimeException: callHostPlugin failed for cmd: network_rules' error.
CLOUDSTACK-4625	Snapshots and templates cannot be deleted from staging storage after create template from snapshot on S3.
CLOUDSTACK-4674	[Baremetal] **`/usr/share/cloudstack-common/scripts/util/ipmi.py`** script need to recognize various IPMI version and BMC type of server.
CLOUDSTACK-4698	DHCP-service enabled network cannot expunge VMs.
CLOUDSTACK-4704	Database upgrade bug is caused by the vpc_service_map table.
CLOUDSTACK-4707	The sourcetemplateid field is not getting set for derived templates.
CLOUDSTACK-4711	Premature API response prevents CloudStack from syncing association status in UCS environment.
CLOUDSTACK-4717	Associate IP does not work on shared networks without Source NAT service.
CLOUDSTACK-4725	KVM agent fails to join if local pool is already registered.
CLOUDSTACK-4745	Exception occurs when trying to apply static NAT rule by using CreateIpForwardingCmd API.
CLOUDSTACK-4746	Allocation capacity of a cluster during HA.
CLOUDSTACK-4750	The bond.VLAN mapping in iptables forward chain is not created consistently.
CLOUDSTACK-4777	NullPointerException instead of working KVM HA.
CLOUDSTACK-4783	Unable to see a derived template if the parent template is deleted.
CLOUDSTACK-4816	No configurable option to choose single or multipart upload to S3 object storage.
CLOUDSTACK-4817	Backup snapshot on XenServer should take global setting s3.multipart.enabled.
CLOUDSTACK-4828	Removing NIC fails if DHCP was not enabled in the network offering.
CLOUDSTACK-4836	Restart network with cleanup=true does not reprogram remote access VPN users in the virtual router.
CLOUDSTACK-4849	LXC not working when using non-oss build.
CLOUDSTACK-4859	No global configuration available to disable storage migration during HA.
CLOUDSTACK-4862	Admin cannot delete shared network scoped to user account.
CLOUDSTACK-4872	VM provisioned using a registered Windows Server 2012 template will show as other OS in vCenter.
CLOUDSTACK-4888	Refresh blades on a decommissioned chassis results in NPE in UCS environment.
CLOUDSTACK-4913	Disabling security group for bridge mode non-security group zone
CLOUDSTACK-4921	Usage service does not start after reboot.
CLOUDSTACK-4946	[VMware] Restore VM with template ID feature does not work.
CLOUDSTACK-4988	The public templates created in ROOT/a/b domains are not visible in /ROOT/a domains
CLOUDSTACK-5061	[VMware] Storage over-provisioning factor is not considered when using thin provisioning over VMFS datastores.
CLOUDSTACK-5066	Existed remote access VPN is dropped when adding new VPN users.
CLOUDSTACK-5076	[Upgrade] Rebooting VM failed after bridge name change.
CLOUDSTACK-5122	[VMware] System VMs are getting recreated with old template after upgrading to 4.2.
CLOUDSTACK-1236	Warning while adding XenServer 6.1 host: Unable to create local link network.
CLOUDSTACK-1749	Cloud agent service running on Secondary Storage VM and Console Proxy VM is named as cloud.com service.
CLOUDSTACK-2024	The cloudstack-setup-management script with https does not work due to incorrect path and missing keystore file.
CLOUDSTACK-2034	No alert generated when deleting a primary storage is failed.
CLOUDSTACK-2413	The Change Compute Offering dialog box for a instance displays the Description instead of the Name of compute offering.
CLOUDSTACK-2767	There is no check on input parameters in API for Global settings, zone settings, and account settings.
CLOUDSTACK-2804	The getEthByIp function in vpc_func.sh can return the wrong network interface.
CLOUDSTACK-2918	In a scaledup environment, hosts fail to come up after

	Management Server restart in a clustered setup.
CLOUDSTACK-3223	[VMware] Exception occurred while creating the CPVM in a setup using the latest SystemVM template.
CLOUDSTACK-3508	NullPointerException observed during the ListVolumeAnswer API call.
CLOUDSTACK-3603	The template_store_ref"' table has Invalid URL References.
CLOUDSTACK-3803	Unable to complete Add zone wizard.
CLOUDSTACK-3873	No error notification is generated when cluster-level Primary storage is added with wrong path.
CLOUDSTACK-4449	Possibility of /tmp/xapilog filling up the Root disk on XenServer.
CLOUDSTACK-4466	DHCP capability breaks in 4.2.
CLOUDSTACK-4482	The getVMPassword() API call does not return password for VMs that are deployed with password enabled templates.
CLOUDSTACK-4521	[VMware] [upgrade] Attaching an uploaded volume to a VM throws NPE.
CLOUDSTACK-4572	The findHostsForMigration API does not return correct host list.
CLOUDSTACK-4612	Specified keyboard language is not showing as default in consoleView passed during deployVM.
CLOUDSTACK-4613	Security group rules issue in hosts.
CLOUDSTACK-4627	HA does not work, nor user VM migrate.
CLOUDSTACK-4636	In a scaled-up setup all VMs in a cluster were stopped or started after Management Server restart.
CLOUDSTACK-4661	[DB Upgrade] The SecondaryStorage entry in the host table before upgrade is not marked as removed after migrating them to image_store table.
CLOUDSTACK-4716	[Upgrade] The resource_count table is not updated after upgrade to 4.2
CLOUDSTACK-4755	Version 4.x does not allow memory upgrade.
CLOUDSTACK-4765	PF rules configure public IP address is not set on the VR when network is up after GC.
CLOUDSTACK-4785	No support for adding details to a user VM.
CLOUDSTACK-4786	Redundant router has a priority limitation.
CLOUDSTACK-4797	[Documentation] Installation guide for 4.2 instructs users to install 4.1.
CLOUDSTACK-4813	Get ExitValue when running bash commands.
CLOUDSTACK-4827	Build failed on 4.2.
CLOUDSTACK-4839	[Documentation] The section 3.5 in the Install Guide provides wrong list of .deb packages.
CLOUDSTACK-4867	NullPointerException on agent while remounting primary storage.
CLOUDSTACK-4882	listClusters/pods/zones and listCapacity(dashboard view) API not accounting for reserved in the used capacity percentage.
CLOUDSTACK-4895	Management Server fails to start because snapshot policy time zones have day light savings.
CLOUDSTACK-4911	[Mixed Hypervisor] VM status is marked as alive when exit status of ping command is not available within command timeout.
CLOUDSTACK-4923	Network limits is missing in Accounts details page.
CLOUDSTACK-4924	AcountCleanup: The IP address is not released if the network failed to delete.
CLOUDSTACK-4947	if apply.allocation.algorithm.to.pods is set to true VM creation fails.
CLOUDSTACK-4948	DeploymentPlanner: Logic to check if cluster can be avoided needs to consider if VM is using a local storage and shared storage.
CLOUDSTACK-4964	Nexus password is logged in Management Server logs during guest network implementation with Cisco VNMC provider.
CLOUDSTACK-4985	NPE while deleting old root volumes of a restored VM during storage garbage collection.
CLOUDSTACK-4987	Adding an Isolated network belonging to an account to a VM belonging to different account is possible.
CLOUDSTACK-4998	The assignVirtualMachine API has wrong response string, causing Cloudmonkey to crash.
CLOUDSTACK-5018	Creation of VM using template from snapshot of RBD volume fails.
CLOUDSTACK-5029	The cloud-bugtool is not available release package.
CLOUDSTACK-5038	[Upgrade] Used CPU is getting bumped up when the over provisioning factor is greater than 1.
CLOUDSTACK-5096	[VMware] Corrupt template is left behind after the copy of a

	template from secondary to primary fails.
CLOUDSTACK-5140	A stopped VM cant start after disable threshold has been reached on the storage pool.
CLOUDSTACK-3100	Add the displayvmflag to listVirtualMachines API.

3.3. Known Issues in 4.2.1

This section includes a summary of known issues in 4.2.1

Issue ID	Description
CLOUDSTACK-4875	[VMware] vCenter 5.5 - SYSTEM VM: Unable to create deployment for VM
CLOUDSTACK-5159	[VMware] Reset SSH keypair randomly fails.
CLOUDSTACK-5188	Password reset of vm on XenServer and VMware does not work on first reboot.
CLOUDSTACK-2140	Host is still marked as being in UP state when the host is shutdown and there are no more hosts in the cluster.
CLOUDSTACK-4545	[VMware] Master template used by linked clones should not be available for deletion.
CLOUDSTACK-4577	[VMware] Unexpected exception while executing org.apache.cloudstack.api.command.user.volume.ResizeVolumeCmd java.lang.NullPointerException.
CLOUDSTACK-4587	VM is failing to deploy on a Legacy zone after adding zone wide primary storage and moving cluster wide primary storage to maintenance mode.
CLOUDSTACK-4594	[VMware] [Upgrade] Failed to revert VM Snapshot which were created before Live Storage Migrating the VM to other clusters.
CLOUDSTACK-4616	When system VMs fail to start when host is down, link local IP addresses do not get released resulting in all the link local IPs being consumed eventually.
CLOUDSTACK-5008	[VMware] Failed to start the VM after performing Cold Migration of Volume to Second Zone wide primary Storage.
CLOUDSTACK-5014	[VMware] DeployVM with data disk failed with exception.
CLOUDSTACK-5054	VM migration involving storage migration on vmware fails with the 'The object has already been deleted or has not been completely created' exception.
CLOUDSTACK-5119	VLAN provisioning broken in F5
CLOUDSTACK-4475	Attaching an uploaded volume to a VM is always going to first primary storage added.
CLOUDSTACK-4492	Attaching volume to a VM fails after upgrade if the volume was uploaded before upgrade.
CLOUDSTACK-4496	[VMware] System VMs are failed to start with NPE when host is in maintenance state.
CLOUDSTACK-4504	VM creation is failing using the Ubuntu ISO with XenServer 6.1 and 6.2
CLOUDSTACK-4536	Inconsistency in volume store location on secondary storage for uploaded and extracted volume.
CLOUDSTACK-4574	NPE while executing DestroyVM command.
CLOUDSTACK-4593	[VMware] [Upgrade] Livestorage Migration and VM Snapshot features are not fully functional after upgrade.
CLOUDSTACK-4620	VM failed to start on the host on which it was running due to not having enough reserved memory when the host was powered on after being shutdown.
CLOUDSTACK-4638	State information is not synced on Starting VM directly via vCenter.
CLOUDSTACK-4639	Status of VM is not synced properly when host is HA during hypervisor failure.
CLOUDSTACK-4657	[CEPH] Attaching a volume to an instance that is migrated from one primary to another primary fails.
CLOUDSTACK-4697	Not able to delete Primary storage when there are no hosts in the cluster.
CLOUDSTACK-4734	Creating snapshot from ROOT volume fails with the Failed to create snapshot due to an internal error creating snapshot for volume 14 error message.
CLOUDSTACK-4743	The applyStaticRoutes/createPrivateGatway/deletePrivateGateway APIs read from the vpc_service_map table instead of relying on hard-coded values.
CLOUDSTACK-4789	Fix ResourceMetaDataManagerTest.
CLOUDSTACK-4850	[UCS] using template instead of cloning profile.
CLOUDSTACK-4861	[VMware] If Guest traffic spans across multiple physical networks, selection of physical network to implement guest network is not working correctly.
CLOUDSTACK-4906	Add network address to the Marvin dependency list.
CLOUDSTACK-4978	[VMware] Provisioning VMs from templates fails with the ROOT-249/ROOT-249.vmdk not found error
CLOUDSTACK-5002	Destroying VM does not work. VM destroy failed with the Stop i-2-59-VM command due to invalid object reference. The object may have

	recently been deleted.
CLOUDSTACK-5005	Stopping multiple VMs does not work.
CLOUDSTACK-5020	Recreate system VM fails in a specific scenario during storage maintenance.
CLOUDSTACK-5075	Various issues with destroying a VM with local storage. VM disk statistics cannot be updated for a VM.
CLOUDSTACK-5090	Anti-Affinity: VM fails to start on a cluster belonging to a different pod.
CLOUDSTACK-5098	[VMware] Entries in **`vmware_data_center`** and **`vmware_data_center_zone_map`** are not cleaned up when there is a failure to add the cluster.
CLOUDSTACK-5118	Virtual Routers are listed multiple times in the Infrastructure page.
CLOUDSTACK-5123	[VMware] Memory over-provisioning behaviour.

Chapter 4. Upgrade Instructions for 4.2.1

This section contains upgrade instructions from prior versions of CloudStack to Apache CloudStack 4.2.1. We include instructions on upgrading to Apache CloudStack from pre-Apache versions of Citrix CloudStack (last version prior to Apache is 3.0.2) and from the releases made while CloudStack was in the Apache Incubator.

If you run into any issues during upgrades, please feel free to ask questions on users@cloudstack.apache.org or dev@cloudstack.apache.org.

4.1. Upgrade from 4.2.0 to 4.2.1

This section will guide you from CloudStack 4.2 to CloudStack 4.2.1.

Any steps that are hypervisor-specific will be called out with a note.

We recommend reading through this section once or twice before beginning your upgrade procedure, and working through it on a test system before working on a production system.

Note

The following upgrade instructions should be performed regardless of hypervisor type.

1. a. While running the existing 4.2.0 system, log in to the UI as root administrator.
   b. In the left navigation bar, click Templates.
   c. In Select view, click Templates.
   d. Click Register template.
   The Register template dialog box is displayed.
   e. In the Register template dialog box, specify the following values (do not change these):

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.2 Description: systemvm-xenserver-4.2 URL:http://download.cloud.com/templates/4.2/systemvmtemplate-2013-07-12-master-xen.vhd.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.2 Description: systemvm-kvm-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-

	2013-06-12-master-kvm.qcow2.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: KVM Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.2 Description: systemvm-vmware-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-4.2-vh7.ova Zone: Choose the zone where this hypervisor is used Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

2. Most users of CloudStack manage the installation and upgrades of CloudStack with one of Linux's predominant package systems, RPM or APT. This guide assumes you'll be using RPM and Yum (for Red Hat Enterprise Linux or CentOS), or APT and Debian packages (for Ubuntu).
3. Create RPM or Debian packages (as appropriate) and a repository from the 4.2.1 source, or check the Apache CloudStack downloads page at http://cloudstack.apache.org/downloads.html for package repositories supplied by community members. You will need them for step 9 or step 12.

   Instructions for creating packages from the CloudStack source are in the Installation Guide.
4. Stop your management server or servers. Run this on all management server hosts:

```
# service cloudstack-management stop
```

5. If you are running a usage server or usage servers, stop those as well:

```
# service cloudstack-usage stop
```

6. Make a backup of your MySQL database. If you run into any issues or need to roll back the upgrade, this will assist in debugging or restoring your existing environment. You'll be prompted for your password.

```
# mysqldump -u root -p cloud > cloudstack-backup.sql
```

7. Perform the following to verify the artifacts:
   a. (optional) Install GPG keys if needed:

```
sudo apt-get install gpg
```

   b. Import the GPG keys stored in the source distribution's KEYS file

```
gpg --import KEYS
```

   Alternatively, download the signing keys, the IDs found in the KEYS file, individually by using a keyserver.

   For example:

```
gpg --recv-keys CC56CEA8
```

   c. Verify signatures and hash files:

```
#gpg --verify apache-cloudstack-4.2.1-src.tar.bz2.asc
#gpg --print-md MD5 apache-cloudstack-4.2.1-src.tar.bz2 | diff - apache-
cloudstack-4.2.1-src.tar.bz2.md5
#gpg --print-md SHA512 apache-cloudstack-4.2.1-src.tar.bz2 | diff - apache-
cloudstack-4.2.1-src.tar.bz2.sha
```

   Each of these commands should return no output. Any output from them implies that there is a difference between the hash you generated locally and the hash that has been pulled from the server.

   d. Get the commit hash from the VOTE email.

   For example: **4cd60f3d1683a3445c3248f48ae064fb573db2a1**. The value changes between releases.

   e. Create two new temporary directories:

```
#mkdir /tmp/cloudstack/git
#mkdir /tmp/cloudstack/tree
```

   f. Check out the 4.2.1 branch:

```
#git clone https://git-wip-us.apache.org/repos/asf/cloudstack.git
/tmp/cloudstack/git
#cd /tmp/cloudstack/git
#git archive --format=tar --prefix=/tmp/cloudstack/tree/ <commit-hash> | tar
Pxf -
```

g. Unpack the release artifact:

```
#cd /tmp/cloudstack
#tar xvfj apache-cloudstack-4.2.1-src.tar.bz2
```

h. Compare the contents of the release artifact with the contents pulled from the repo:

```
#diff -r /tmp/cloudstack/apache-cloudstack-4.2.1-src /tmp/cloudstack/tree
```

Ensure that content is the same.

i. Verify the Code License Headers:

```
#cd /tmp/cloudstack/apache-cloudstack-4.2.1-src
#mvn --projects='org.apache.cloudstack:cloudstack' org.apache.rat:apache-rat-
plugin:0.8:check
```

The build fails if any non-compliant files are present that are not specifically excluded from the ASF license header requirement. You can optionally review the target/rat.txt file after the run completes. Passing the build implies that RAT certifies that the files are compliant and this test is passed.

8. (KVM Only) If primary storage of type local storage is in use, the path for this storage needs to be verified to ensure it passes new validation. Check local storage by querying the cloud.storage_pool table:

```
# mysql -u cloud -p -e "select id,name,path from cloud.storage_pool where
pool_type='Filesystem'"
```

If local storage paths are found to have a trailing forward slash, remove it:

```
# mysql -u cloud -p -e 'update cloud.storage_pool set path="/var/lib/libvirt/images"
where path="/var/lib/libvirt/images/"';
```

9. If you are using Ubuntu, follow this procedure to upgrade your packages. If not, skip to step 12.

Community Packages

This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and APT repository, substitute your own URL for the ones used in these examples.

a. The first order of business will be to change the sources list for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent. (No changes should be necessary for hosts that are running VMware or Xen.)

Start by opening **`/etc/apt/sources.list.d/cloudstack.list`** on any systems that have CloudStack packages installed.

This file should have one line, which contains:

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

We'll change it to point to the new package repository:

```
deb http://cloudstack.apt-get.eu/ubuntu precise 4.2
```

If you're using your own package repository, change this line to read as appropriate for your 4.2.1 repository.

b. Now update your apt package list:

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

c. Now that you have the repository configured, it's time to install the **`cloudstack-management`** package. This will pull in any other dependencies you need.

```
$ sudo apt-get install cloudstack-management
```

d. You will need to manually install the **`cloudstack-agent`** package:

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

During the installation of **`cloudstack-agent`**, APT will copy your **`agent.properties`**, **`log4j-cloud.xml`**, and **`environment.properties`** from **`/etc/cloud/agent`** to **`/etc/cloudstack/agent`**.

When prompted whether you wish to keep your configuration, say Yes.

e. Verify that the file **`/etc/cloudstack/agent/environment.properties`** has a line that reads:

```
paths.script=/usr/share/cloudstack-common
```

If not, add the line.

f. Restart the agent:

```
service cloudstack-agent stop
killall jsvc
service cloudstack-agent start
```

10. (VMware only) Additional steps are required for each VMware cluster. These steps will not affect running guests in the cloud. These steps are required only for clouds using VMware clusters:

a. Stop the Management Server:

```
service cloudstack-management stop
```

b. Generate the encrypted equivalent of your vCenter password:

```
java -classpath /usr/share/cloudstack-common/lib/jasypt-1.9.0.jar
org.jasypt.intf.cli.JasyptPBEStringEncryptionCLI encrypt.sh
input="_your_vCenter_password_" password="`cat /etc/cloudstack/management/key`"
verbose=false
```

Store the output from this step, we need to add this in cluster_details table and vmware_data_center tables in place of the plain text password

c. Find the ID of the row of cluster_details table that you have to update:

```
mysql -u <username> -p<password>
```

```
select * from cloud.cluster_details;
```

d. Update the plain text password with the encrypted one

```
update cloud.cluster_details set value = '_ciphertext_from_step_1_' where id =
_id_from_step_2_;
```

e. Confirm that the table is updated:

```
select * from cloud.cluster_details;
```

f. Find the ID of the correct row of vmware_data_center that you want to update

```
select * from cloud.vmware_data_center;
```

g. update the plain text password with the encrypted one:

```
update cloud.vmware_data_center set password = '_ciphertext_from_step_1_' where
id = _id_from_step_5_;
```

h. Confirm that the table is updated:

```
select * from cloud.vmware_data_center;
```

i. Start the CloudStack Management server

```
service cloudstack-management start
```

11. (KVM only) Additional steps are required for each KVM host. These steps will not affect running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.
    a. Configure the CloudStack yum repository as detailed above.
    b. Stop the running agent.

```
# service cloud-agent stop
```

    c. Update the agent software.

```
# yum update cloudstack-agent
```

    d. Start the agent.

```
# service cloudstack-agent start
```

12. If you are using CentOS or RHEL, follow this procedure to upgrade your packages. If not, skip to step 14.

Community Packages

This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and yum repository, substitute your own URL for the ones used in these examples.

    a. The first order of business will be to change the yum repository for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent.

    (No changes should be necessary for hosts that are running VMware or Xen.)

    Start by opening **`/etc/yum.repos.d/cloudstack.repo`** on any systems that have CloudStack packages installed.

    This file should have content similar to the following:

```
[apache-cloudstack]
name=Apache CloudStack
baseurl=http://cloudstack.apt-get.eu/rhel/4.0/
enabled=1
gpgcheck=0
```

    If you are using the community provided package repository, change the base url to http://cloudstack.apt-get.eu/rhel/4.2/

    If you're using your own package repository, change this line to read as appropriate for your 4.2.1 repository.

    b. Now that you have the repository configured, it's time to install the **`cloudstack-management`** package by upgrading the older **`cloudstack-management`** package.

```
$ sudo yum upgrade cloudstack-management
```

    c. For KVM hosts, you will need to upgrade the **`cloud-agent`** package, similarly installing the new version as **`cloudstack-agent`**.

```
$ sudo yum upgrade cloudstack-agent
```

d. Verify that the file **/etc/cloudstack/agent/environment.properties** has a line that reads:

```
paths.script=/usr/share/cloudstack-common
```

If not, add the line.

e. Restart the agent:

```
service cloudstack-agent stop
killall jsvc
service cloudstack-agent start
```

13. Now it's time to restart the management server

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

14. Once you've upgraded the packages on your management servers, you'll need to restart the system VMs. Ensure that the admin port is set to 8096 by using the "integration.api.port" global parameter. This port is used by the cloud-sysvmadm script at the end of the upgrade procedure. For information about how to set this parameter, see "Setting Global Configuration Parameters" in the Installation Guide. Changing this parameter will require management server restart. Also make sure port 8096 is open in your local host firewall to do this.

    There is a script that will do this for you, all you need to do is run the script and supply the IP address for your MySQL instance and your MySQL credentials:

```
# nohup cloudstack-sysvmadm -d IP address -u cloud -p -a > sysvm.log 2>&1 &
```

    You can monitor the log for progress. The process of restarting the system VMs can take an hour or more.

```
# tail -f sysvm.log
```

    The output to **sysvm.log** will look something like this:

```
Stopping and starting 1 secondary storage vm(s)...
Done stopping and starting secondary storage vm(s)
Stopping and starting 1 console proxy vm(s)...
Done stopping and starting console proxy vm(s).
Stopping and starting 4 running routing vm(s)...
Done restarting router(s).
```

15. 

For Xen Hosts: Copy vhd-utils

This step is only for CloudStack installs that are using Xen hosts.

    Copy the file **vhd-utils** to **/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver**.

4.2. Upgrade from 4.1.x to 4.2.1

This section will guide you from CloudStack 4.1.x versions to CloudStack 4.2.1.

Any steps that are hypervisor-specific will be called out with a note.

We recommend reading through this section once or twice before beginning your upgrade procedure, and working through it on a test system before working on a production system.

1. Most users of CloudStack manage the installation and upgrades of CloudStack with one of Linux's predominant package systems, RPM or APT. This guide assumes you'll be using RPM and Yum (for Red Hat Enterprise Linux or CentOS), or APT and Debian packages (for Ubuntu).

2. 

Note

The following upgrade instructions should be performed regardless of hypervisor type.

    a. While running the existing 4.1.x system, log in to the UI as root administrator.
    b. In the left navigation bar, click Templates.
    c. In Select view, click Templates.
    d. Click Register template.
    The Register template dialog box is displayed.
    e. In the Register template dialog box, specify the following values (do not change these):

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.2 Description: systemvm-xenserver-4.2 URL:http://download.cloud.com/templates/4.2/systemvmtemplate-2013-07-12-master-xen.vhd.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no

	Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.2 Description: systemvm-kvm-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-2013-06-12-master-kvm.qcow2.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: KVM Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.2 Description: systemvm-vmware-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-4.2-vh7.ova Zone: Choose the zone where this hypervisor is used Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

3. Create RPM or Debian packages (as appropriate) and a repository from the 4.2.1 source, or check the Apache CloudStack downloads page at http://cloudstack.apache.org/downloads.html for package repositories supplied by community members. You will need them for step 8 or step 11.

   Instructions for creating packages from the CloudStack source are in the Installation Guide.

4. Stop your management server or servers. Run this on all management server hosts:

```
# service cloudstack-management stop
```

5. If you are running a usage server or usage servers, stop those as well:

```
# service cloudstack-usage stop
```

6. Make a backup of your MySQL database. If you run into any issues or need to roll back the upgrade, this will assist in debugging or restoring your existing environment. You'll be prompted for your password.

```
# mysqldump -u root -p cloud > cloudstack-backup.sql
```

7. (KVM Only) If primary storage of type local storage is in use, the path for this storage needs to be verified to ensure it passes new validation. Check local storage by querying the cloud.storage_pool table:

```
#mysql -u cloud -p -e "select id,name,path from cloud.storage_pool where
pool_type='Filesystem'"
```

   If local storage paths are found to have a trailing forward slash, remove it:

```
#mysql -u cloud -p -e 'update cloud.storage_pool set path="/var/lib/libvirt/images"
where path="/var/lib/libvirt/images/"';
```

8. If you are using Ubuntu, follow this procedure to upgrade your packages. If not, skip to step 11.

Community Packages

This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and APT repository, substitute your own URL for the ones used in these examples.

   a. The first order of business will be to change the sources list for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent. (No changes should be necessary for hosts that are running VMware or Xen.)

      Start by opening **`/etc/apt/sources.list.d/cloudstack.list`** on any systems that have CloudStack packages installed.

      This file should have one line, which contains:

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

      We'll change it to point to the new package repository:

```
deb http://cloudstack.apt-get.eu/ubuntu precise 4.2
```

      If you're using your own package repository, change this line to read as appropriate for your 4.2.1

repository.

b. Now update your apt package list:

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

c. Now that you have the repository configured, it's time to install the **`cloudstack-management`** package. This will pull in any other dependencies you need.

```
$ sudo apt-get install cloudstack-management
```

d. You will need to manually install the **`cloudstack-agent`** package:

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

During the installation of **`cloudstack-agent`**, APT will copy your **`agent.properties`**, **`log4j-cloud.xml`**, and **`environment.properties`** from **`/etc/cloud/agent`** to **`/etc/cloudstack/agent`**.

When prompted whether you wish to keep your configuration, say Yes.

e. Verify that the file **`/etc/cloudstack/agent/environment.properties`** has a line that reads:

```
paths.script=/usr/share/cloudstack-common
```

If not, add the line.

f. Restart the agent:

```
service cloudstack-agent stop
killall jsvc
service cloudstack-agent start
```

9. (VMware only) Additional steps are required for each VMware cluster. These steps will not affect running guests in the cloud. These steps are required only for clouds using VMware clusters:

a. Stop the Management Server:

```
service cloudstack-management stop
```

b. Generate the encrypted equivalent of your vCenter password:

```
java -classpath /usr/share/cloudstack-common/lib/jasypt-1.9.0.jar
org.jasypt.intf.cli.JasyptPBEStringEncryptionCLI encrypt.sh
input="_your_vCenter_password_" password="`cat /etc/cloudstack/management/key`"
verbose=false
```

Store the output from this step, we need to add this in cluster_details table and vmware_data_center tables in place of the plain text password

c. Find the ID of the row of cluster_details table that you have to update:

```
mysql -u <username> -p<password>
```

```
select * from cloud.cluster_details;
```

d. Update the plain text password with the encrypted one

```
update cloud.cluster_details set value = '_ciphertext_from_step_1_' where id =
_id_from_step_2_;
```

e. Confirm that the table is updated:

```
select * from cloud.cluster_details;
```

f. Find the ID of the correct row of vmware_data_center that you want to update

```
select * from cloud.vmware_data_center;
```

g. update the plain text password with the encrypted one:

```
update cloud.vmware_data_center set password = '_ciphertext_from_step_1_' where
id = _id_from_step_5_;
```

h. Confirm that the table is updated:

```
select * from cloud.vmware_data_center;
```

i. Start the CloudStack Management server

```
service cloudstack-management start
```

10. (KVM only) Additional steps are required for each KVM host. These steps will not affect running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.

a. Configure the CloudStack yum repository as detailed above.

b. Stop the running agent.

```
# service cloud-agent stop
```

c. Update the agent software.

```
# yum update cloudstack-agent
```

d. Start the agent.

```
# service cloudstack-agent start
```

11. If you are using CentOS or RHEL, follow this procedure to upgrade your packages. If not, skip to step 13.

    Community Packages

    This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and yum repository, substitute your own URL for the ones used in these examples.

    a. The first order of business will be to change the yum repository for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent.

    (No changes should be necessary for hosts that are running VMware or Xen.)

    Start by opening **/etc/yum.repos.d/cloudstack.repo** on any systems that have CloudStack packages installed.

    This file should have content similar to the following:

    ```
    [apache-cloudstack]
    name=Apache CloudStack
    baseurl=http://cloudstack.apt-get.eu/rhel/4.0/
    enabled=1
    gpgcheck=0
    ```

    If you are using the community provided package repository, change the base url to http://cloudstack.apt-get.eu/rhel/4.2/

    If you're using your own package repository, change this line to read as appropriate for your 4.2.1 repository.

    b. Now that you have the repository configured, it's time to install the **cloudstack-management** package by upgrading the older **cloudstack-management** package.

    ```
    $ sudo yum upgrade cloudstack-management
    ```

    c. For KVM hosts, you will need to upgrade the **cloud-agent** package, similarly installing the new version as **cloudstack-agent**.

    ```
    $ sudo yum upgrade cloudstack-agent
    ```

    d. Verify that the file **/etc/cloudstack/agent/environment.properties** has a line that reads:

    ```
    paths.script=/usr/share/cloudstack-common
    ```

    If not, add the line.

    e. Restart the agent:

    ```
    service cloudstack-agent stop
    killall jsvc
    service cloudstack-agent start
    ```

12. Now it's time to restart the management server

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

13. Once you've upgraded the packages on your management servers, you'll need to restart the system VMs. Ensure that the admin port is set to 8096 by using the "integration.api.port" global parameter. This port is used by the cloud-sysvmadm script at the end of the upgrade procedure. For information about how to set this parameter, see "Setting Global Configuration Parameters" in the Installation Guide. Changing this parameter will require management server restart. Also make sure port 8096 is open in your local host firewall to do this.

    There is a script that will do this for you, all you need to do is run the script and supply the IP address for your MySQL instance and your MySQL credentials:

    ```
    # nohup cloudstack-sysvmadm -d IP address -u cloud -p -a > sysvm.log 2>&1 &
    ```

    You can monitor the log for progress. The process of restarting the system VMs can take an hour or more.

    ```
    # tail -f sysvm.log
    ```

    The output to **sysvm.log** will look something like this:

    ```
    Stopping and starting 1 secondary storage vm(s)...
    Done stopping and starting secondary storage vm(s)
    Stopping and starting 1 console proxy vm(s)...
    Done stopping and starting console proxy vm(s).
    Stopping and starting 4 running routing vm(s)...
    Done restarting router(s).
    ```

14. **For Xen Hosts: Copy vhd-utils**

    This step is only for CloudStack installs that are using Xen hosts.

    Copy the file **vhd-utils** to **/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver**.

4.3. Upgrade from 4.0.x to 4.2.1

This section will guide you from CloudStack 4.0.x versions to CloudStack 4.2.1.

Any steps that are hypervisor-specific will be called out with a note.

Package Structure Changes

The package structure for CloudStack has changed significantly since the 4.0.x releases. If you've compiled your own packages, you'll notice that the package names and the number of packages has changed. This is *not* a bug. However, this *does* mean that the procedure is not as simple as an **`apt-get upgrade`** or **`yum update`**, so please follow this section carefully.

We recommend reading through this section once or twice before beginning your upgrade procedure, and working through it on a test system before working on a production system.

1. Most users of CloudStack manage the installation and upgrades of CloudStack with one of Linux's predominant package systems, RPM or APT. This guide assumes you'll be using RPM and Yum (for Red Hat Enterprise Linux or CentOS), or APT and Debian packages (for Ubuntu).

   Create RPM or Debian packages (as appropriate) and a repository from the 4.1.0 source, or check the Apache CloudStack downloads page at http://cloudstack.apache.org/downloads.html for package repositories supplied by community members. You will need them for step 9 or step 10.

   Instructions for creating packages from the CloudStack source are in the Installation Guide.

2. 

   Note

   The following upgrade instructions should be performed regardless of hypervisor type.

   a. While running the existing 4.0.0 system, log in to the UI as root administrator.
   b. In the left navigation bar, click Templates.
   c. In Select view, click Templates.
   d. Click Register template.

      The Register template dialog box is displayed.

   e. In the Register template dialog box, specify the following values (do not change these):

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.2 Description: systemvm-xenserver-4.2 URL:http://download.cloud.com/templates/4.2/systemvmtemplate-2013-07-12-master-xen.vhd.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.2 Description: systemvm-kvm-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-2013-06-12-master-kvm.qcow2.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: KVM Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.2 Description: systemvm-vmware-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-4.2-vh7.ova Zone: Choose the zone where this hypervisor is used Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

3. Stop your management server or servers. Run this on all management server hosts:

```
# service cloud-management stop
```

4. If you are running a usage server or usage servers, stop those as well:

```
# service cloud-usage stop
```

5. Make a backup of your MySQL database. If you run into any issues or need to roll back the upgrade, this will assist in debugging or restoring your existing environment. You'll be prompted for your password.

```
# mysqldump -u root -p cloud > cloudstack-backup.sql
```

6. Whether you're upgrading a Red Hat/CentOS based system or Ubuntu based system, you're going to need to stop the CloudStack management server before proceeding.

```
# service cloud-management stop
```

7. If you have made changes to **`/etc/cloud/management/components.xml`**, you'll need to carry these over manually to the new file, **`/etc/cloudstack/management/componentContext.xml`**. This is not done automatically. (If you're unsure, we recommend making a backup of the original **`components.xml`** to be on the safe side.
8. After upgrading to 4.2.1, API clients are expected to send plain text passwords for login and user creation, instead of MD5 hash. Incase, api client changes are not acceptable, following changes are to be made for backward compatibility:

   Modify componentsContext.xml, and make PlainTextUserAuthenticator as the default authenticator (1st entry in the userAuthenticators adapter list is default)

```
<!-- Security adapters -->
<bean id="userAuthenticators" class="com.cloud.utils.component.AdapterList">
  <property name="Adapters">
    <list>
      <ref bean="PlainTextUserAuthenticator"/>
      <ref bean="MD5UserAuthenticator"/>
      <ref bean="LDAPUserAuthenticator"/>
    </list>
  </property>
</bean>
```

   PlainTextUserAuthenticator works the same way MD5UserAuthenticator worked prior to 4.2.1.
9. If you are using Ubuntu, follow this procedure to upgrade your packages. If not, skip to step 10.

Community Packages

This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and APT repository, substitute your own URL for the ones used in these examples.

   a. The first order of business will be to change the sources list for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent. (No changes should be necessary for hosts that are running VMware or Xen.)

      Start by opening **`/etc/apt/sources.list.d/cloudstack.list`** on any systems that have CloudStack packages installed.

      This file should have one line, which contains:

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

      We'll change it to point to the new package repository:

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

      If you're using your own package repository, change this line to read as appropriate for your 4.1.0 repository.

   b. Now update your apt package list:

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

   c. Now that you have the repository configured, it's time to install the **`cloudstack-management`** package. This will pull in any other dependencies you need.

```
$ sudo apt-get install cloudstack-management
```

   d. You will need to manually install the **`cloudstack-agent`** package:

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

      During the installation of **`cloudstack-agent`**, APT will copy your **`agent.properties`**, **`log4j-cloud.xml`**, and **`environment.properties`** from **`/etc/cloud/agent`** to **`/etc/cloudstack/agent`**.

      When prompted whether you wish to keep your configuration, say Yes.

   e. Verify that the file **`/etc/cloudstack/agent/environment.properties`** has a line that reads:

```
paths.script=/usr/share/cloudstack-common
```

      If not, add the line.

   f. Restart the agent:

```
service cloud-agent stop
killall jsvc
service cloudstack-agent start
```

g. During the upgrade, **`log4j-cloud.xml`** was simply copied over, so the logs will continue to be added to **`/var/log/cloud/agent/agent.log`**. There's nothing *wrong* with this, but if you prefer to be consistent, you can change this by copying over the sample configuration file:

```
cd /etc/cloudstack/agent
mv log4j-cloud.xml.dpkg-dist log4j-cloud.xml
service cloudstack-agent restart
```

h. Once the agent is running, you can uninstall the old cloud-* packages from your system:

```
sudo dpkg --purge cloud-agent
```

10. If you are using CentOS or RHEL, follow this procedure to upgrade your packages. If not, skip to step 11.

Community Packages

This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and yum repository, substitute your own URL for the ones used in these examples.

a. The first order of business will be to change the yum repository for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent. (No changes should be necessary for hosts that are running VMware or Xen.)

Start by opening **`/etc/yum.repos.d/cloudstack.repo`** on any systems that have CloudStack packages installed.

This file should have content similar to the following:

```
[apache-cloudstack]
name=Apache CloudStack
baseurl=http://cloudstack.apt-get.eu/rhel/4.0/
enabled=1
gpgcheck=0
```

If you are using the community provided package repository, change the baseurl to http://cloudstack.apt-get.eu/rhel/4.1/

If you're using your own package repository, change this line to read as appropriate for your 4.2.1 repository.

b. Now that you have the repository configured, it's time to install the **`cloudstack-management`** package by upgrading the older **`cloud-client`** package.

```
$ sudo yum upgrade cloud-client
```

c. For KVM hosts, you will need to upgrade the **`cloud-agent`** package, similarly installing the new version as **`cloudstack-agent`**.

```
$ sudo yum upgrade cloud-agent
```

During the installation of **`cloudstack-agent`**, the RPM will copy your **`agent.properties`**, **`log4j-cloud.xml`**, and **`environment.properties`** from **`/etc/cloud/agent`** to **`/etc/cloudstack/agent`**.

d. Verify that the file **`/etc/cloudstack/agent/environment.properties`** has a line that reads:

```
paths.script=/usr/share/cloudstack-common
```

If not, add the line.

e. Restart the agent:

```
service cloud-agent stop
killall jsvc
service cloudstack-agent start
```

11. Once you've upgraded the packages on your management servers, you'll need to restart the system VMs. Make sure port 8096 is open in your local host firewall to do this.

There is a script that will do this for you, all you need to do is run the script and supply the IP address for your MySQL instance and your MySQL credentials:

```
# nohup cloudstack-sysvmadm -d IP address -u cloud -p -a > sysvm.log 2>&1 &
```

You can monitor the log for progress. The process of restarting the system VMs can take an hour or more.

```
# tail -f sysvm.log
```

The output to **`sysvm.log`** will look something like this:

```
Stopping and starting 1 secondary storage vm(s)...
Done stopping and starting secondary storage vm(s)
Stopping and starting 1 console proxy vm(s)...
Done stopping and starting console proxy vm(s).
Stopping and starting 4 running routing vm(s)...
Done restarting router(s).
```

12. **For Xen Hosts: Copy vhd-utils**

    This step is only for CloudStack installs that are using Xen hosts.

    Copy the file **vhd-utils** to **/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver**.

4.4. Upgrade from 3.0.x to 4.2.1

This section will guide you from Citrix CloudStack 3.0.x to Apache CloudStack 4.2.1. Sections that are hypervisor-specific will be called out with a note.

1. **Note**

   The following upgrade instructions should be performed regardless of hypervisor type.

   a. While running the existing 3.0.x system, log in to the UI as root administrator.
   b. In the left navigation bar, click Templates.
   c. In Select view, click Templates.
   d. Click Register template.
      The Register template dialog box is displayed.
   e. In the Register template dialog box, specify the following values (do not change these):

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.2 Description: systemvm-xenserver-4.2 URL:http://download.cloud.com/templates/4.2/systemvmtemplate-2013-07-12-master-xen.vhd.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.2 Description: systemvm-kvm-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-2013-06-12-master-kvm.qcow2.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: KVM Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.2 Description: systemvm-vmware-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-4.2-vh7.ova Zone: Choose the zone where this hypervisor is used Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

   f. Watch the screen to be sure that the template downloads successfully and enters the READY state. Do not proceed until this is successful.

2. (KVM on RHEL 6.0/6.1 only) If your existing CloudStack deployment includes one or more clusters of KVM hosts running RHEL 6.0 or RHEL 6.1, perform the following:
   a. Ensure that you upgrade the operating system version on those hosts before upgrading CloudStack
      To do that, change the yum repository for each system with CloudStack packages, that implies that all the Management Servers and any hosts that have the KVM agent.
   b. Open **/etc/yum.repos.d/cloudstack.repo** on any systems that have CloudStack packages installed.

c. Edit as follows:

```
[upgrade]
name=rhel63
baseurl=url-of-your-rhel6.3-repo
enabled=1
gpgcheck=0
[apache CloudStack]
name= Apache CloudStack
baseurl= http://cloudstack.apt-get.eu/rhel/4.0/
enabled=1
gpgcheck=0
```

If you are using the community provided package repository, change the baseurl to http:// cloudstack.apt-get.eu/rhel/4.2/

If you are using your own package repository, change this line to read as appropriate for your 4.2.0 repository.

d. Now that you have the repository configured, upgrade the host operating system from RHEL 6.0 to 6.3:

```
# yum upgrade
```

3. Stop all Usage Servers if running. Run this on all Usage Server hosts.

```
# service cloud-usage stop
```

4. Stop the Management Servers. Run this on all Management Server hosts.

```
# service cloud-management stop
```

5. On the MySQL master, take a backup of the MySQL databases. We recommend performing this step even in test upgrades. If there is an issue, this will assist with debugging.

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.

```
# mysqldump -u root -pmysql_password cloud > cloud-backup.dmp
# mysqldump -u root -pmysql_password cloud_usage > cloud-usage-backup.dmp
```

6. Either build RPM/DEB packages as detailed in the Installation Guide, or use one of the community provided yum/apt repositories to gain access to the CloudStack binaries.
7. If you are using Ubuntu, follow this procedure to upgrade your packages. If not, skip to step 8.

Community Packages

This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and APT repository, substitute your own URL for the ones used in these examples.

a. The first order of business will be to change the sources list for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent. (No changes should be necessary for hosts that are running VMware or Xen.)

Start by opening **/etc/apt/sources.list.d/cloudstack.list** on any systems that have CloudStack packages installed.

This file should have one line, which contains:

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

We'll change it to point to the new package repository:

```
deb http://cloudstack.apt-get.eu/ubuntu precise 4.2
```

If you're using your own package repository, change this line to read as appropriate for your 4.2.1 repository.

b. Now update your apt package list:

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

c. Now that you have the repository configured, it's time to install the **cloudstack-management** package. This will pull in any other dependencies you need.

```
$ sudo apt-get install cloudstack-management
```

d. You will need to manually install the **cloudstack-agent** package:

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

During the installation of **cloudstack-agent**, APT will copy your **agent.properties**, **log4j-cloud.xml**, and **environment.properties** from **/etc/cloud/agent** to **/etc/cloudstack/agent**.

When prompted whether you wish to keep your configuration, say Yes.

e. Verify that the file **/etc/cloudstack/agent/environment.properties** has a line that reads:

```
paths.script=/usr/share/cloudstack-common
```

If not, add the line.

f. Restart the agent:

```
service cloud-agent stop
killall jsvc
service cloudstack-agent start
```

g. During the upgrade, **`log4j-cloud.xml`** was simply copied over, so the logs will continue to be added to **`/var/log/cloud/agent/agent.log`**. There's nothing *wrong* with this, but if you prefer to be consistent, you can change this by copying over the sample configuration file:

```
cd /etc/cloudstack/agent
mv log4j-cloud.xml.dpkg-dist log4j-cloud.xml
service cloudstack-agent restart
```

h. Once the agent is running, you can uninstall the old cloud-* packages from your system:

```
sudo dpkg --purge cloud-agent
```

8. If you are using CentOS or RHEL, follow this procedure to upgrade your packages. If not, skip to step 9.

Community Packages

This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and yum repository, substitute your own URL for the ones used in these examples.

a. The first order of business will be to change the yum repository for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent. (No changes should be necessary for hosts that are running VMware or Xen.)

Start by opening **`/etc/yum.repos.d/cloudstack.repo`** on any systems that have CloudStack packages installed.

This file should have content similar to the following:

```
[apache-cloudstack]
name=Apache CloudStack
baseurl=http://cloudstack.apt-get.eu/rhel/4.0/
enabled=1
gpgcheck=0
```

If you are using the community provided package repository, change the baseurl to http://cloudstack.apt-get.eu/rhel/4.2/

If you're using your own package repository, change this line to read as appropriate for your 4.2.0 repository.

b. Now that you have the repository configured, it's time to install the **`cloudstack-management`** package by upgrading the older **`cloud-client`** package.

```
$ sudo yum upgrade cloud-client
```

c. For KVM hosts, you will need to upgrade the **`cloud-agent`** package, similarly installing the new version as **`cloudstack-agent`**.

```
$ sudo yum upgrade cloud-agent
```

During the installation of **`cloudstack-agent`**, the RPM will copy your **`agent.properties`**, **`log4j-cloud.xml`**, and **`environment.properties`** from **`/etc/cloud/agent`** to **`/etc/cloudstack/agent`**.

d. Verify that the file **`/etc/cloudstack/agent/environment.properties`** has a line that reads:

```
paths.script=/usr/share/cloudstack-common
```

If not, add the line.

e. Restart the agent:

```
service cloud-agent stop
killall jsvc
service cloudstack-agent start
```

9. If you have made changes to your copy of **`/etc/cloud/management/components.xml`** the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 4.2.0.

a. Make a backup copy of **`/etc/cloud/management/components.xml`**. For example:

```
# mv /etc/cloud/management/components.xml /etc/cloud/management/components.xml-
backup
```

b. Copy **`/etc/cloud/management/components.xml.rpmnew`** to create a new **`/etc/cloud/management/components.xml`**:

```
# cp -ap /etc/cloud/management/components.xml.rpmnew
/etc/cloud/management/components.xml
```

c. Merge your changes from the backup file into the new **`components.xml`**.

```
# vi /etc/cloudstack/management/components.xml
```

Note

If you have more than one management server node, repeat the upgrade steps on each node.

10. After upgrading to 4.2.1, API clients are expected to send plain text passwords for login and user creation, instead of MD5 hash. Incase, api client changes are not acceptable, following changes are to be made for backward compatibility:

    Modify componentContext.xml, and make PlainTextUserAuthenticator as the default authenticator (1st entry in the userAuthenticators adapter list is default)

    ```
    <!-- Security adapters -->
    <bean id="userAuthenticators" class="com.cloud.utils.component.AdapterList">
      <property name="Adapters">
        <list>
          <ref bean="PlainTextUserAuthenticator"/>
          <ref bean="MD5UserAuthenticator"/>
          <ref bean="LDAPUserAuthenticator"/>
        </list>
      </property>
    </bean>
    ```

    PlainTextUserAuthenticator works the same way MD5UserAuthenticator worked prior to 4.2.1

11. Start the first Management Server. Do not start any other Management Server nodes yet.

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

    Wait until the databases are upgraded. Ensure that the database upgrade is complete. After confirmation, start the other Management Servers one at a time by running the same command on each node.

    Note

    Failing to restart the Management Server indicates a problem in the upgrade. Having the Management Server restarted without any issues indicates that the upgrade is successfully completed.

12. Start all Usage Servers (if they were running on your previous version). Perform this on each Usage Server host.

    # service cloudstack-usage start

13. Additional steps are required for each KVM host. These steps will not affect running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.
    a. Configure a yum or apt repository containing the CloudStack packages as outlined in the Installation Guide.
    b. Stop the running agent.

       # service cloud-agent stop

    c. Update the agent software with one of the following command sets as appropriate for your environment.

       # yum update cloud-*

       # apt-get update

       # apt-get upgrade cloud-*

    d. Edit **/etc/cloudstack/agent/agent.properties** to change the resource parameter from "com.cloud.agent.resource.computing.LibvirtComputingResource" to "com.cloud.hypervisor.kvm.resource.LibvirtComputingResource".
    e. Upgrade all the existing bridge names to new bridge names by running this script:

       ```
       # cloudstack-agent-upgrade
       ```

    f. Install a libvirt hook with the following commands:

       ```
       # mkdir /etc/libvirt/hooks
       # cp /usr/share/cloudstack-agent/lib/libvirtqemuhook /etc/libvirt/hooks/qemu
       # chmod +x /etc/libvirt/hooks/qemu
       ```

    g. Restart libvirtd.

       ```
       # service libvirtd restart
       ```

    h. Start the agent.

       ```
       # service cloudstack-agent start
       ```

    i. When the Management Server is up and running, log in to the CloudStack UI and restart the virtual router for proper functioning of all the features.
14. Log in to the CloudStack UI as administrator, and check the status of the hosts. All hosts should come to Up state (except those that you know to be offline). You may need to wait 20 or 30 minutes, depending on the number of hosts.

    Note

    Troubleshooting: If login fails, clear your browser cache and reload the page.

    Do not proceed to the next step until the hosts show in Up state.
15. If you are upgrading from 3.0.x, perform the following:

a. Ensure that the admin port is set to 8096 by using the "integration.api.port" global parameter.

   This port is used by the cloud-sysvmadm script at the end of the upgrade procedure. For information about how to set this parameter, see "Setting Global Configuration Parameters" in the Installation Guide.

b. Restart the Management Server.

Note

If you don't want the admin port to remain open, you can set it to null after the upgrade is done and restart the management server.

16. Run the **cloudstack-sysvmadm** script to stop, then start, all Secondary Storage VMs, Console Proxy VMs, and virtual routers. Run the script once on each management server. Substitute your own IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the **-c** and **-r** arguments. For example:

    ```
    # nohup cloudstack-sysvmadm -d 192.168.1.5 -u cloud -p password -c -r > sysvm.log 2>&1 &
    # tail -f sysvm.log
    ```

    This might take up to an hour or more to run, depending on the number of accounts in the system.

17. If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudStack 4.2.1. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudStack 4.2.1 Installation Guide under "Upgrading XenServer Versions."

18. Now apply the XenServer hotfix XS602E003 (and any other needed hotfixes) to XenServer v6.0.2 hypervisor hosts.

    a. Disconnect the XenServer cluster from CloudStack.

       In the left navigation bar of the CloudStack UI, select Infrastructure. Under Clusters, click View All. Select the XenServer cluster and click Actions - Unmanage.

       This may fail if there are hosts not in one of the states Up, Down, Disconnected, or Alert. You may need to fix that before unmanaging this cluster.

       Wait until the status of the cluster has reached Unmanaged. Use the CloudStack UI to check on the status. When the cluster is in the unmanaged state, there is no connection to the hosts in the cluster.

    b. To clean up the VLAN, log in to one XenServer host and run:

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

    c. Now prepare the upgrade by running the following on one XenServer host:

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

       If you see a message like "can't eject CD", log in to the VM and unmount the CD, then run this script again.

    d. Upload the hotfix to the XenServer hosts. Always start with the Xen pool master, then the slaves. Using your favorite file copy utility (e.g. WinSCP), copy the hotfixes to the host. Place them in a temporary folder such as /tmp.

       On the Xen pool master, upload the hotfix with this command:

       ```
       xe patch-upload file-name=XS602E003.xsupdate
       ```

       Make a note of the output from this command, which is a UUID for the hotfix file. You'll need it in another step later.

Note

(Optional) If you are applying other hotfixes as well, you can repeat the commands in this section with the appropriate hotfix number. For example, XS602E004.xsupdate.

    e. Manually live migrate all VMs on this host to another host. First, get a list of the VMs on this host:

       ```
       # xe vm-list
       ```

       Then use this command to migrate each VM. Replace the example host name and VM name with your own:

       ```
       # xe vm-migrate live=true host=host-name vm=VM-name
       ```

Troubleshooting

If you see a message like "You attempted an operation on a VM which requires PV drivers to be installed but the drivers were not detected," run: **/opt/xensource/bin/make_migratable.sh b6cf79c8-02ee-050b-922f-49583d9f1a14**.

    f. Apply the hotfix. First, get the UUID of this host:

       ```
       # xe host-list
       ```

       Then use the following command to apply the hotfix. Replace the example host UUID with the current host ID, and replace the hotfix UUID with the output from the patch-upload command you ran on this machine earlier. You can also get the hotfix UUID by running xe patch-list.

       ```
       xe patch-apply host-uuid=host-uuid uuid=hotfix-uuid
       ```

    g. Copy the following files from the CloudStack Management Server to the host.

Copy from here...	...to here
/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver/xenserver60/NFSSR.py	/opt/xensource/sm/NFSSR.py
/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver/setupxenserver.sh	/opt/xensource/bin/setupxenserver.sh
/usr/lib64/cloud/common/scripts/vm/hypervisor/xenserver/make_migratable.sh	/opt/xensource/bin/make_migratable.sh

h. (Only for hotfixes XS602E005 and XS602E007) You need to apply a new Cloud Support Pack.
   - Download the CSP software onto the XenServer host from one of the following links:
     For hotfix XS602E005: http://coltrane.eng.hq.xensource.com/release/XenServer-6.x/XS-6.0.2/hotfixes/XS602E005/56710/xe-phase-2/xenserver-cloud-supp.tgz
     For hotfix XS602E007: http://coltrane.eng.hq.xensource.com/release/XenServer-6.x/XS-6.0.2/hotfixes/XS602E007/57824/xe-phase-2/xenserver-cloud-supp.tgz
   - Extract the file:

     ```
     # tar xf xenserver-cloud-supp.tgz
     ```
   - Run the following script:

     ```
     # xe-install-supplemental-pack xenserver-cloud-supp.iso
     ```
   - If the XenServer host is part of a zone that uses basic networking, disable Open vSwitch (OVS):

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

i. Reboot this XenServer host.
j. Run the following:

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

   Note

   If the message "mv: cannot stat `/etc/cron.daily/logrotate': No such file or directory" appears, you can safely ignore it.

k. Run the following:

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

l. On each slave host in the Xen pool, repeat these steps, starting from "manually live migrate VMs."

Troubleshooting Tip

If passwords which you know to be valid appear not to work after upgrade, or other UI issues are seen, try clearing your browser cache and reloading the UI page.

4.5. Upgrade from 2.2.14 to 4.2.1

1. Ensure that you query your IPaddress usage records and process them; for example, issue invoices for any usage that you have not yet billed users for.
   Starting in 3.0.2, the usage record format for IP addresses is the same as the rest of the usage types. Instead of a single record with the assignment and release dates, separate records are generated per aggregation period with start and end dates. After upgrading to 4.2.1, any existing IP address usage records in the old format will no longer be available.
2. If you are using version 2.2.0 - 2.2.13, first upgrade to 2.2.14 by using the instructions in the 2.2.14 Release Notes.

   KVM Hosts

   If KVM hypervisor is used in your cloud, be sure you completed the step to insert a valid username and password into the host_details table on each KVM node as described in the 2.2.14 Release Notes. This step is critical, as the database will be encrypted after the upgrade to 4.2.1.

3. While running the 2.2.14 system, log in to the UI as root administrator.
4. Using the UI, add a new System VM template for each hypervisor type that is used in your cloud. In each zone, add a system VM template for each hypervisor used in that zone
   a. In the left navigation bar, click Templates.
   b. In Select view, click Templates.
   c. Click Register template.
      The Register template dialog box is displayed.
   d. In the Register template dialog box, specify the following values depending on the hypervisor type (do not change these):

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.2 Description: systemvm-xenserver-4.2 URL:http://download.cloud.com/templates/4.2/systemvmtemplate-2013-07-12-master-xen.vhd.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian

	release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.2 Description: systemvm-kvm-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-2013-06-12-master-kvm.qcow2.bz2 Zone: Choose the zone where this hypervisor is used Hypervisor: KVM Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.2 Description: systemvm-vmware-4.2 URL: http://download.cloud.com/templates/4.2/systemvmtemplate-4.2-vh7.ova Zone: Choose the zone where this hypervisor is used Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

5. Watch the screen to be sure that the template downloads successfully and enters the READY state. Do not proceed until this is successful
6. **WARNING**: If you use more than one type of hypervisor in your cloud, be sure you have repeated these steps to download the system VM template for each hypervisor type. Otherwise, the upgrade will fail.
7. (KVM on RHEL 6.0/6.1 only) If your existing CloudStack deployment includes one or more clusters of KVM hosts running RHEL 6.0 or RHEL 6.1, perform the following:
    a. Ensure that you upgrade the operating system version on those hosts before upgrading CloudStack

       To do that, change the yum repository for each system with CloudStack packages, that implies that all the Management Servers and any hosts that have the KVM agent.
    b. Open **`/etc/yum.repos.d/cloudstack.repo`** on any systems that have CloudStack packages installed.
    c. Edit as follows:

       ```
       [upgrade]
       name=rhel63
       baseurl=url-of-your-rhel6.3-repo
       enabled=1
       gpgcheck=0
       [apache CloudStack]
       name= Apache CloudStack
       baseurl= http://cloudstack.apt-get.eu/rhel/4.2/
       enabled=1
       gpgcheck=0
       ```

       If you are using the community provided package repository, change the baseurl to http:// cloudstack.apt-get.eu/rhel/4.2/

       If you are using your own package repository, change this line to read as appropriate for your 4.2.0 repository.
    d. Now that you have the repository configured, upgrade the host operating system from RHEL 6.0 to 6.3:

       ```
       # yum upgrade
       ```
8. Stop all Usage Servers if running. Run this on all Usage Server hosts.

   ```
   # service cloud-usage stop
   ```
9. Stop the Management Servers. Run this on all Management Server hosts.

   ```
   # service cloud-management stop
   ```
10. On the MySQL master, take a backup of the MySQL databases. We recommend performing this step even in test upgrades. If there is an issue, this will assist with debugging.

    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.

    ```
    # mysqldump -u root -pmysql_password cloud > cloud-backup.dmp
    # mysqldump -u root -pmysql_password cloud_usage > cloud-usage-backup.dmp
    ```

11. Either build RPM/DEB packages as detailed in the Installation Guide, or use one of the community provided yum/apt repositories to gain access to the CloudStack binaries.
12. If you are using Ubuntu, follow this procedure to upgrade your packages. If not, skip to step 13.

Community Packages

This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and APT repository, substitute your own URL for the ones used in these examples.

    a. The first order of business will be to change the sources list for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent. (No changes should be necessary for hosts that are running VMware or Xen.)

    Start by opening **`/etc/apt/sources.list.d/cloudstack.list`** on any systems that have CloudStack packages installed.

    This file should have one line, which contains:

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

    We'll change it to point to the new package repository:

    ```
    deb http://cloudstack.apt-get.eu/ubuntu precise 4.2
    ```

    If you're using your own package repository, change this line to read as appropriate for your 4.2.0 repository.

    b. Now update your apt package list:

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

    c. Now that you have the repository configured, it's time to install the **`cloudstack-management`** package. This will pull in any other dependencies you need.

    ```
    $ sudo apt-get install cloudstack-management
    ```

    d. On KVM hosts, you will need to manually install the **`cloudstack-agent`** package:

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

    During the installation of **`cloudstack-agent`**, APT will copy your **`agent.properties`**, **`log4j-cloud.xml`**, and **`environment.properties`** from **`/etc/cloud/agent`** to **`/etc/cloudstack/agent`**.

    When prompted whether you wish to keep your configuration, say Yes.

    e. Verify that the file **`/etc/cloudstack/agent/environment.properties`** has a line that reads:

    ```
    paths.script=/usr/share/cloudstack-common
    ```

    If not, add the line.

    f. Restart the agent:

    ```
    service cloud-agent stop
    killall jsvc
    service cloudstack-agent start
    ```

    g. During the upgrade, **`log4j-cloud.xml`** was simply copied over, so the logs will continue to be added to **`/var/log/cloud/agent/agent.log`**. There's nothing *wrong* with this, but if you prefer to be consistent, you can change this by copying over the sample configuration file:

    ```
    cd /etc/cloudstack/agent
    mv log4j-cloud.xml.dpkg-dist log4j-cloud.xml
    service cloudstack-agent restart
    ```

    h. Once the agent is running, you can uninstall the old cloud-* packages from your system:

    ```
    sudo dpkg --purge cloud-agent
    ```

13. If you are using CentOS or RHEL, follow this procedure to upgrade your packages. If not, skip to step 14.

Community Packages

This section assumes you're using the community supplied packages for CloudStack. If you've created your own packages and yum repository, substitute your own URL for the ones used in these examples.

    a. The first order of business will be to change the yum repository for each system with CloudStack packages. This means all management servers, and any hosts that have the KVM agent. (No changes should be necessary for hosts that are running VMware or Xen.)

    Start by opening **`/etc/yum.repos.d/cloudstack.repo`** on any systems that have CloudStack packages installed.

    This file should have content similar to the following:

    ```
    [apache-cloudstack]
    name=Apache CloudStack
    baseurl=http://cloudstack.apt-get.eu/rhel/4.0/
    enabled=1
    gpgcheck=0
    ```

If you are using the community provided package repository, change the baseurl to http://cloudstack.apt-get.eu/rhel/4.2/

If you're using your own package repository, change this line to read as appropriate for your 4.2.1 repository.

b. Now that you have the repository configured, it's time to install the **cloudstack-management** package by upgrading the older **cloud-client** package.

```
$ sudo yum upgrade cloud-client
```

c. For KVM hosts, you will need to upgrade the **cloud-agent** package, similarly installing the new version as **cloudstack-agent**.

```
$ sudo yum upgrade cloud-agent
```

During the installation of **cloudstack-agent**, the RPM will copy your **agent.properties**, **log4j-cloud.xml**, and **environment.properties** from **/etc/cloud/agent** to **/etc/cloudstack/agent**.

d. Verify that the file **/etc/cloudstack/agent/environment.properties** has a line that reads:

```
paths.script=/usr/share/cloudstack-common
```

If not, add the line.

e. Restart the agent:

```
service cloud-agent stop
killall jsvc
service cloudstack-agent start
```

14. If you have made changes to your existing copy of the file components.xml in your previous-version CloudStack installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 4.0.0-incubating.

Note

How will you know whether you need to do this? If the upgrade output in the previous step included a message like the following, then some custom content was found in your old components.xml, and you need to merge the two files:

```
warning: /etc/cloud/management/components.xml created as
/etc/cloud/management/components.xml.rpmnew
```

a. Make a backup copy of your **/etc/cloud/management/components.xml** file. For example:

```
# mv /etc/cloud/management/components.xml
/etc/cloud/management/components.xml-backup
```

b. Copy **/etc/cloud/management/components.xml.rpmnew** to create a new **/etc/cloud/management/components.xml**:

```
# cp -ap /etc/cloud/management/components.xml.rpmnew
/etc/cloud/management/components.xml
```

c. Merge your changes from the backup file into the new components.xml file.

```
# vi /etc/cloudstack/management/components.xml
```

15. After upgrading to 4.2.1, API clients are expected to send plain text passwords for login and user creation, instead of MD5 hash. If API client changes are not acceptable, following changes are to be made for backward compatibility:

Modify componentContext.xml, and make PlainTextUserAuthenticator as the default authenticator (1st entry in the userAuthenticators adapter list is default)

```
<!-- Security adapters -->
<bean id="userAuthenticators" class="com.cloud.utils.component.AdapterList">
  <property name="Adapters">
    <list>
      <ref bean="PlainTextUserAuthenticator"/>
      <ref bean="MD5UserAuthenticator"/>
      <ref bean="LDAPUserAuthenticator"/>
    </list>
  </property>
</bean>
```

PlainTextUserAuthenticator works the same way MD5UserAuthenticator worked prior to 4.2.

16. If you have made changes to your existing copy of the **/etc/cloud/management/db.properties** file in your previous-version CloudStack installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with this version.

a. Make a backup copy of your file **/etc/cloud/management/db.properties**. For example:

```
# mv /etc/cloud/management/db.properties /etc/cloud/management/db.properties-
backup
```

b. Copy **/etc/cloud/management/db.properties.rpmnew** to create a new **/etc/cloud/management/db.properties**:

```
# cp -ap /etc/cloud/management/db.properties.rpmnew
etc/cloud/management/db.properties
```

c. Merge your changes from the backup file into the new db.properties file.

```
# vi /etc/cloudstack/management/db.properties
```

17. On the management server node, run the following command. It is recommended that you use the command-line flags to provide your own encryption keys. See Password and Key Encryption in the Installation Guide.

```
# cloudstack-setup-encryption -e encryption_type -m management_server_key -k
database_key
```

When used without arguments, as in the following example, the default encryption type and keys will be used:

- (Optional) For encryption_type, use file or web to indicate the technique used to pass in the database encryption password. Default: file.
- (Optional) For management_server_key, substitute the default key that is used to encrypt confidential parameters in the properties file. Default: password. It is highly recommended that you replace this with a more secure value
- (Optional) For database_key, substitute the default key that is used to encrypt confidential parameters in the CloudStack database. Default: password. It is highly recommended that you replace this with a more secure value.

18. Repeat steps 10 - 14 on every management server node. If you provided your own encryption key in step 14, use the same key on all other management servers.
19. Start the first Management Server. Do not start any other Management Server nodes yet.

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

Wait until the databases are upgraded. Ensure that the database upgrade is complete. You should see a message like "Complete! Done." After confirmation, start the other Management Servers one at a time by running the same command on each node.

20. Start all Usage Servers (if they were running on your previous version). Perform this on each Usage Server host.

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

21. (KVM only) Perform the following additional steps on each KVM host.

These steps will not affect running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.

a. Configure your CloudStack package repositories as outlined in the Installation Guide

b. Stop the running agent.

```
# service cloud-agent stop
```

c. Update the agent software with one of the following command sets as appropriate.

```
# yum update cloud-*
```

```
# apt-get update
# apt-get upgrade cloud-*
```

d. Copy the contents of the **agent.properties** file to the new **agent.properties** file by using the following command

```
sed -i
's/com.cloud.agent.resource.computing.LibvirtComputingResource/com.cloud.hyperv
isor.kvm.resource.LibvirtComputingResource/g'
/etc/cloudstack/agent/agent.properties
```

e. Upgrade all the existing bridge names to new bridge names by running this script:

```
# cloudstack-agent-upgrade
```

f. Install a libvirt hook with the following commands:

```
# mkdir /etc/libvirt/hooks
# cp /usr/share/cloudstack-agent/lib/libvirtqemuhook /etc/libvirt/hooks/qemu
# chmod +x /etc/libvirt/hooks/qemu
```

g. Restart libvirtd.

```
# service libvirtd restart
```

h. Start the agent.

```
# service cloudstack-agent start
```

i. When the Management Server is up and running, log in to the CloudStack UI and restart the virtual router for proper functioning of all the features.

22. Log in to the CloudStack UI as admin, and check the status of the hosts. All hosts should come to Up state (except those that you know to be offline). You may need to wait 20 or 30 minutes, depending on the number of hosts.

Do not proceed to the next step until the hosts show in the Up state. If the hosts do not come to the Up state, contact support.

23. Run the following script to stop, then start, all Secondary Storage VMs, Console Proxy VMs, and virtual routers.

a. Run the command once on one management server. Substitute your own IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those

parameters, provide the "-c" and "-r" arguments. For example:

```
# nohup cloudstack-sysvmadm -d 192.168.1.5 -u cloud -p password -c -r >
sysvm.log 2>&1 &
# tail -f sysvm.log
```

This might take up to an hour or more to run, depending on the number of accounts in the system.

b. After the script terminates, check the log to verify correct execution:

```
# tail -f sysvm.log
```

The content should be like the following:

```
                                Stopping and starting 1 secondary storage
vm(s)...
                                Done stopping and starting secondary storage
vm(s)
                                Stopping and starting 1 console proxy vm(s)...
                                Done stopping and starting console proxy vm(s).
                                Stopping and starting 4 running routing
vm(s)...
                                Done restarting router(s).
```

24. If you would like additional confirmation that the new system VM templates were correctly applied when these system VMs were rebooted, SSH into the System VM and check the version.

    Use one of the following techniques, depending on the hypervisor.

    XenServer or KVM:

    SSH in by using the link local IP address of the system VM. For example, in the command below, substitute your own path to the private key used to log in to the system VM and your own link local IP.

    Run the following commands on the XenServer or KVM host on which the system VM is present:

    ```
    # ssh -i private-key-path link-local-ip -p 3922
                          # cat /etc/cloudstack-release
    ```

    The output should be like the following:

    ```
    Cloudstack Release 4.0.0-incubating Mon Oct 9 15:10:04 PST 2012
    ```

    ESXi

    SSH in using the private IP address of the system VM. For example, in the command below, substitute your own path to the private key used to log in to the system VM and your own private IP.

    Run the following commands on the Management Server:

    ```
    # ssh -i private-key-path private-ip -p 3922
                           # cat /etc/cloudstack-release
    ```

    The output should be like the following:

    ```
    Cloudstack Release 4.0.0-incubating Mon Oct 9 15:10:04 PST 2012
    ```

25. If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudStack 4.0.0-incubating. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudStack 4.0.0-incubating Installation Guide.
26. Apply the XenServer hotfix XS602E003 (and any other needed hotfixes) to XenServer v6.0.2 hypervisor hosts.
    a. Disconnect the XenServer cluster from CloudStack.

       In the left navigation bar of the CloudStack UI, select Infrastructure. Under Clusters, click View All. Select the XenServer cluster and click Actions - Unmanage.

       This may fail if there are hosts not in one of the states Up, Down, Disconnected, or Alert. You may need to fix that before unmanaging this cluster.

       Wait until the status of the cluster has reached Unmanaged. Use the CloudStack UI to check on the status. When the cluster is in the unmanaged state, there is no connection to the hosts in the cluster.

    b. To clean up the VLAN, log in to one XenServer host and run:

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

    c. Prepare the upgrade by running the following on one XenServer host:

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

       If you see a message like "can't eject CD", log in to the VM and umount the CD, then run this script again.

    d. Upload the hotfix to the XenServer hosts. Always start with the Xen pool master, then the slaves. Using your favorite file copy utility (e.g. WinSCP), copy the hotfixes to the host. Place them in a temporary folder such as /root or /tmp.

       On the Xen pool master, upload the hotfix with this command:

       ```
       xe patch-upload file-name=XS602E003.xsupdate
       ```

       Make a note of the output from this command, which is a UUID for the hotfix file. You'll need it in another step later.

Note

(Optional) If you are applying other hotfixes as well, you can repeat the commands in this section with the appropriate hotfix number. For example, XS602E004.xsupdate.

e. Manually live migrate all VMs on this host to another host. First, get a list of the VMs on this host:

```
# xe vm-list
```

Then use this command to migrate each VM. Replace the example host name and VM name with your own:

```
# xe vm-migrate live=true host=host-name vm=VM-name
```

Troubleshooting

If you see a message like "You attempted an operation on a VM which requires PV drivers to be installed but the drivers were not detected," run:
/opt/xensource/bin/make_migratable.sh b6cf79c8-02ee-050b-922f-49583d9f1a14.

f. Apply the hotfix. First, get the UUID of this host:

```
# xe host-list
```

Then use the following command to apply the hotfix. Replace the example host UUID with the current host ID, and replace the hotfix UUID with the output from the patch-upload command you ran on this machine earlier. You can also get the hotfix UUID by running xe patch-list.

```
xe patch-apply host-uuid=host-uuid uuid=hotfix-uuid
```

g. Copy the following files from the CloudStack Management Server to the host.

Copy from here...	...to here
/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/lib64/cloudstack-common/scripts/vm/hypervisor/xenserver/make_migratable.sh	**/opt/xensource/bin/make_migratable.sh**

h. (Only for hotfixes XS602E005 and XS602E007) You need to apply a new Cloud Support Pack.

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

  For hotfix XS602E005: http://coltrane.eng.hq.xensource.com/release/XenServer-6.x/XS-6.0.2/hotfixes/XS602E005/56710/xe-phase-2/xenserver-cloud-supp.tgz

  For hotfix XS602E007: http://coltrane.eng.hq.xensource.com/release/XenServer-6.x/XS-6.0.2/hotfixes/XS602E007/57824/xe-phase-2/xenserver-cloud-supp.tgz
- Extract the file:

  ```
  # tar xf xenserver-cloud-supp.tgz
  ```
- Run the following script:

  ```
  # xe-install-supplemental-pack xenserver-cloud-supp.iso
  ```
- If the XenServer host is part of a zone that uses basic networking, disable Open vSwitch (OVS):

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

i. Reboot this XenServer host.

j. Run the following:

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

Note

If the message "mv: cannot stat `/etc/cron.daily/logrotate': No such file or directory" appears, you can safely ignore it.

k. Run the following:

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

l. On each slave host in the Xen pool, repeat these steps, starting from "manually live migrate VMs."

Chapter 5. API Changes from 4.2 to 4.2.1

Due to the Section 3.1.3, “Cisco UCS Enhancements”, the following API changes have been introduced:

- listUcsProfiles is deprecated.
- listUcsTemplates is added. This is to replace listUcsProfiles. Retrieve pre-created UCS templates from UCS Manager. Typically used when preparing to create a profile from the template and associate the profile to a selected blade.
- instantiateUcsTemplateAndAssocaciateToBlade is added. Associates a profile to a blade, using a given profile template. First call listUcsTemplates to get the template and listUcsBlade to get the blade.
- refreshUcsBlades is added. Syncs CloudStack with any changes that have been made on the UCS Manager side.