Citrix CloudPlatform (powered by Apache CloudStack) Version 4.3.0.1 Release Notes

Revised September 29, 2014 3:00 PM PST

Citrix CloudPlatform (powered by Apache CloudStack) Version 4.3.0.1 Release Notes
Revised September 29, 2014 3:00 PM PST

Release notes for Citrix CloudPlatform version 4.3.0.1

Submitting Feedback and Getting Help

The support team is available to help customers plan and execute their installations. To contact the support team, log in to *the Support Portal*[1] by using the account credentials you received when you purchased your support contract.

[1] http://support.citrix.com/cms/kc/cloud-home/

Support Matrix

This section describes the operating systems, browsers, and hypervisors that have been newly tested and certified compatible with CloudPlatform 4.3.0.1 Most earlier OS and hypervisor versions are also still supported for use with 4.3.0.1. For a complete list, see the System Requirements section of the CloudPlatform 4.3 Installation Guide.

2.1. Supported OS Versions for Management Server

- RHEL versions 5.5, 6.2, 6.3, and 6.4
- CentOS versions 5.10, 6.2, 6.3, and 6.4

2.2. Supported Hypervisor Versions

The following new hypervisor support has been added:

- Windows Server 2012 R2 (with Hyper-V Role enabled)
- Hyper-V Server 2012 R2
- XenServer version 6.2 SPI Hotfix XS62ESP1005
- XenServer version 6.2 SPI Hotfix XS62ESP1004
- XenServer version 6.2 SP1 Hotfix XS62ESP1003
- VMware vCenter 5.5

Other supported hypervisors for CloudPlatform:

- XenServer versions 5.6 SP2 with latest hotfixes.
- XenServer versions 6.0.2 with latest hotfixes (for CloudPlatform 3.0.2 and greater)
- XenServer versions 6.0 with latest hotfixes (for CloudPlatform 3.0.0 and greater)
- XenServer versions 6.1 with latest hotfixes.
- KVM versions 6.2 and 6.3
- VMware versions 5.0 Update 1B, 5.0 Update 3, and 5.1 Update 1C
- 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 CloudPlatform Installation Guide.

2.3. Supported External Devices

- Netscaler MPX versions 9.3 and 10.e
- Netscaler VPX versions 9.3 and 10.e
- Netscaler SDX version 9.3
- SRX (Model srx100b) versions 10.3 to 10.4 R7.5
- F5 11.X

2.4. System VM Templates

CloudPlatform 4.3.0.1 supports 64-bit System VM templates. This release does not provide 32-bit support for System VM templates.

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.3 Description: systemvm-xenserver-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-xen.vhd.bz2* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the XenServer zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit and 64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
Hyper-V	Name: systemvm-hyperv-4.3 Description: systemvm-hyperv-4.3

Hypervisor	Description
	URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-hyperv.vhd.bz2* [1] Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running Hyper-V, choose All Zones to make the template available in all the Hyper-V zones. Hypervisor: Hyper-V Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit and 64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.3 Description: systemvm-kvm-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-kvm.qcow2.bz2* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running KVM, choose All Zones to make the template available in all the KVM zones. Hypervisor: KVM Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (32-bit and 64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no

[1] http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-hyperv.vhd.bz2 2

Hypervisor	Description
	Public: no Featured: no
VMware	Name: systemvm-vmware-4.3 Description: systemvm-vmware-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-vmware.ova* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running VMware, choose All Zones to make the template available in all the VMware zones. 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

2.5. Supported Browsers

- Internet Explorer versions 10 and 11
- Firefox versions 26 or lower
- Google Chrome versions 31.0.1650.63
- Safari 7.0 (Mac)

2.6. Feature Parity Between CloudPlatform and Apache CloudStack

The following features are supported in Apache CloudStack but not in CloudPlatform. Though these features are available in CloudPlatform, Citrix does not provide any support. However, you can contact Citrix partners for support.

Feature Category	Feature Details
Network	KVM QinQ VLAN support
Network	Redundant virtual router

Feature Category	Feature Details
	This feature was available in version 3.0.3 to 3.0.6, and later removed in 4.2.
Network	Juniper Contrail SDN Plug-in
Network	Palo Alto Firewall Integration
Network	NS SSL Termination
SDN	Stratosphere SDN work
VR	VR Extension
VR	VR cleanup
Storage	Clustered LVM Storage support
Storage	Ceph RBD support
Storage	IOPS for data volumes in disk offering (Hypervisor or Storage based) for XenServer and VMware
Storage	IOPS for data volumes in disk offering (Hypervisor or Storage based) for KVM
Storage	IOPS for root volumes in compute offering (Hypervisor-based only)
Storage	Root volume resize
Storage	Volume provisioning type option: thin vs fat, for KVM
Storage	IOPS for root volumes in compute offering, for XenServer and VMware
Storage	Create GUI to add primary storage based on plug-ins
Security	SELinux support
Automation/ Puppet integration	Puppet integration
Console Proxy	Console Proxy enhancements
OS	Debian support
OS	LXC support
Management	Sync Domain/Account/User information across Regions
Management	Cloudstack event enhancements

The following are the unsupported UI options in CloudPlatform 4.3:

Unsupported UI Options	UI Wizard
Hypervisors: LXC, OVM	• Infrastructure > Zones > Add Zone • Infrastructure > Clusters > Add Cluster • Infrastructure > Sockets Templates > Register Templates • Other places where hypervisors are listed

Unsupported UI Options	UI Wizard
Isolation methods: GRE, VNS, SSP	Infrastructure > Zones > Add Zone (Advanced) > Setup Network > Isolation Method
Network Service providers: BigSwitch, MidoNet	Infrastructure > Zones > Select a Zone > Physical Network (Tab) > Select a Physical Network > Network Service Providers > Configure
Swift Storage	Infrastructure > Secondary Storage > Add Secondary Storage > Provider (Swift)
Disk IO Throttling (QoS) added by Solidfire	• Service Offerings > Add Compute Offering > Remove the following options: Disk read rate (BPS), Disk write rate (BPS), Disk read rate (IOPS), Disk write rate (IOPS) • Service Offerings > Add Disk Offering > QoS Type = Hypervisor > Remove the following options: Disk read rate (BPS), Disk write rate (BPS), Disk read rate (IOPS), Disk write rate (IOPS) • Service Offerings > Add Disk Offering > QoS Type = Storage > Remove the following options: Custom IOPS, Min IOPS, Max IOPS

Upgrade Instructions

3.1. Upgrade from 4.3.0 to 4.3.0.1

Perform the following to upgrade from version 4.3.0 to version 4.3.0.1.

1. Download the latest System VM templates:

   The System VM templates includes fixes for the OpenSSL HeartBleed vulnerability issues.

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.3 Description: systemvm-xenserver-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-xen.vhd.bz2* Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, select each zone and individually register the template to make the template available in all the XenServer zones. (Prior to version 4.3): Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.3 Description: systemvm-kvm-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/*

Hypervisor	Description
	systemvm64template-2014-06-23-master-kvm.qcow2.bz2 Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running KVM, select each zone and individually register the template to make the template available in all the zones. (Prior to version 4.3): Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the zones. Hypervisor: KVM Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.3 Description: systemvm-vmware-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-vmware.ova* Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running VMware, select each zone and individually register the template to make the template available in all the zones. (Prior to version 4.3): Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the zones. Hypervisor: VMware

Hypervisor	Description
	Format: OVA OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
Hyper-V (Applicable only for 4.3)	Name: systemvm-hyperv-4.3 Description: systemvm-hyperv-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-hyperv.vhd.bz2* [1] Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running Hyper-V, choose All Zones to make the template available in all the XenServer zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

2. Ensure that the latest System VM are copied to all the primary storages.

3. (KVM on RHEL 6.0/6.1 only) If your existing CloudPlatform deployment includes one or more clusters of KVM hosts running RHEL 6.0 or RHEL 6.1, you must first upgrade the operating system version on those hosts before upgrading CloudPlatform itself.

   Run the following commands on every KVM host.

[1] http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-hyperv.vhd.bz2 2

a. Download the CloudPlatform 4.3.0.1 RHEL 6.3 binaries from *https://www.citrix.com/downloads/cloudplatform.html*.

b. Extract the binaries:

```
# cd /root
# tar xvf CloudPlatform-4.3.0.1-1-rhel6.3.tar.gz
```

c. Create a CloudPlatform 4.3 qemu repo:

```
# cd CloudPlatform-4.3.0.1-1-rhel6.3/6.3
# createrepo
```

d. Prepare the yum repo for upgrade. Edit the file /etc/yum.repos.d/rhel63.repo. For example:

```
[upgrade]
name=rhel63
baseurl=url-of-your-rhel6.3-repo
enabled=1
gpgcheck=0
[cloudstack]
name=cloudstack
baseurl=file:///root/CloudPlatform-4.3.0.1-1-rhel6.3/6.3
enabled=1
gpgcheck=0
```

e. Upgrade the host operating system from RHEL 6.0 to 6.3:

```
yum upgrade
```

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

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

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

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

6. 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 CloudPlatform recommended best practice. Substitute your own MySQL root password.

```
# mysqldump -u root -p<mysql_password> cloud >> cloud-backup.dmp
# mysqldump -u root -p<mysql_password> cloud_usage > cloud-usage-backup.dmp
```

7. (RHEL/CentOS 5.x) If you are currently running CloudPlatform on RHEL/CentOS 5.x, use the following command to set up an Extra Packages for Enterprise Linux (EPEL) repo:

```
rpm -Uvh http://mirror.pnl.gov/epel/5/i386/epel-release-5-4.noarch.rpm
```

8. Download CloudPlatform 4.3.0.1 onto the management server host where it will run. Get the software from the following link:

   https://www.citrix.com/English/ss/downloads/.

   You need a *My Citrix Account*[2].

9. Upgrade the CloudPlatform packages. You should have a file in the form of “CloudPlatform-4.3.0-N-OSVERSION.tar.gz”. Untar the file, then run the install.sh script inside it. Replace the file and directory names below with those you are using:

   ```
   # tar xzf CloudPlatform-4.3.0-N-OSVERSION.tar.gz
   # cd CloudPlatform-4.3.0-N-OSVERSION
   # ./install.sh
   ```

   You should see a few messages as the installer prepares, followed by a list of choices.

10. Choose "U" to upgrade the package

    ```
    >U
    ```

    You should see some output as the upgrade proceeds, ending with a message like "Complete! Done."

11. If you have made changes to your existing copy of the configuration files db.properties or server.xml in your previous-version CloudPlatform 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 4.3.

    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 file, and you need to merge the two files:

    ```
    warning: /etc/cloud.rpmsave/management/server.xml created as /etc/cloudstack/management/
    server.xml.rpmnew
    ```

    a. Make a backup copy of your previous version file. For example: (substitute the file name in these commands as needed)

       ```
       # mv /etc/cloudstack/management/server.xml /etc/cloudstack/management/server.xml-
       backup
       ```

    b. Copy the *.rpmnew file to create a new file. For example:

[2] http://www.citrix.com/lang/English/publicindex.asp?destURL=%2FEnglish%2FmyCitrix%2Findex.asp%3F#

```
# cp -ap /etc/cloudstack/management/server.xml.rpmnew /etc/cloudstack/management/
server.xml
```

c. Merge your changes from the backup file into the new file. For example:

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

12. Repeat steps *7* - *11* on each management server node.

13. 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. Restarting the Management Server without any issues indicates that the upgrade is successfully completed.

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

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

15. (VMware only) If you have existing clusters created in CloudPlatform 3.0.6, additional steps are required to update the existing vCenter password 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. Perform the following on each VMware cluster:

i. Encrypt the 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
```

Save the output from this step for later use. You need to add this in the cluster_details and vmware_data_center tables in place of the existing password.

ii. Find the ID of the cluster from the cluster_details table:

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

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

iii. Update the existing password with the encrypted one:

```
update cloud.cluster_details set value = <_ciphertext_from_step_i_> where id =
 <_id_from_step_ii_>;
```

iv. Confirm that the table is updated:

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

v. Find the ID of the VMware data center that you want to work with:

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

vi. Change the existing password to the encrypted one:

```
update cloud.vmware_data_center set password = <_ciphertext_from_step_i_> where
 id = <_id_from_step_v_>;
```

vii. Confirm that the table is updated:

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

c. Start the CloudPlatform Management server

```
service cloudstack-management start
```

16. (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.

Note

After the software upgrade on a KVM machine, the Ctrl+Alt+Del button on the console view of a VM doesn't work. Use Ctrl+Alt+Insert to log in to the console of the VM.

a. Copy the CloudPlatform 4.3.0.1.tgz download to the host, untar it, and change to the resulting directory.

b. Stop the running agent.

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

c. Update the agent software.

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

d. Choose "U" to update the packages.

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
```

17. Log in to the CloudPlatform 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. If the hosts do not come to the Up state, contact support.

18. Perform the following on all the System VMs including Secondary Storage VMs, Console Proxy VMs, and virtual routers.

a. Upgrade Secondary Storage VMs and Console Proxy VMs either from the UI or by using the following script:

```
# cloudstack-sysvmadm -d <IP address> -u cloud -p <password> –s
```

Substitute your own IP address of Secondary Storage VMs and Console Proxy VMs.

b. Selectively upgrade the virtual routers:

i. Log in to the CloudPlatform UI as the root administrator.

ii. In the left navigation, choose Infrastructure.

iii. On Virtual Routers, click View More.

All the VRs are listed in the Virtual Routers page.

iv. In Select View drop-down, select desired grouping based on your requirement:

You can use either of the following:

- Group by zone
- Group by pod
- Group by cluster
- Group by account

v. Click the group which has the virtual routers to be upgraded.

vi. Click the Upgrade button to upgrade all the virtual routers.

For example, if you have selected Group by zone, select the name of the desired zone .

vii. Click OK to confirm.

19. (XenServer only) Upgrade all existing XenServer clusters to XenServer 6.2 SP1 Hotfix XS62ESP1005.

For more information, see *Section 3.6.4, "Upgrading to XenServer 6.2 SP1 Hotfix XS62ESP1005"*.

For instructions for upgrading XenServer software and applying hotfixes, see *Section 3.6.2, "Applying Hotfixes to a XenServer Cluster"*.

20. (VMware only) After upgrade, if you want to change a Standard vSwitch zone to a VMware dvSwitch Zone, perform the following:

a. Ensure that the Public and Guest traffics are not on the same network as the Management and Storage traffic.

b. Set vmware.use.dvswitch to true.

c. Access the physical network for the Public and guest traffic, then change the traffic labels as given below:

```
<dvSwitch name>,<VLANID>,<Switch Type>
```

For example: dvSwitch18,,vmwaredvs

VLANID is optional.

d. Stop the Management server.

e. Start the Management server.

f. Add the new VMware dvSwitch-enabled cluster to this zone.

Post-Upgrade Considerations

Consider the following:

- Manually update **`systemvm.iso`** as given in *Section 3.5, "Updating SystemVM.ISO"*.

  In the previous 4.x releases, the Management Server version stored in the database version table is in x.x.x format. For example, 4.3.0 and 4.3.0.1 are stored as 4.3.0 as only the first 3 digits are considered as release version. Therefore, because the Mangement Server version number is the same for both the releases, the latest systemvm.iso files are not pushed after upgrade. Thererefore, you must manually push systemvm.iso after upgrade.

- Restart the network with setting cleanup to true if DHCP services run concurrently on two VRs.

  Service monitoring is enabled for redundant VR in 4.3, which causes DHCP services to run simultaneously on two VRs. Stopping service monitoring for the existing routers should resolve this issue.

- 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.

- (VMware only) After upgrade, whenever you add a new VMware cluster to a zone that was created with a previous version of CloudPlatform, the fields vCenter host, vCenter Username, vCenter Password, and vCenter Datacenter are required. The Add Cluster dialog in the CloudPlatform user interface incorrectly shows them as optional, and will allow you to proceed with adding the cluster even though these important fields are blank. If you do not provide the values, you will see an error message like "Your host and/or path is wrong. Make sure it's of the format http://hostname/path".

- If you are using LDAP authentication, change the default values based on the LDAP server that you are using:

LDAP Attribute	OpenLDAP	Active Directory
ldap.user.object	inetOrgPerson	user
ldap.username.attribute	uid	sAMAccountName
ldap.group.object	groupOfUniqueNames	group
ldap.group.user.uniquemember	member	uniquemember

3.2. Upgrade from 4.2.x to 4.3.0.1

Perform the following to upgrade from version 4.2.x to version 4.3.0.1.

1. Download the latest System VM templates:

   The System VM templates includes fixes for the OpenSSL HeartBleed vulnerability issues.

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.3 Description: systemvm-xenserver-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/*

Hypervisor	Description
	systemvm64template-2014-06-23-master-xen.vhd.bz2 Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, select each zone and individually register the template to make the template available in all the XenServer zones. (Prior to version 4.3): Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.3 Description: systemvm-kvm-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-kvm.qcow2.bz2* Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running KVM, select each zone and individually register the template to make the template available in all the zones. (Prior to version 4.3): Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the zones. Hypervisor: KVM

Hypervisor	Description
	Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.3 Description: systemvm-vmware-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-vmware.ova* Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running VMware, select each zone and individually register the template to make the template available in all the zones. (Prior to version 4.3): Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the zones. Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
Hyper-V (Applicable only for 4.3)	Name: systemvm-hyperv-4.3 Description: systemvm-hyperv-4.3

Hypervisor	Description
	URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-hyperv.vhd.bz2* [3] Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running Hyper-V, choose All Zones to make the template available in all the XenServer zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

2. By using the prepareTemplate API, download the latest System VM to all the primary storages.
3. (KVM on RHEL 6.0/6.1 only) If your existing CloudPlatform deployment includes one or more clusters of KVM hosts running RHEL 6.0 or RHEL 6.1, you must first upgrade the operating system version on those hosts before upgrading CloudPlatform itself.

   Run the following commands on every KVM host.

   a. Download the CloudPlatform 4.3.0.1 RHEL 6.3 binaries from *https://www.citrix.com/downloads/cloudplatform.html*.

   b. Extract the binaries:

   ```
   # cd /root
   # tar xvf CloudPlatform-4.3.0.1-1-rhel6.3.tar.gz
   ```

   c. Create a CloudPlatform 4.3 qemu repo:

   ```
   # cd CloudPlatform-4.3.0.1-1-rhel6.3/6.3
   # createrepo
   ```

   d. Prepare the yum repo for upgrade. Edit the file /etc/yum.repos.d/rhel63.repo. For example:

[3] http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-hyperv.vhd.bz2 2

```
[upgrade]
name=rhel63
baseurl=url-of-your-rhel6.3-repo
enabled=1
gpgcheck=0
[cloudstack]
name=cloudstack
baseurl=file:///root/CloudPlatform-4.3.0.1-1-rhel6.3/6.3
enabled=1
gpgcheck=0
```

e. Upgrade the host operating system from RHEL 6.0 to 6.3:

```
yum upgrade
```

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

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

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

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

6. 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 CloudPlatform recommended best practice. Substitute your own MySQL root password.

```
# mysqldump -u root -p<mysql_password> cloud >> cloud-backup.dmp
# mysqldump -u root -p<mysql_password> cloud_usage > cloud-usage-backup.dmp
```

7. (RHEL/CentOS 5.x) If you are currently running CloudPlatform on RHEL/CentOS 5.x, use the following command to set up an Extra Packages for Enterprise Linux (EPEL) repo:

```
rpm -Uvh http://mirror.pnl.gov/epel/5/i386/epel-release-5-4.noarch.rpm
```

8. Download CloudPlatform 4.3.0.1 onto the management server host where it will run. Get the software from the following link:

   https://www.citrix.com/English/ss/downloads/.

   You need a *My Citrix Account*[4].

9. Upgrade the CloudPlatform packages. You should have a file in the form of “CloudPlatform-4.3.0-N-OSVERSION.tar.gz”. Untar the file, then run the install.sh script inside it. Replace the file and directory names below with those you are using:

```
# tar xzf CloudPlatform-4.3.0-N-OSVERSION.tar.gz
# cd CloudPlatform-4.3.0-N-OSVERSION
```

[4] http://www.citrix.com/lang/English/publicindex.asp?destURL=%2FEnglish%2FmyCitrix%2Findex.asp%3F#

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

You should see a few messages as the installer prepares, followed by a list of choices.

10. Choose "U" to upgrade the package

```
>U
```

You should see some output as the upgrade proceeds, ending with a message like "Complete! Done."

11. If you have made changes to your existing copy of the configuration files db.properties or server.xml in your previous-version CloudPlatform 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 4.3.

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 file, and you need to merge the two files:

```
warning: /etc/cloud.rpmsave/management/server.xml created as /etc/cloudstack/management/
server.xml.rpmnew
```

a. Make a backup copy of your previous version file. For example: (substitute the file name in these commands as needed)

```
# mv /etc/cloudstack/management/server.xml /etc/cloudstack/management/server.xml-
backup
```

b. Copy the *.rpmnew file to create a new file. For example:

```
# cp -ap /etc/cloudstack/management/server.xml.rpmnew /etc/cloudstack/management/
server.xml
```

c. Merge your changes from the backup file into the new file. For example:

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

12. Repeat steps *7* - *11* on each management server node.

13. 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. Restarting the Management Server without any issues indicates that the upgrade is successfully completed.

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

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

15. (VMware only) If you have existing clusters created in CloudPlatform 3.0.6, additional steps are required to update the existing vCenter password 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. Perform the following on each VMware cluster:

        i. Encrypt the 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
        ```

        Save the output from this step for later use. You need to add this in the cluster_details and vmware_data_center tables in place of the existing password.

        ii. Find the ID of the cluster from the cluster_details table:

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

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

        iii. Update the existing password with the encrypted one:

        ```
        update cloud.cluster_details set value = <_ciphertext_from_step_i_> where id =
         <_id_from_step_ii_>;
        ```

        iv. Confirm that the table is updated:

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

v. Find the ID of the VMware data center that you want to work with:

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

vi. Change the existing password to the encrypted one:

```
update cloud.vmware_data_center set password = <_ciphertext_from_step_i_> where
 id = <_id_from_step_v_>;
```

vii. Confirm that the table is updated:

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

c. Start the CloudPlatform Management server

```
service cloudstack-management start
```

16. (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.

Note

After the software upgrade on a KVM machine, the Ctrl+Alt+Del button on the console view of a VM doesn't work. Use Ctrl+Alt+Insert to log in to the console of the VM.

a. Copy the CloudPlatform 4.3.0.1.tgz download to the host, untar it, and change to the resulting directory.

b. Stop the running agent.

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

c. Update the agent software.

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

d. Choose "U" to update the packages.

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
```

17. Log in to the CloudPlatform 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. If the hosts do not come to the Up state, contact support.

18. Perform the following on all the System VMs including Secondary Storage VMs, Console Proxy VMs, and virtual routers.

a. Upgrade Secondary Storage VMs and Console Proxy VMs either from the UI or by using the following script:

```
# cloudstack-sysvmadm -d <IP address> -u cloud -p <password> –s
```

Substitute your own IP address of Secondary Storage VMs and Console Proxy VMs.

b. Selectively upgrade the virtual routers:

i. Log in to the CloudPlatform UI as the root administrator.

ii. In the left navigation, choose Infrastructure.

iii. On Virtual Routers, click View More.

All the VRs are listed in the Virtual Routers page.

iv. In Select View drop-down, select desired grouping based on your requirement:

You can use either of the following:

- Group by zone
- Group by pod
- Group by cluster

- Group by account

v. Click the group which has the virtual routers to be upgraded.

vi. Click the Upgrade button to upgrade all the virtual routers.

For example, if you have selected Group by zone, select the name of the desired zone .

vii. Click OK to confirm.

19. (XenServer only) Upgrade all existing XenServer clusters to XenServer 6.2 SP1 Hotfix XS62ESP1005.

For more information, see *Section 3.6.4, "Upgrading to XenServer 6.2 SP1 Hotfix XS62ESP1005"*.

For instructions for upgrading XenServer software and applying hotfixes, see *Section 3.6.2, "Applying Hotfixes to a XenServer Cluster"*.

20. (VMware only) After upgrade, if you want to change a Standard vSwitch zone to a VMware dvSwitch Zone, perform the following:

a. Ensure that the Public and Guest traffics are not on the same network as the Management and Storage traffic.

b. Set vmware.use.dvswitch to true.

c. Access the physical network for the Public and guest traffic, then change the traffic labels as given below:

```
<dvSwitch name>,<VLANID>,<Switch Type>
```

For example: dvSwitch18,,vmwaredvs

VLANID is optional.

d. Stop the Management server.

e. Start the Management server.

f. Add the new VMware dvSwitch-enabled cluster to this zone.

Post-Upgrade Considerations

Consider the following:

- Update **`systemvm.iso`** as given in *Section 3.5, "Updating SystemVM.ISO"*.

  In the previous 4.x releases, the Management Server version stored in the database version table is in x.x.x format. For example, 4.3.0 and 4.3.0.1 are stored as 4.3.0 as only the first 3 digits are considered as release version. Therefore, because the Mangement Server version number is the same for both the releases, the latest systemvm.iso files are not pushed after upgrade. Thererefore, manually push systemvm.iso after upgrade.

- 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.

- (VMware only) After upgrade, whenever you add a new VMware cluster to a zone that was created with a previous version of CloudPlatform, the fields vCenter host, vCenter Username, vCenter Password, and vCenter Datacenter are required. The Add Cluster dialog in the CloudPlatform user interface incorrectly shows them as optional, and will allow you to proceed with adding the cluster even though these important fields are blank. If you do not provide the values, you will see an error message like "Your host and/or path is wrong. Make sure it's of the format http://hostname/path".
- If you are using LDAP authentication, change the default values based on the LDAP server that you are using:

LDAP Attribute	OpenLDAP	Active Directory
ldap.user.object	inetOrgPerson	user
ldap.username.attribute	uid	sAMAccountName
ldap.group.object	groupOfUniqueNames	group
ldap.group.user.uniquemember	member	uniquemember

3.3. Upgrade from 3.0.x to 4.3.0.1

Perform the following to upgrade from version 3.0.0, 3.0.1, 3.0.2, 3.0.3, 3.0.4, 3.0.5, 3.0.6, or 3.0.7 to version 4.3.0.1.

1. If you are upgrading from 3.0.0 or 3.0.1, ensure that you query your IP address 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, any existing IP address usage records in the old format will no longer be available.

2. While running the 3.0.x system, log in to the UI as root administrator.

3. 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.

   

   Note

   You might notice that the size of the system VM template has increased compared to previous CloudPlatform versions. This is because the new version of the underlying Debian template has an increased disk size.

   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):

The System VM templates includes fixes for the OpenSSL HeartBleed vulnerability issues.

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.3 Description: systemvm-xenserver-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-xen.vhd.bz2* Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, select each zone and individually register the template to make the template available in all the XenServer zones. (Prior to version 4.3): Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.3 Description: systemvm-kvm-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-kvm.qcow2.bz2* Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running KVM, select each zone and

Hypervisor	Description
	individually register the template to make the template available in all the zones. (Prior to version 4.3): Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the zones. Hypervisor: KVM Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.3 Description: systemvm-vmware-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-vmware.ova* Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running VMware, select each zone and individually register the template to make the template available in all the zones. (Prior to version 4.3): Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the zones. Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown)

Hypervisor	Description
	Extractable: no Password Enabled: no Public: no Featured: no
Hyper-V (Applicable only for 4.3)	Name: systemvm-hyperv-4.3 Description: systemvm-hyperv-4.3 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-hyperv.vhd.bz2* [5] Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running Hyper-V, choose All Zones to make the template available in all the XenServer zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

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

f. If you use more than one type of hypervisor in your cloud, repeat these steps to download the system VM template for each hypervisor type.

[5] http://download.cloud.com/templates/4.3/systemvm64template-2014-06-23-master-hyperv.vhd.bz2 2

Warning

If you do not repeat the steps for each hypervisor type, the upgrade will fail.

4. By using the prepareTemplate API, download the latest System VM to all the primary storages.

5. (KVM on RHEL 6.0/6.1 only) If your existing CloudPlatform deployment includes one or more clusters of KVM hosts running RHEL 6.0 or RHEL 6.1, you must first upgrade the operating system version on those hosts before upgrading CloudPlatform itself.

   Run the following commands on every KVM host.

   a. Download the CloudPlatform 4.3.0.1 RHEL 6.3 binaries from *https://www.citrix.com/downloads/cloudplatform.html*.

   b. Extract the binaries:

   ```
   # cd /root
   # tar xvf CloudPlatform-4.3.0.1-1-rhel6.3.tar.gz
   ```

   c. Create a CloudPlatform 4.3.0.1 qemu repo:

   ```
   # cd CloudPlatform-4.3.0.1-1-rhel6.3/6.3
   # createrepo
   ```

   d. Prepare the yum repo for upgrade. Edit the file /etc/yum.repos.d/rhel63.repo. For example:

   ```
   [upgrade]
   name=rhel63
   baseurl=url-of-your-rhel6.3-repo
   enabled=1
   gpgcheck=0
   [cloudstack]
   name=cloudstack
   baseurl=file:///root/CloudPlatform-4.3.0.1-1-rhel6.3/6.3
   enabled=1
   gpgcheck=0
   ```

   e. Upgrade the host operating system from RHEL 6.0 to 6.3:

   ```
   yum upgrade
   ```

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

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

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

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

8. 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 CloudPlatform recommended best practice. Substitute your own MySQL root password.

   ```
   # mysqldump -u root -p<mysql_password> cloud >> cloud-backup.dmp
   # mysqldump -u root -p<mysql_password> cloud_usage > cloud-usage-backup.dmp
   ```

9. (RHEL/CentOS 5.x) If you are currently running CloudPlatform on RHEL/CentOS 5.x, use the following command to set up an Extra Packages for Enterprise Linux (EPEL) repo:

   ```
   rpm -Uvh http://mirror.pnl.gov/epel/5/i386/epel-release-5-4.noarch.rpm
   ```

10. Download CloudPlatform 4.3.0.1 onto the management server host where it will run. Get the software from the following link:

    https://www.citrix.com/English/ss/downloads/.

    You need a *My Citrix Account*[6].

11. Upgrade the CloudPlatform packages. You should have a file in the form of “CloudPlatform-4.3.0-N-OSVERSION.tar.gz”. Untar the file, then run the install.sh script inside it. Replace the file and directory names below with those you are using:

    ```
    # tar xzf CloudPlatform-4.3.0-N-OSVERSION.tar.gz
    # cd CloudPlatform-4.3.0-N-OSVERSION
    # ./install.sh
    ```

    You should see a few messages as the installer prepares, followed by a list of choices.

12. Choose "U" to upgrade the package

    ```
    >U
    ```

    You should see some output as the upgrade proceeds, ending with a message like "Complete! Done."

13. If you have made changes to your existing copy of the configuration files components.xml, db.properties, or server.xml in your previous-version CloudPlatform 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 4.3.0.1

[6] http://www.citrix.com/lang/English/publicindex.asp?destURL=%2FEnglish%2FmyCitrix%2Findex.asp%3F#

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 file, and you need to merge the two files:

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

a. Make a backup copy of your previous version file. For example: (substitute the file name components.xml, db.properties, or server.xml in these commands as needed)

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

b. Copy the *.rpmnew file to create a new file. For example:

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

c. Merge your changes from the backup file into the new file. For example:

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

14. Repeat steps *9* - *13* on each management server node.

15. 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. Restarting the Management Server without any issues indicates that the upgrade is successfully completed.

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

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

Note

After upgrade from 3.0.4 to 4.3.0.1, if the usage server fails to restart then copy db.properties from /etc/cloudstack/management to /etc/cloudstack/usage. Then start the Usage Server.

17. (VMware only) If you are upgrading from 3.0.6 or beyond and you have existing clusters created in 3.0.6, additional steps are required to update the existing vCenter password 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. Perform the following on each VMware cluster:

        i. Encrypt the 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
        ```

        Save the output from this step for later use. You need to add this in the cluster_details and vmware_data_center tables in place of the existing password.

        ii. Find the ID of the cluster from the cluster_details table:

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

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

        iii. Update the existing password with the encrypted one:

        ```
        update cloud.cluster_details set value = <_ciphertext_from_step_i_> where id =
         <_id_from_step_ii_>;
        ```

        iv. Confirm that the table is updated:

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

        v. Find the ID of the VMware data center that you want to work with:

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

vi. Change the existing password to the encrypted one:

```
update cloud.vmware_data_center set password = <_ciphertext_from_step_i_> where
 id = <_id_from_step_v_>;
```

vii. Confirm that the table is updated:

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

c. Start the CloudPlatform Management server

```
service cloudstack-management start
```

18. (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.

Note

After the software upgrade on a KVM machine, the Ctrl+Alt+Del button on the console view of a VM doesn't work. Use Ctrl+Alt+Insert to log in to the console of the VM.

a. Copy the CloudPlatform 4.3.0.1.tgz download to the host, untar it, and cd into the resulting directory.

b. Stop the running agent.

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

c. Update the agent software.

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

d. Choose "U" to update the packages.

e. 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`**.

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

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

g. 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
```

h. Restart libvirtd.

```
# service libvirtd restart
```

i. Start the agent.

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

19. Log in to the CloudPlatform 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. If the hosts do not come to the Up state, contact support.

20. If you are upgrading from 3.0.1 or 3.0.2, 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 cloudstack-sysvmadm script later in the upgrade procedure. For information about how to set this parameter, see “Setting 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.

21. Perform the following on all the System VMs including Secondary Storage VMs, Console Proxy VMs, and virtual routers.

a. Upgrade Secondary Storage VMs and Console Proxy VMs either from the UI or by using the following script:

```
# cloudstack-sysvmadm -d <IP address> -u cloud -p <password> –s
```

Substitute your own IP address of Secondary Storage VMs and Console Proxy VMs.

b. Selectively upgrade the virtual routers:

i. Log in to the CloudPlatform UI as the root administrator.

ii. In the left navigation, choose Infrastructure.

iii. On Virtual Routers, click View More.

All the VRs are listed in the Virtual Routers page.

iv. In Select View drop-down, select desired grouping based on your requirement:

You can use either of the following:

- Group by zone
- Group by pod
- Group by cluster
- Group by account

v. Click the group which has the virtual routers to be upgraded.

vi. Click the Upgrade button to upgrade all the virtual routers.

For example, if you have selected Group by zone, select the name of the desired zone .

vii. Click OK to confirm.

22. 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 /root/.ssh/id_rsa.cloud <link-local-ip> -p 3922
# cat /etc/cloudstack-release
```

The output should be like the following:

```
Cloudstack Release 4.3.0.1 Mon June 14 15:10:04 PST 2013
```

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 /var/cloudstack/management/.ssh/id_rsa <private-ip> -p 3922
# cat /etc/cloudstack-release
```

The output should be like the following:

```
Cloudstack Release 4.3.0.1 Fri June 8 15:10:04 PST 2014
```

23. If you want to close the admin port again (recommended in production systems), set integration.api.port to null. Then restart the Management Server.

    For information about how to set integration.api.port, see “Setting Configuration Parameters” in the Installation Guide.

24. (XenServer only) Upgrade all existing XenServer clusters to XenServer 6.2 SP1 Hotfix XS62ESP1005.

    For more information, see *Section 3.6.4, “Upgrading to XenServer 6.2 SP1 Hotfix XS62ESP1005”*.

    For instructions for upgrading XenServer software and applying hotfixes, see *Section 3.6.2, “Applying Hotfixes to a XenServer Cluster”*.

25. (VMware only) After upgrade, if you want to change a Standard vSwitch zone to a VMware dvSwitch Zone, perform the following:

    a. Ensure that the Public and Guest traffics are not on the same network as the Management and Storage traffic.

    b. Set vmware.use.dvswitch to true.

    c. Access the physical network for the Public and guest traffic, then change the traffic labels as given below:

       ```
       <dvSwitch name>,<VLANID>,<Switch Type>
       ```

       For example: dvSwitch18,,vmwaredvs

       VLANID is optional.

    d. Stop the Management server.

    e. Start the Management server.

    f. Add the new VMware dvSwitch-enabled cluster to this zone.

Post-Upgrade Considerations

Consider the following:

- 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.
- (VMware only) After upgrade, whenever you add a new VMware cluster to a zone that was created with a previous version of CloudPlatform, the fields vCenter host, vCenter Username, vCenter Password, and vCenter Datacenter are required. The Add Cluster dialog in the CloudPlatform user

interface incorrectly shows them as optional, and will allow you to proceed with adding the cluster even though these important fields are blank. If you do not provide the values, you will see an error message like "Your host and/or path is wrong. Make sure it's of the format http://hostname/path".

- If you are using LDAP authentication, change the default values based on the LDAP server that you are using:

LDAP Attribute	OpenLDAP	Active Directory
ldap.user.object	inetOrgPerson	user
ldap.username.attribute	uid	sAMAccountName
ldap.group.object	groupOfUniqueNames	group
ldap.group.user.uniquemember	member	uniquemember

3.4. Upgrade CloudPlatform Baremetal Agent on PXE and DHCP Servers

If you installed bare metal clusters using a previous version of CloudPlatform, use the following steps to upgrade the baremetal agent in order to get the latest bug fixes for 4.3.0.

1. Log in as root to the host or virtual machine running the Baremetal PXE server and DHCP server.
2. Download CloudPlatform 4.3.0.1 onto the PXE or DHCP server. Get the software from the following link:

   https://www.citrix.com/English/ss/downloads/.

   You need a *My Citrix Account*[7].
3. Upgrade the CloudPlatform packages. You should have a file in the form of “CloudPlatform-4.3.0-N-OSVERSION.tar.gz”. Untar the file, then run the install.sh script inside it. Replace the file and directory names below with those you are using:

   ```
   # tar xzf CloudPlatform-4.3.0-N-OSVERSION.tar.gz
   # cd CloudPlatform-4.3.0-N-OSVERSION
   # ./install.sh
   ```

   You should see a few messages as the installer prepares, followed by a list of choices.
4. Choose "U" to upgrade the package

   ```
   >U
   ```

   You should see some output as the upgrade proceeds, ending with a message like "Complete! Done."
5. Run the bare metal setup script:

   ```
   cloudstack-setup-baremetal
   ```

[7] http://www.citrix.com/lang/English/publicindex.asp?destURL=%2FEnglish%2FmyCitrix%2Findex.asp%3F#

3.5. Updating SystemVM.ISO

- On CloudPlatform versions 3.0.5.x and 3.0.7.x **systemvm.iso** will get propagated automatically; therefore, no separate procedure is required.
- On CloudPlatform versions 4.2.1.x and 4.3.x, perform the following based on the hypervisor that you use:
  - XenServer: No action is required.
  - KVM
    a. On the KVM host, stop the CloudPlatform agent.
    b. Upgrade the CloudPlatform agent.
    c. Restart the CloudPlatform agent.
    d. Stop and Start SystemVMs.
  - HyperV (for CloudPlatform versions 4.3 and above)
    a. Stop all the Management Servers.
    b. Remove **systemvm-4.3.x.x.iso** from the **systemvm** directory in the Secondary Storage directory, **\\<secondary_storage_path>\systemvm**.
    c. Remove **systemvm-4.3.x.x.iso** from each Hyper-V host.

       The location of the file is **C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks**.
    d. Start the Management Server.
    e. Destroy SystemVMs.

       New SystemVMs will be spawned and the new iso, **systemvm-4.3.x.x.iso**, is copied to the secondary storage and Hypervisor host.
  - VMware
    a. Stop all the Management Servers.
    b. Remove the old **systemvm<version>.iso** file from the **systemvm** directory, **\ \<secondary_storage_path>\systemvm**.

       Where <version> denotes the Management Server version number.
    c. Start the Management Server.

       Verify if the new **systemvm.iso** is pushed to the **systemvm** folder in the Secondary Storage directory.
    d. Stop and Start SystemVMs.

3.6. Upgrading and Hotfixing XenServer Hypervisor Hosts

In CloudPlatform 4.3.0, you can upgrade XenServer hypervisor host software without having to disconnect the XenServer cluster. You can upgrade XenServer 5.6 GA, 5.6 FP1, or 5.6 SP2 to any

newer version that is supported by CloudPlatform. The actual upgrade is described in XenServer documentation, but there are some additional steps you must perform before and after the upgrade.

3.6.1. Upgrading to a New XenServer Version

To upgrade XenServer hosts when running CloudPlatform 4.3.0.1:

1. Edit the file /etc/cloudstack/management/environment.properties and add the following line:

   ```
   manage.xenserver.pool.master=false
   ```

2. Restart the Management Server to put the new setting into effect.

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

3. Find the hostname of the master host in your XenServer cluster (pool):

   a. Run the following command on any host in the pool, and make a note of the host-uuid of the master host:

      ```
      # xe pool-list
      ```

   b. Now run the following command, and find the host that has a host-uuid that matches the master host from the previous step. Make a note of this host's hostname. You will need to input it in a later step.

      ```
      # xe host-list
      ```

4. On CloudPlatform, put the master host into maintenance mode. Use the hostname you discovered in the previous step.

   

   Note

   In the latest XenServer upgrade procedure, even after putting the master host into maintenance mode, the master host continues to stay as master.

   Any VMs running on this master will be automatically migrated to other hosts, unless there is only one UP host in the cluster. If there is only one UP host, putting the host into maintenance mode will stop any VMs running on the host.

5. Disconnect the XenServer cluster from CloudPlatform. It will remain disconnected only long enough to upgrade one host.

   a. Log in to the CloudPlatform UI as root.

   b. Navigate to the XenServer cluster, and click Actions – Unmanage.

   c. Watch the cluster status until it shows Unmanaged.

6. Upgrade the XenServer software on the master host:

a. Insert the XenXerver CD.

b. Reboot the host.

c. Upgrade to the newer version of XenServer. Use the steps in XenServer documentation.

7. Cancel the maintenance mode on the master host.
8. Reconnect the XenServer cluster to CloudPlatform.

a. Log in to the CloudPlatform UI as root.

b. Navigate to the XenServer cluster, and click Actions – Manage.

c. Watch the status to see that all the hosts come up.

9. Upgrade the slave hosts in the cluster:

a. Put a slave host into maintenance mode.

Wait until all the VMs are migrated to other hosts.

b. Upgrade the XenServer software on the slave.

c. Cancel maintenance mode for the slave.

d. Repeat steps *a* through *c* for each slave host in the XenServer pool.

10. You might need to change the OS type settings for VMs running on the upgraded hosts, if any of the following apply:

- If you upgraded from XenServer 5.6 GA to XenServer 5.6 SP2, change any VMs that have the OS type CentOS 5.5 (32-bit), Oracle Enterprise Linux 5.5 (32-bit), or Red Hat Enterprise Linux 5.5 (32-bit) to Other Linux (32-bit). Change any VMs that have the 64-bit versions of these same OS types to Other Linux (64-bit).
- If you upgraded from XenServer 5.6 SP2 to XenServer 6.0.2 or higher, change any VMs that have the OS type CentOS 5.6 (32-bit), CentOS 5.7 (32-bit), Oracle Enterprise Linux 5.6 (32-bit), Oracle Enterprise Linux 5.7 (32-bit), Red Hat Enterprise Linux 5.6 (32-bit) , or Red Hat Enterprise Linux 5.7 (32-bit) to Other Linux (32-bit). Change any VMs that have the 64-bit versions of these same OS types to Other Linux (64-bit).
- If you upgraded from XenServer 5.6 to XenServer 6.0.2 or higher, do all of the above.

3.6.2. Applying Hotfixes to a XenServer Cluster

1. Edit the file /etc/cloudstack/management/environment.properties and add the following line:

```
manage.xenserver.pool.master=false
```

2. Restart the Management Server to put the new setting into effect.

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

3. Find the hostname of the master host in your XenServer cluster (pool):

a. Run the following command on any host in the pool, and make a note of the host-uuid of the master host:

```
# xe pool-list
```

b. Now run the following command, and find the host that has a host-uuid that matches the master host from the previous step. Make a note of this host's hostname. You will need to input it in a later step.

```
# xe host-list
```

4. On CloudPlatform, put the master host into maintenance mode. Use the hostname you discovered in the previous step.

   Any VMs running on this master will be automatically migrated to other hosts, unless there is only one UP host in the cluster. If there is only one UP host, putting the host into maintenance mode will stop any VMs running on the host.

5. Disconnect the XenServer cluster from CloudPlatform. It will remain disconnected only long enough to hotfix one host.

   a. Log in to the CloudPlatform UI as root.

   b. Navigate to the XenServer cluster, and click Actions – Unmanage.

   c. Watch the cluster status until it shows Unmanaged.

6. Hotfix the master host:

   a. Add the XenServer hot fixes to the master host.

      i. Assign a UUID to the update file:

      ```
      xe patch-upload file-name=XS602E015.xsupdate
      ```

      The command displays the UUID of the update file:

      ```
      33af688e-d18c-493d-922b-ec51ea23cfe9
      ```

      ii. Repeat the xe patch-upload command for all other XenServer updates: XS62ESP1005.xsupdate, XS62ESP1003.xsupdate.

      Take a note of the UUIDs of the update files. The UUIDs are required in the next step.

   b. Apply XenServer hot fixes to master host:

   ```
   xe patch-apply host-uuid=<master uuid> uuid=<hotfix uuid>
   ```

   c. Repeat xe patch-apply command for all the hot fixes.

   d. Install the required CSP files.

   ```
   xe-install-supplemental-pack <csp-iso-file>
   ```

e. Restart the master host.

7. Cancel the maintenance mode on the master host.
8. Reconnect the XenServer cluster to CloudPlatform.
   a. Log in to the CloudPlatform UI as root.
   b. Navigate to the XenServer cluster, and click Actions – Manage.
   c. Watch the status to see that all the hosts come up.
9. Hotfix the slave hosts in the cluster:
   a. Put a slave host into maintenance mode.

      Wait until all the VMs are migrated to other hosts.

   b. Apply the XenServer hot fixes to the slave host:

      ```
      xe patch-apply host-uuid=<slave uuid> uuid=<hotfix uuid>
      ```

   c. Repeat Step a through b for each slave host in the XenServer pool.
   d. Install the required CSP files.

      ```
      xe-install-supplemental-pack <csp-iso-file>
      ```

   e. Restart the slave hosts.

      Wait until all the slave hosts are up. It might take several minutes for the hosts to come up.
10. Cancel the maintenance mode on the slave hosts.
11. You might need to change the OS type settings for VMs running on the upgraded hosts, if any of the following apply:
    - If you upgraded from XenServer 5.6 SP2 to XenServer 6.0.2, change any VMs that have the OS type CentOS 5.6 (32-bit), CentOS 5.7 (32-bit), Oracle Enterprise Linux 5.6 (32-bit), Oracle Enterprise Linux 5.7 (32-bit), Red Hat Enterprise Linux 5.6 (32-bit) , or Red Hat Enterprise Linux 5.7 (32-bit) to Other Linux (32-bit). Change any VMs that have the 64-bit versions of these same OS types to Other Linux (64-bit).
    - If you upgraded from XenServer 5.6 GA or 5.6 FP1 to XenServer 6.0.2, change any VMs that have the OS type CentOS 5.5 (32-bit), CentOS 5.6 (32-bit), CentOS 5.7 (32-bit), Oracle Enterprise Linux 5.5 (32-bit), Oracle Enterprise Linux 5.6 (32-bit), Oracle Enterprise Linux 5.7 (32-bit), Red Hat Enterprise Linux 5.5 (32-bit), Red Hat Enterprise Linux 5.6 (32-bit) , or Red Hat Enterprise Linux 5.7 (32-bit) to Other Linux (32-bit). Change any VMs that have the 64-bit versions of these same OS types to Other Linux (64-bit).

3.6.3. Install CloudPlatform XenServer Support Package (CSP)

Ensure that you install CloudPlatform XenServer Support Package (CSP) to enable security groups, elastic load balancing, and elastic IP on XenServer.

For more information, see the Install CloudPlatform XenServer Support Package (CSP) in the Installation Guide.

If your hosts on versions prior to 6.2 operated on bridge mode with CSP packages installed, after upgrade, run only the following to restore the desired Security Groups configuration:

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

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

2. Restart the host machine when prompted.
3. If you are using XenServer 6.1 or greater, perform the following:
   a. Run the following commands:

```
echo 1 > /proc/sys/net/bridge/bridge-nf-call-iptables
echo 1 > /proc/sys/net/bridge/bridge-nf-call-arptables
```

   b. To persist the above changes across reboots, set the following values in the /etc/sysctl.conf file. Run the following command:

```
sysctl -p /etc/sysctl.conf
```

   Set these to 1:

```
net.bridge.bridge-nf-call-iptables = 1
net.bridge.bridge-nf-call-arptables = 1
```

3.6.4. Upgrading to XenServer 6.2 SP1 Hotfix XS62ESP1005

It is highly recommended that all XenServer clusters are upgraded to XenServer 6.2 SP1 Hotfix XS62ESP1005. You can upgrade from any prior version of XenServer to the latest version, which might include multiple hops as part of a single upgrade process. For example, if you are upgrading from 6.0.2, upgrade the master host by using the upgrade path given below, followed by each slave host upgrading to XenServer 6.2 SP1 Hotfix XS62ESP1005 by using this same upgrade path:

1. XenServer 6.0.2 to XenServer 6.2
2. XenServer 6.2 to XenServer 6.2 SP1
3. XenServer 6.2 SP1 to XenServer 6.2 SP1 Hotfix XS62ESP1005

After upgrading, ensure that XenServer Pool HA is enabled.

For information on enabling Pool HA for HA support, see Enabling Pool HA section in the Citrix CloudPlatform Installation Guide.

What's New in 4.3.0.1

CloudPlatform 4.3.0.1 is a maintenance release that mainly focusses on the issues around replacing the domain, realhostip.com, with custom defined domain name. This release includes no new features or API changes.

4.1. Replacing Realhostip with Custom Domain

Prior to CloudPlatform version 4.3, the console viewing functionality for SystemVMs used a dynamic DNS service under the domain name realhostip.com. This domain name assists in providing SSL security to console sessions. The domain, realhostip.com, has been depreciated. CloudPlatform deployments prior to version 4.3 that have not been reconfigured to use a DNS domain other than realhostip.com for Console Proxy or Secondary Storage must make changes to for the SystemVMs to continue functioning. To use one SSL certificate across all the instances among different deployments, CloudPlatform provides a global parameter based mechanism. To achieve that you need the following:

- A software that runs a wildcard DNS service.
- A wildcard certificate for this domain name.
  - Public certificate of root CA in PEM format
  - Public certificate(s) of intermediate CA(s) (if any) in PEM format
  - Wildcard domain certificate in PEM format
  - Private key in PKCS8 format

Note

Self-signed certificates are not supported.

- A domain, which can run a DNS service that is capable of resolving queries for addresses of the form aaa-bbb-ccc-ddd.yourdomain.com to an IPv4 IP address in the form aaa.bbb.ccc.ddd, for example, 202.8.44.1.

4.1.1. Prerequisites and Considerations

- When you switch the communication mode from HTTPS to HTTP or vice-versa, stop all the running Console Proxy VMs. Doing so ensures that the Console Proxy VMs are listening on the right port.
- Specify the same domain name in the following:
  - SSL certificates you upload
  - *`consoleproxy.url.domain`*
  - *`secstorage.ssl.cert.domain`*

4.1.2. Procedure

1. Backup existing **`systemvm.iso`**:

Copy **systemvm.iso** available at **/usr/share/cloudstack-common/vms** to a temporary location)

2. Upgrade to the latest CloudPlatform version by following the instructions given in the Upgrade section.

3. Once the Management Server and SystemVM agents are upgraded successfully, follow the instructions given in *Section 4.1.3, "Console Proxy"* and *Section 4.1.5, "Secondary Storage VM"*.

4. Restart the Management Server.

5. Update **systemvm.iso**.

   See *Section 3.5, "Updating SystemVM.ISO"*.

6. Upload Custom Certificates to replace realhostip.com with your own domain name.

   See *Section 4.1.6.2, "Uploading Custom Certificates"*.

4.1.3. Console Proxy

For Console Proxy sessions, you can use one of the following modes: HTTP, HTTPS with wildcard certificate, and HTTPS with a certificate signed under an exact domain name. For each mode, you need to set the global parameter, *consoleproxy.url.domain*to different forms of IP address, which can later be resolved by your DNS server.

1. Ensure that you set up a domain in your DNS server.

   In this example, assume that your DNS server is BIND, and the domain name is yourdomain.com.

2. Set up your zone in your DNS server.

   If you are using BIND 9:

```
zone "yourhostip.com" IN {
      type master;
      file "yourhostip.com.zone";
      allow-update { none; };
};
```

3. Populate an A record for every public IP you have entered in CloudPlatform that the console proxy could allocate.

   For example, a range such as 55.66.77.100 to 55.66.77.200.

```
55-66-77-100      IN      A      55.66.77.100
55-66-77-101      IN      A      55.66.77.101
55-66-77-102      IN      A      55.66.77.102
55-66-77-103      IN      A      55.66.77.103

etc..

55-66-77-200      IN      A      55.66.77.200
```

4. Update CloudPlatform with the new domain name:

   a. Log in to the CloudPlatform UI as an administrator.

b. In the left navigation pane, select Global Settings.

c. Select the *consoleproxy.url.domain* parameter.

d. Depending on your requirement, perform one of the following:

Console Proxy Mode	Global Parameter Settings	Console Proxy URL
HTTP	Set *consoleproxy.url.domain* to empty.	http://aaa.bbb.ccc.ddd/xxxxx Where xxxxx is the token.
HTTPS with wildcard certificate	Set *consoleproxy.url.domain* to *.yourdomain.com	http://aaa.bbb.ccc.ddd.yourdomain.com/xxxxx Each public IP entered in CloudPlatform is converted to a DNS name, for example, 77.88.99.11 and maps to 77-88-99-11.yourdomain.com/xxxxx, where xxxxx is the secure token. When the browser connects to this URL, it try to match to wildcard cert *.yourdomain.com. For more information on generating wildcard certificates, see the CloudPlatform Administrator Guide.
HTTPS with a certificate signed under an exact domain name	Set *consoleproxy.url.domain* to xyz.yourdomain.com.	https://xyz.yourdomain.com/xxxxx For more information, see *Section 4.1.4, "Load Balancing Console Proxy VMs"*.

5. Restart the Management Server.

4.1.4. Load Balancing Console Proxy VMs

1. On an external LB device, such as Citrix Netscaler, configure an LB rule.
2. Map the LB rule to one of the public IPs from the public IP pool of Console Proxy.
3. In CloudPlatform, set the *consoleproxy.url.domain* parameter to *xyz.yourdomain.com* to perform LB on Console Proxy VMS.
4. Configure DNS server to resolve the specific domain name, xyz.yourdomain.com, to the LB public IP you have configured.
5. Restart the Management Server for the new settings to take effect.

CloudPlatform sends a request as given below :

```
# wget https://xyz.yourdomain.com/ajax?token=token
```

When you open a Console Proxy VM, CloudPlatform sends the request to xyz.yourdomain.com, which is internally mapped to the public IP of the LB rule on the DNS server. DNS server forwards this request to the LB Public IP. When the external LB device receives, request is internally load balanced and forwarded to associated Console Proxy VMs.

4.1.5. Secondary Storage VM

Use the *secstorage.encrypt.copy* parameter to turn on the secure connection. To customize domain for SSVM, set the *secstorage.ssl.cert.domain* parameter to *.yourdomain.com. The certificate can be changed by using the Upload SSL certificate functionality in the CloudPlatform UI under Infrastructure tab, or by using the API calls.

Note

Provide the full certificate path for the System VMs if you are using a certificate from an intermediate CA. The certificate path begins with the certificate of that certifying entity, and each certificate in the chain is signed by the entity identified by the next certificate in the chain. The chain terminates with a root CA certificate. For browsers to trust the site's certificate, you must specify the full chain: site certificate, intermediate CA, and root CA. Use the uploadCustomCertificate API calls for each level of the chain. The certificate and private key parameters need to have the full text in PEM encoded format. For example: **'certificate':'-----BEGIN CERTIFICATE----- \nMIIDYTCCAkmgAwIBAgIQCgEBAQAAAnwasdfKasd**

4.1.6. Using Custom Certificates

You can obtain a signed wildcard certificate for your domain from any Certificate Authority, such as VeriSign. Before you use the the custom certificate, consider the following CloudPlatform specific instructions.

4.1.6.1. Prerequisites

- System VMs and the corresponding agents are up and running.

  If they are not up, the existing URL might still be pointing to the obsolete realhostip.com domain.

- Use the uploadCustomCertificate API to upload root and intermediate certificate. Server certificate and private key can also be uploaded through the UI.

- The certificates are URL encoded.

  One method to do so is using Google chrome Advanced Rest Client to URL encode your certificate. It converts a new line into %0A, and therefore the certificate becomes single line rather than multiple lines.

- The certificates are in PEM format.

- Consider the following while uploading intermediate certificates:
  - Intermediate certificate is not required for custom certificates.
  - Upload intermediate certificate for custom chained certificates.
- Upload certificates in the correct order. Use **id=1** for the first root certificate, then for the subsequent intermediate certificates use **id=2**, **id=3**, **id=4**, and so on.
- There is no convention for the name parameter. However, name the root certificate as "root", and intermediate certificates as "intermediate1", "intermediate2" and so on for convenience. Keep the names always unique.
- Use the same domain name for the global configuration parameters, secstorage.ssl.cert.domain and consoleproxy.url.domain, and for all the certificates.

4.1.6.2. Uploading Custom Certificates

1. Upload the root certificate by using the uploadCustomCertificate API. For example:

```
http://123.23.23.23:8080/client/api?
command=uploadCustomCertificate&id=1&sessionkey=LAM0wM%2B0cejIYxCHprtGc4w15sg%3D&name
=root1&domainsuffix=customamogh.com&certificate=-----BEGIN+CERTIFICATE-----%0AMIID
%2FBAcMAlNDMRQwEgYDVQQKDAtDdXN0%0Ab2-----END+CERTIFICATE-----
```

2. Before uploading the next certificate, ensure that all the SystemVM agents are up and running.
3. (optional) Upload the intermediate certificate by using the uploadCustomCertificate API. For example:

```
http://123.123.123.123:8080/client/api?
command=uploadCustomCertificate&id=2&sessionkey=LAM0wM%2B0cejIYxCHprtGc4w15sg%3D&name
=intermed1&domainsuffix=customamogh.com&certificate=-----BEGIN+CERTIFICATE-----
%0AMIID5TCCAs2gAwIBAgICEAAwDQYJKo%0A-----END+CERTIFICATE-----
```

4. Using the CloudPlatform UI, upload the server certificate and private key:
   a. In the left navigation pane, click Infrastructure.
   b. Click SSL Certificate.

      The SSL Certificate window is displayed.
   c. In the SSL Certificate window, specify the following:
      - The server certificate.
      - Private key in PKCS#8 format.
      - DNS Domain suffix. For example, .yourdomain.com.
5. Click OK.

   If the certificate is successfully uploaded, you see the "Update SSL certificate succeeded" message.
6. Restart the SystemVMs for the changes to take effect.

7. To verify, perform the following:

    - Open a Console Proxy VM console. It should show the embedded iframe source URL with HTTP (for version 4.3) or HTTPS protocol.
    - For Secondary Storage VM, copying a template from one zone to another should work as expected. Alternatively, download a template, volume, or iso. The download URL should display HTTP / HTTPS protocol in its path, and you should be able to download the entity.

Fixed Issues

Issue ID	Description
CS-20187	[KVM] Memory size has been increased to fix a memory issue on the Management Server.
CS-20116	Scheduled snapshots no longer breaks subsequent async jobs.
CS-20109	An account can be created with a password that contains '#' character.
CS-20031	"InvocationTargetException" error no longer occurs when you delete a port forwarding, firewall, or load balancer rule.
CS-20022	Shared networks with the same CIDR and IP ranges can be created on different VLANs.
CS-20020	The listUsageRecords API no longer generates null pointer exception for expunging instances.
CS-20009	[VMware] System VMs now successfully start on CloudPlatform 4.3 with vSphere 5.5 and DVS.
CS-20005	The metadata API is now accessible after upgrade.
CS-19986	[KVM] Private gateway works as expected in VPC router.
CS-19972	Async Job for detaching a volume now includes the instance UUID.
CS-19962	An instance now can be deployed to multiple Advanced network with Security Group.
CS-19961	The listUsageRecords API works as expected across domains.
CS-19951	[VMware] VMs successfully start up after a failed migration attempt.
CS-19947, CS-19758	[KVM] Traffic label are no longer ignored in Basic zone.
CS-19946	[VMware] VM Sync no longer shows running VMs' status as Stopped on the host.
CS-19905	During VM operations, neglect the "reaching concurrency limit 1" error message as long as no CPU spikes occurs.
CS-19900	Secondary Management Server successfully connects to the peer Management Server.
CS-19884	Multiple LDAP users can now be imported into a CloudPlatform account.
CS-19871	[XenServer] Attaching and detaching volume works as expected.
CS-19865	DHCP service no longer concurrently runs on two VRs in a Redundant VR setup.

Issue ID	Description
CS-19812, CS-19854	The security policy and firewall filter term are no longer removed When a VM with a Static NAT bound is destroyed.
CS-19806	[VMware] Storage traffic label is no longer ignored. Storage traffic port group is created successfully on vSwitch4 and therefore Secondary Storage VM can now access storage.
CS-19757	[VMware] Tagged VLAN support is now fixed for Management/Control/Storage traffic.
CS-18980	Various EventBus issues have been fixed.

Known Issues

Issue ID	Description
CS-16008	In a clustered management server deployment, hosts are not load balanced across management servers in cluster. This is by design. **Workaround**: All Management server in cluster must be synced by running: `# ntpdate 0.xenserver.pool.ntp.org` `# service ntpd start`
CS-16373	[KVM] When a KVM cluster is taken to the Unmanaged state, then returned to the Managed state, the hosts do not come into the UP state. **Workaround**: Manually restart cloud-agent on the KVM hosts to bring up the hosts.
CS-18561	[VMware] After upgrading from 3.0.x to 4.2 and higher versions, restoring the existing VM which has an additional disk fails to boot. **Workaround**: If the *vmware.root.disk.controller* global parameter is set to *ide* in 3.0.x setup, after upgrade perform following: • Before performing any VM operations, such as start and restore, set *vmware.root.disk.controller* to *scsi*. • Restart the Management Server. If *vmware.root.disk.controller* is set to *scsi* in 3.0.x setup, you need not change anything, because the controller setting is consistent across upgrade operations.
CS-18728	Re-copying templates to other zones doesn't work.
CS-18616	Event messages should provide VM name along with VM ID when deleting VMs.
CS-18605	Order of templates and ISOs not honored by UI or API.
CS-18558	Version 4.2 does not show account information on UI for dedicated host.
CS-18743	[XenServer] VM state is incorrectly reflected in CloudPlatform if VM is deleted outside of CloudPlatform. In this case, the VM state is

Issue ID	Description
	marked as Stopped in CloudPlatform. Depending on whether or not the on-disk information is still maintained, you may or may not be able to start it again in CloudPlatform.
CS-18834	[Hyper-V] More than 13 disks cannot be attached to a guest VM.
CS-18973	[VMware] Volumes cannot be downloaded after SSVM is HAed. Download fails with the "Failed to copy the volume from the source primary storage pool to secondary storage" error. **Workaround**: Either remove the host that experiences the issue from the vCenter or bring it back. This issue is caused by limitations from vCenter when one of host is at disconnect or down state. If the host is at disconnect or down state in vCenter, vCenter will encounter an internal server error when it serves the URL request for file downloading and uploading operations to its datastores.
CS-18991	HA rebooted several VMs while they were still running on a disconnected host.
CS-19109	Async response from addAccountToProject doesn't contain resource ID and description information.
CS-19105	At times virtual router is configured with a network IP which is invalid.
CS-19177	CloudPlatform does not support external LB's private interface on a different network segment than the guest network.
CS-19259	Templates created from snapshots are not replicated to multiple secondary storage.
CS-19253	[XenServer] Discrepancy in the CloudPlatform and XenServer view of available memory.
CS-19285	[VMware] When changes to a VM state is performed out-of-band, VR goes out of sync and is eventually shuts down. Workaround: Stop and restart the VM by using the CloudPlatform Management Server.
CS-19250	The iptables chain name is too long; it must be under 30 characters.
CS-19492	CloudPlatform fails to acquire a Source NAT IP in the presence of 2 or more isolated networks with a minimum one of them is configured with external device.

Issue ID	Description
CS-19405	[XenServer] *vm.instancename.flag = true* has no effect when creating a VM.
CS-19530	Template ordering in the UI does not work as expected.
CS-19659	[Hyper-V] VRs might be force stopped when guest VMs are deployed across more than 20 isolated networks in parallel.
CS-19675	[VMware] In clusters with multiple primary storages configured VMs fail to restart when either Reset VM operation is performed or the compute offering has the Volatile option enabled.
CS-19685	VMware Distributed vSwitch is only supported for public and guest networks, but not for management and storage networks.
CS-19707	[VMware] Legacy Windows VMs cannot be restarted after attaching a DATA volume. This issue is observed only when the value for *vmware.root.disk.controller* is changed from *ide* to *osdefault*, which in turn results in losing the previous controller information. **Workaround**: Update the user_vm_details table such that the information about the previous controller before changing to osdefault is persisted in database. Sample query: `#insert ignore user_vm_details (vm_id,name,value,display_detail) values(2,'rootDiskController','ide',1);`
CS-19895	[Realhostip] The certificate for a custom domain can't be reverted after it's uploaded. To use the realhostip domain, upload the realhostip certificate and key again.
CS-19885	[Realhostip] Certificates uploaded in 4.x versions without realhostip-related fixes fail after upgrading to a version with those defect fixes. **Workaround**: After the upgrade, upload the certificate again in the correct order with supplying all the parameters.
CS-20150	After upgrading from CloudPlatform 4.2.1 to 4.3, the VPN Customer Gateway functionality goes missing. The script to encrypt **ipsec_psk** during upgrade is missing in version 4.2.1, which causes this issue. **Workaround**: Run the following to encrypt the values of **ipsec_psk** in the **s2s_customer_gateway** table:

Issue ID	Description
	`` # java -classpath /usr/share/ cloudstack-common/lib/jasypt-1.9.0.jar org.jasypt.intf.cli. JasyptPBEStringEncryptionCLI encrypt.sh input=<clearText> password=<secretKey> verbose=false ``` Use the secret key for the database.
CS-20181	[Realhostip] The SSL certificates uploaded with invalid sequence numbers are not handled. **Workaround**: Upload certificates in the correct order. Use id=1 for the first root certificate, then for the subsequent intermediate certificates use id=2, id=3, id=4, and so on.
CS-20192	[Realhostip] Specify the same domain name in the following: • SSL certificates you upload • *`consoleproxy.url.domain`* • *`secstorage.ssl.cert.domain`* Using seperate domain name for the SSL certificate and each of these System VM global parameters is not supported.
CS-20246	[Realhostip] If invalid certificates are uploaded, the SSL error you get while viewing the console might refer to realhostip.com. Neglect this error for debugging. Uploading a valid certificate would resolve the issue.
CS-20319	[Realhostip] The Console Proxy VMs need to be recreated after changing the communication mode from HTTP to HTTPS vice versa. **Workaround**: Stop all the running Console Proxy VMs so that they are directed to listen on the right port.
CLOUDSTACK-1717	Local region entry that is added by default should not include "/api" for its end_point. Additionally, the endpoint should have the actual hostname instead of localhost.
CLOUDSTACK-2112	VM will go into stopped state after a failed live migration during a scale up VMs operation. **Workaroud**: Manually restart the VM.
CLOUDSTACK-2293	DeletePhysicalNetworkCmd is not deleting the external devices.
CLOUDSTACK-2646	When firewall and LB service providers are different, CloudPlatform incorrectly allows both

Issue ID	Description
	the rules on the same public IP. Workaround: Admin should not create network offering with different service providers for firewall and LB, while keeping conserve mode on.
CLOUDSTACK-2910	Ctrl combined with > is not working on SC IME. **Workaround**: Click the “Chinese/Western Punctuation(Ctrl+.)” in the IME tool bar to switch the punctuation between full-width and half-width.
CLOUDSTACK-3111	Volume listing screen shows Hypervisor column as empty if the volumes are attached to instances running in KVM Hypervisor.
CLOUDSTACK-3212	Default guest network can now have multiple subnets per VLAN, but the IP range list page does not display the netmask and gateway for each subnet. **Workaround**: Use the API listVlanIPRanges to get the complete details.
CLOUDSTACK-3317	Management and storage network traffic cannot be configured to use VMware Distributed vSwitch (DVS). Continue to use standard vSwitch.
CLOUDSTACK-3895	VM Migration across VMware clusters which are added with different switches (Standard Switch,VMware DVS, Cisco Nexus 1000v) is not supported.
CLOUDSTACK-3680	[KVM on CentOS 5.5, 5.6] While accessing console view of a guest virtual machine, the keystrokes tab, ctrl, \, tilde, single quote, double quote, and caret ^ do not work on CentOS 5.5\5.6 running on KVM. This is due to a known bug in CentOS (see *http://www.centos.org/modules/newbb/viewtopic.php?topic_id=33233&forum=55*[1].
CLOUDSTACK-3968	Distributed port groups on DV Switch are not removed when the associated account from CloudPlatform is removed.
CLOUDSTACK-4016	The listPublicIpAddresses API lists the portable IP that was already transferred to a different Isolated network.
CLOUDSTACK-4139	[VMware] The volumes created from snapshots on VMware deployments cannot be resized when attached to a running VM. The volume is created with IDE disk instead of SCSCI disk which cannot be resized.

[1] http://www.centos.org/modules/newbb/viewtopic.php?topic_id=33233&forum=55

Issue ID	Description
	Workaround: Detach the volume created from a snapshot and resize it, and then reattach it to the VM.
CLOUDSTACK-4207	The following exception is observed when the Management Server is started after upgrade from any older versions to CloudPlatform 4.2. **`jsonParseException: The JsonDeserializer com.cloud.agent.transport. ArrayTypeAdaptor@2426e26f failed to deserialize json object`** Ignore this exception, this would stop after you upgrade the System VM. However, if you want to prevent this, stop system VM from the hypervisor before upgrade.
CLOUDSTACK-4364	Restore VM needs to log usage event for volume so that it is correctly charged for usage.
CLOUDSTACK-4475	If cluster-wide and zone-wide primary storage are mixed together, the data disk by default will be created on cluster wide primary storage. **Workaround**: If admin wants data disk to be created on zone-wide primary storage, then create a disk offering with the tag on zone-wide primary storage.
CLOUDSTACK-4492	Uploaded volume state was not set to "Uploaded" in CloudPlatform 3.0.6. After upgrade to 4.x, volume attach fails because of volume being in incorrect state. **Workaround**: Upload and attach volume after the upgrade.
CLOUDSTACK-4517	Deployment of VM using CentOS 6.2 template registered before upgrade is failing.
CLOUDSTACK-4578	[VMware] If the host where the SSVM is running goes down, the SSVM is not being recreated on another host in the cluster. **Workaround**: Forcefully stop the SSVM through the CloudPlatform API call stopSystemVm. Then the new SSVM will be created on a second host.
CLOUDSTACK-4593	Live Storage Migration and VM Snapshot features are not fully functional after upgrade. **Workaround**: Stop and then start the VM post upgrade.
CLOUDSTACK-4622	If a VM from a guest network is added to a network tier of a VPC, then IP reservation allows

Issue ID	Description
	the CIDR to be the superset of Network CIDR for that VPC tier.
CLOUDSTACK-5452	[KVM] Agent is not able to connect back if the Management Server was restarted when pending tasks to the hosts are remaining. **Workaround**: Restart the agent.
CLOUDSTACK-5463	[Hyper-V] Stopped VMs are not reported, because out of band state changes occurred on VMs or hosts are not reconciled by CloudPlatform.
CLOUDSTACK-5485	[VMware] When 10 hourly snapshots are scheduled in parallel,only 5 of them are being simultaneously processed actively. To increase the number of simultaneous commands processed in SSVM (increase the count of worker threads), modify the agent properties file in SSVM to specify the number of workers. • Stop the cloud service: `service cloud stop` • In SSVM, update the following file to add the number of line workers: `/usr/local/cloud/systemvm/conf/agent.properties` • Run the cloud service: `service cloud start`
CLOUDSTACK-5501	Creating more than one VPN connection per customer gateway is not supported.
CLOUDSTACK-5660	[Hyper-V] Even when live migration of a VM succeeds, the following error is thrown: "Failed to migrate the system vm".
CLOUDSTACK-5753	[Hyper-V] ConsoleProxyLoadReportCommand does not honor the default value of consoleproxy.loadscan.interval, which is 10 second.
CLOUDSTACK-5815	[Hyper-V] Two SNAT rules for one isolated network is created if the acquired IP is from a different VLAN.