Citrix CloudPlatform (powered by Apache CloudStack) Version 4.3 Release Notes

Revised April 9, 2014 3:00 pm IST

Citrix CloudPlatform (powered by Apache CloudStack) Version 4.3 Release Notes
Revised April 9, 2014 3:00 pm IST

Release notes for Citrix CloudPlatform version 4.3.

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. Most earlier OS and hypervisor versions are also still supported for use with 4.3. 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 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 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-2014-01-14-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 URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2013-12-23-hyperv.vhd.bz2*

Hypervisor	Description
	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-2014-01-14-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 Public: no Featured: no
VMware	Name: systemvm-vmware-4.3 Description: systemvm-vmware-4.3

Hypervisor	Description
	URL (64-bit system VM template): *http://download.cloud.com/templates/4.3/systemvm64template-2014-01-14-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 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

Feature Category	Feature Details
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
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

Unsupported UI Options	UI Wizard
	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 4.2.x to 4.3

Perform the following to upgrade from version 4.2.x to version 4.3.

1. Download the latest System VM templates:

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.3 Description: systemvm-xenserver-4.3 URL: *http://download.cloud.com/templates/4.3/systemvm64template-2014-01-14-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: *http://download.cloud.com/templates/4.3/systemvm64template-2014-01-14-master-kvm.qcow2.bz2*

Hypervisor	Description
	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 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: *http://download.cloud.com/templates/4.3/systemvm64template-2014-02-13-master-vmware.ova* 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 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

Hypervisor	Description
	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 RHEL 6.3 binaries from *https://www.citrix.com/downloads/cloudplatform.html*.

   b. Extract the binaries:

   ```
   # cd /root
   # tar xvf CloudPlatform-4.3.0.0-1-rhel6.3.tar.gz
   ```

   c. Create a CloudPlatform 4.3 qemu repo:

   ```
   # cd CloudPlatform-4.3.0.0-1-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-4.3.0.0-1-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 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*[1].

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.

[1] 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/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.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 XS62ESP1004.

    For more information, see *Section 3.5.4, “Upgrading to XenServer 6.2 SP1 Hotfix XS62ESP1004”*.

    For instructions for upgrading XenServer software and applying hotfixes, see *Section 3.5.2, “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.

Note

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.

Note

(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".

3.2. Upgrade from 3.0.x to 4.3

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.

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):

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.3 Description: systemvm-xenserver-4.3 URL: *http://download.cloud.com/templates/4.3/systemvm64template-2014-01-14-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

Hypervisor	Description
	Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.3 Description: systemvm-kvm-4.3 URL: *http://download.cloud.com/templates/4.3/systemvm64template-2014-01-14-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 XenServer, 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: *http://download.cloud.com/templates/4.3/systemvm64template-2014-02-13-master-vmware.ova* Zone: (4.3 and beyond) Choose the zone where this hypervisor is used. If your

Hypervisor	Description
	CloudPlatform deployment includes multiple zones running XenServer, 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

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.

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 RHEL 6.3 binaries from *https://www.citrix.com/downloads/cloudplatform.html*.

   b. Extract the binaries:

```
# cd /root
```

```
# tar xvf CloudPlatform-4.3.0.0-1-rhel6.3.tar.gz
```

c. Create a CloudPlatform 4.30.0 qemu repo:

```
# cd CloudPlatform-4.3.0.0-1-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-4.3.0.0-1-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 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].

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.

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:

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

```
# 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, 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.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 Mon Nov 12 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 Fri Nov 8 15:10:04 PST 2012
```

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 XS62ESP1004.

    For more information, see *Section 3.5.4, “Upgrading to XenServer 6.2 SP1 Hotfix XS62ESP1004”*.

    For instructions for upgrading XenServer software and applying hotfixes, see *Section 3.5.2, “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.

Note

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.

Note

(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".

3.3. Upgrade from 2.2.x to 4.3.0

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 to 4.3.0, any existing IP address usage records in the old format will no longer be available.

2. If you are using version 2.2.0 - 2.2.13, first upgrade to 2.2.14 by using the instructions in the *2.2.14 Release Notes*[3].

[3] http://download.cloud.com/releases/2.2.0/CloudStack2.2.14ReleaseNotes.pdf

Note

(KVM only) If KVM hypervisor is used in your cloud, be sure you completed the step to insert a valid username and password into the host_details table on each KVM node as described in the 2.2.14 Release Notes. This step is critical, as the database will be encrypted after the upgrade to 4.3.0.

3. While running the 2.2.x system (which by this step should be at version 2.2.14 or greater), log in to the UI as root administrator.

4. Using the UI, add a new System VM template for each hypervisor type that is used in your cloud. In each zone, add a system VM template for each hypervisor used in that zone.

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):

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.3 Description: systemvm-xenserver-4.3 URL: *http://download.cloud.com/templates/4.3/systemvm64template-2014-01-14-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.

Hypervisor	Description
	(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: *http://download.cloud.com/templates/4.3/systemvm64template-2014-01-14-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 XenServer, 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

Hypervisor	Description
	Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.3 Description: systemvm-vmware-4.3 URL: *http://download.cloud.com/templates/4.3/systemvm64template-2014-02-13-master-vmware.ova* 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 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

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.

Warning

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

5. (KVM on RHEL 6.0, 6.1) 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 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-rhel6.3.tar.gz
   ```

   c. Create a CloudPlatform 4.3.0 qemu repo:

   ```
   # cd CloudPlatform-4.3.0-1-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-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 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].

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
```

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.

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
```

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

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

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

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

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

15. Repeat steps *9* - *14* on every management server node. If you provided your own encryption key in step *14*, use the same key on all other management servers.

16. 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.

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

```
# service cloudstack-usage 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 .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 admin, and check the status of the hosts. All hosts should come to Up state (except those that you know to be offline). You may need to wait 20 or 30 minutes, depending on the number of hosts.

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

20. 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.

21. 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 Mon Nov 12 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 Fri Nov 8 15:10:04 PST 2012
```

22. (XenServer only) Upgrade all existing XenServer clusters to XenServer 6.2 SP1 Hotfix XS62ESP1004.

    For more information, see *Section 3.5.4, "Upgrading to XenServer 6.2 SP1 Hotfix XS62ESP1004"*.

    For instructions for upgrading XenServer software and applying hotfixes, see *Section 3.5.2, "Applying Hotfixes to a XenServer Cluster"*.

23. (VMware only) Ensure that you provide the values vCenter host, vCenter Username, vCenter Password, and vCenter Datacenter when you add a new VMware cluster to a zone that was created with a previous version of CloudPlatform.

    The Add Cluster dialog in the CloudPlatform user interface incorrectly shows these options 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".

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 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*[5].

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

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
```

3.5. 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.

3.5.1. Upgrading to a New XenServer Version

To upgrade XenServer hosts when running CloudPlatform 4.3.0:

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.

3.5.2. 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: XS62ESP1004.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).

3.5.3. 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
      ```

3.5.4. Upgrading to XenServer 6.2 SP1 Hotfix XS62ESP1004

It is highly recommended that all XenServer clusters are upgraded to XenServer 6.2 SP1 Hotfix XS62ESP1004. 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 XS62ESP1004 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 XS62ESP1004

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

CloudPlatform 4.3 includes the following new features. For the latest APIs changes, see the CloudPlatform 4.3 Developer's Guide.

4.1. Hyper-V Support

CloudPlatform 4.3 rolls out support for Hyper-V hosts. For Hyper-V, CloudPlatform supports SMB-based storage. If you want to run guest VMs on Hyper-V hosts, install CloudPlatform Agents on each Hyper-V hosts. Before you use Hyper-V, review the following list of supported and non-supported features. For detailed instruction, see the Installing Hyper-V for CloudPlatform chapter in the CloudPlatform 4.3 Installation Guide.

4.1.1. Supported Functionalities

- VM Compute
  - All the VM operations, except VM Snapshots
  - Live Migration
  - Service Offerings (Scale up on stopped VMs)
  - Console access
  - SSH key and reseting SSH key
  - Upload and download templates, volumes, and ISO
  - Create VMs from template and ISO
  - Create template from volume
  - Attach and detach VMs from ISO and password-enabled template
  - Copy template across zone
- Storage
  - Primary Storage (SMB and Local)
  - Root and data volumes on Local and SMB
  - Add, delete, attach, detach volumes (one or more volumes per VM)
  - Single and multiple secondary storage (SMB)
- Network
  - VLANs (Isolated and Shared)
  - All VR services: DNS, DHCP, SourceNAT, LB, PF, Firewall, StaticNAT, Userdata, and VPN
  - External device support for both Isolated and Shared networks: Netscaler, SRX, F5
  - Multiple physical networks

  - Dedicated IP range, Public VLANs (to account)
  - Network Offering upgrades and updates
  - L4-L7 services in Shared network
  - Multiple IP ranges and portable IPs
- Host and Storage in maintenance mode

4.1.2. Unsupported Functionalities

- Affinity an Anti-Affinity Groups
- Network throttling
- Security groups (Advanced Zone)
- IPv6
- Snapshot: VM and disk
- PVLAN
- VPC
- HA of guest VMs
- Redundant VR
- Object Store
- Mixed hypervisor zone
- Zone-wide Primary storage
- NIC bonding

4.2. Enhanced Upgrade for Virtual Routers

Upgrading VRs is made flexible. The CloudPlatform administrators will be able to control the sequence of the VR upgrades. The sequencing is based on Infrastructure hierarchy, such as by Cluster, Pod, or Zone, and Administrative hierarchy, such as by Tenant or Domain. This implies, for example, that you will have the flexibility to upgrade a VR in a specified zone. As an administrator, you can also determine when a particular VR can be upgraded within a specified upgrade interval. Additionally, upgrade operation is enhanced to increase the upgrade speed by allowing as many upgrade operations in parallel as possible. During the entire duration of the upgrade, users cannot launch new services or make changes to an existing service.

To support this feature, a new API, upgradeRouterTemplate, has been introduced.

The detailed instruction is provided in the CloudPlatform 4.3 Administration Guide. See section 17.5.5. Enhanced Upgrade for Virtual Routers.

4.3. Service Monitoring Tool for Virtual Router

Various services running on the CloudPlatform virtual routers can be monitored by using a Service Monitoring tool. The tool ensures that services are successfully running until CloudPlatform deliberately disables them. If a service goes down, the tool automatically performs a restart, and if that does not help bringing up the service, an alert as well as an event is generated indicating the failure.

The following services are monitored in a VR:

- DNS
- HA Proxy
- SSH
- Apache Web Server

Only the services with daemons are monitored.

The following networks are supported:

- Isolated Networks
- Shared Networks in both Advanced and Basic zone

This feature is supported on the following hypervisors: XenServer, VMware, and KVM.

The detailed instruction is provided in the CloudPlatform 4.3 Administration Guide. See section 17.5.4. Service Monitoring Tool for Virtual Router.

4.4. Remote Access VPN for VPC

Support for Remote access VPN in Isolated networks is now extended to VPC networks. Remote users will now be able to initiate a VPN connection to a VPC network. To enable this feature, enable VPN in the Source NAT IP of the VPC.

4.5. Site to Site VPN Connection Between VPC Networks

CloudPlatform provides you with the ability to establish a site-to-site VPN connection between CloudPlatform virtual routers. With this functionality, users can deploy applications in multiple Availability Zones or VPCs, which can communicate with each other by using a secure Site-to-Site VPN Tunnel. Creating a typical Site to Site VPN connection between VPC networks involves the following:

1. Create two VPCs. For example, VPC A and VPC B.
2. Create VPN gateways on both the VPCs you created.
3. Create VPN customer gateway for both the VPCs.
4. Enable a VPN connection on VPC A in passive mode.

   Ensure that the customer gateway is pointed to VPC B. The VPN connection is shown in the Disconnected state.
5. Enable a VPN connection on VPC B.

Ensure that the customer gateway is pointed to VPC A. Because virtual router of VPC A, in this case, is in passive mode and is waiting for the virtual router of VPC B to initiate the connection. The virtual router of VPC B should not be in passive mode.

The VPN connection is shown in the Disconnected state.

Creating VPN connection on both the VPCs initiates a VPN connection. Wait for few seconds. The default is 30 seconds for both the VPN connections to show the Connected state.

4.6. Reporting CPU Sockets

CloudPlatform now provides an additional infrastructure statistics for CPU sockets managed by CloudPlatform, which in turn reflects the size of the cloud. The Infrastructure tab has a new tab for sockets. The Socket page will give you the number of hosts an sockets used for each hypervisor type. This feature is not supported in versions prior to XenServer 6.2.

4.7. Database High Availability

To help ensure high availability of the databases that store the internal data for CloudPlatform, you can set up database replication. This covers both the main CloudPlatform database and the Usage database. Replication is achieved using the MySQL connector parameters and two-way replication. Tested with MySQL 5.1 and 5.5. Database replication in CloudPlatform is provided using the MySQL replication capabilities. The steps to set up replication can be found in the MySQL documentation.

4.8. LDAP User Provisioning

LDAP user provisioning has been enhanced by allowing user import from the configured LDAP servers. You will be able to add multiple LDAP servers and selectively import LDAP users. You can o filter by group name and import all the users within a group. After they have been imported to CloudPlatform, in contrast to manually adding them in previous releases, users are allowed to directly log in to CloudPlatform by using the LDAP credentials.

4.9. Migrating NFS Secondary Storage to Object Store

In an existing zone that is using NFS for secondary storage, you can upgrade the zone to use a region-wide object storage without causing downtime. The existing NFS storage in the zone will be converted to an NFS Staging Store. After migration, the data that was on the NFS storage remains there. CloudPlatform does not provide a way to automatically migrate all data to the new object storage. The data remaining on the old NFS storage will remain accessible for read and delete operations only. Newly created snapshots and templates will be placed in the newly configured object storage.

4.10. VXLAN Plugin Support

The VXLAN plugin adds VXLAN as one of the guest network isolation methods in CloudPlatform. This plugin enables more than 4096 isolated guest networks in a Zone, with almost the same usability as VLAN isolation. This plugin provides no network services. Use virtual router for network services. This plugin is supported on KVM hypervisors.

4.11. Contrail Network Plugin Support

The Contrail virtual network controller is an open source project that provides an overlay implementation of network virtualization that is interoperable with network devices that support existing

network virtualization standards. Support for the Contrail plugin has been added to CloudPlatform to provide NAT services to the XenServer hosts. The plugin supports isolated networks, Static NAT implemented by the VRouter dataplane, and Source NAT implemented by using a virtual appliance with full NAT functionality.

4.12. Support for XenDesktop on CloudPlatform

Support for XenDesktop as a workload on CloudPlatform has been added. If you want to use this feature, ensure that XenServer version 6.2 SPI Hotfix XS62ESP1003 has been applied to all the XenServer hosts.

4.13. Publishing Alert Using the Web ROOT Admin API

In previous releases of CloudPlatform code alerts are generated for CloudPlatform services (Usage service) only if they run on the same host as the Management Server. A new API has been introduced in 4.3, which can be used by the following services to generate and publish. The services need not be running on the same host where the Management Server is running.

- Any new services added to CloudPlatform.
- Usage service when run on a separate storage host.
- Console Proxy and Secondary Storage VM services.

The main advantage of this feature is that the third party systems integrating with CloudPlatform will be able to utilize the Alert notification system publish alerts.

4.14. Recording Usage Events for Dynamically Assigned Resources

CloudPlatform supports recording usage events as per the dynamically assigned resources. Usage events are registered when a VM is created from dynamic service offering, and the values of parameters, such as CPU, speed, RAM are recorded. If VM is deployed by using template and dynamic root disk size is mentioned, the same value is recorded in the usage event.

4.15. Handling Command Execution at Hypervisor and VR Level

Prior to CloudPlatform 4.3, ability to execute parallel commands at hypervisor and VR level was controlled by the following global parameters: *`execute.in.sequence.hypervisor.commands`* and *`execute.in.sequence.network.element.commands`*. From CloudPlatform 4.3 onwards, you will not have the ability to use these global parameters to issue commands for parallel VM deployment or VM migration. Instead, CloudPlatform will have a single mode of command operation depending on the hypervisor type.

VMware

By default, parallel execution is enabled if linked-clone is set. Serial execution is enabled if full-clone is set.

XenServer

Serial execution is enabled by default.

KVM

Serial execution is enabled by default.

Hyper-V

Serial execution is enabled by default.

Irrespective of the hypervisor, commands will always be sent in parallel to the VR. At VR level, these commands get executed sequentially.

4.16. Assigning IP to a VM at Deployment

Deploying a VM in one or multiple networks with custom IP addresses specified for each network is supported. This feature is supported on VPC, Isolated, and Shared networks.

4.17. Support for Pluggable VM Snapshots

CloudPlatform implements a plugin to integrate a third-party storage provider. Third party storage providers can integrate with CloudPlatform to provide either primary storage or secondary storage. The user enables a storage plugin through the UI. A new dialog box choice is offered to select the storage provider. Depending on which provider is selected, additional input fields may appear so that the user can provide the additional details required by that provider, such as a user name and password for a third-party storage account.

4.18. Enhanced CloudPlatform UI

A complete UI makeover is implemented to enhance the usability and user experience in modern browsers. The visual look-and-feel has been changed for the Header, Navigation, Buttons, text fields, drop-downs, tables and so on. Consistent color themes has been introduced to match with the Citrix branding.

The current UI flow remains the same.

4.19. List View Widget

List view widget has been enhanced to allow concurrent actions on multiple list items. You can select multiple list view items, and execute actions on them at once. For example, you can simply select multiple primary storages and take snapshot.

Fixed Issues

Issue ID	Description
CS-13674	[XenServer] If the HOST_NOT_ENOUGH_FREE_MEMORY error is encountered, a new VM on another host/ cluster/pod is now created.
CS-17637	Serial job processing is removed in VMware environment.
CS-18122	JVM now work as expected if max heap memory size over 2666m.
CS-18177	All VMs in a cluster are no longer stopped or started after the Management Server restart.
CS-18271	Help link no longer points to nonexistent docs site.
CS-18303	VDI corruption issue is now fixed.
CS-18414	Timezone difference in snapshots is fixed now. The Management Server no longer fails to start due to this issue.
CS-18501	Default IP table rules configuration no longer fails on VR.
CS-18535	[VMware] After every cold migration of a volume to another primary store, start the VM associated with that volume before you move another volume. This is to ensure that the data structures between CloudPlatform and VMware vCenter are better aligned.
CS-18355	[Baremetal] The Security group ingress and egress rules now function as expected.
CS-18500	[XenServer] Time zone issue is fixed on Windows VMs.
CS-18517	The host capacity is now updated after force reconnect from the Management Server.
CS-18539	The networks that are not implemented can now be removed successfully.
CS-18542	An option has been added to the createVolume API to specify a VM for the volume.
CS-18574	[VMware] Getting VM statics no longer fails with NullPointerException.
CS-18584	[XenServer] The Redundant VR works as designed on XenServer 6.2 hosts with the bridge networking back-end.
CS-18531	Template deletion no longer fails if template status is connection refused or no route to host.

Issue ID	Description
CS-18591	Security Group rules are now successfully programmed for any VM after upgrading to version 4.2.1.
CS-18578	Duplicate entries no longer exists for router VMs in the UI under project view when logged in as root admin.
CS-18598	[KVM] Hypervisor now honors ICMP rules.
CS-18603	[XenServer] Host migration no longer fails during 3.0.7 to 4.2.1 upgrade.
CS-18608	The listNetworks API now properly handles the page size and page parameters.
CS-18609	VPN active sessions are no longer dropped if a new VPN user is created on VR.
CS-18610	Downloading template works as expected as the issue with the storage.PrimaryStorageDownloadCommand is fixed.
CS-18614	Ping timeout no longer occurs on the hosts which are in the UP state.
CS-18621	The VR NIC details now persists in the database for additional public ranges. Migration no longer fails because the bridges for NICS are correctly created.
CS-18622	The regular expression in edithosts.sh script on the VR is now modified properly. Therefore, IPs are not accidentally removed during update.
CS-18623	The listVirtualMachines no longer returns NICs in random order.
CS-18627	On router reboot, existing firewall CIDR is now successfully loaded.
CS-18637	[XenServer] When migrating VMs between hosts of different versions,time offset is maintained.
CS-18607	Instance displayname is returned in the response.
CS-18649	NFS storage pools are updated as expected during over-provisioning.
CS-18606	Ability is added to start Virtual Router on Guest VM reboot.
CS-18644	You can now start instance with disk offering of storage tag 'DATA_DISK'.
CS-18645	Firewall rules are now restored on Virtual Router when it is restarted.
CS-18660	The listHosts API command is narrowed down in UI on System VMs page.

Issue ID	Description
CS-18634	CPU cap calculated correctly for VMs on XenServer hosts.
CS-18711	You can delete a template or ISO that was failed to download.
CS-18723	Guest OS support for Windows 8.1
CS-18792	Requested device ids are mirrored in a Linux instance.
CS-18722	Local disk usage on host shows up in the UI.
CS-18754	You can delete snapshot with Error state from the UI.
CS-18724	When migrating System VMs browser no longer shows progress icon forever.
CS-18732	Public templates are visible outside the domain tree.
CS-18753	Search box for VMs work as expected on Enable Static NAT page.
CS-18729	Templates created from a snapshots can be copied to other zones.
CS-18713	The login API can now be used with api key and signature.
CS-18730	OVA/OVF files are now consistently created for templates.
CS-18757	When S3 object store is used as Secondary Storage, the template created from different zone is not available for the other zones.
CS-18785	The VMs deployed before XenServer 6.0.2 XS602E030 patch installation now acquire new rules set as expected after the patch installation.
CS-18801	The create.Pod API no longer hangs when all values passed are -1.
CS-18820	VMs are migrated in parallel when hosts are kept in Maintenance mode.
CS-18876	The listVirtualmachine API response no longer contains duplicate NICs entries.
CS-18861	Listing hosts for stopped instances no longer fails with an error dialog popping up.
CS-18808	System VMs page now supports partial match search.
CS-18800	Response of listAccounts API call no longer includes removed users.
CS-18871	Value of CPU allocated for VMs is no longer shows 0%.
CS-18941	The awsapi behaviour is now stable on instance creation with official ec2 tools and boto script.

Issue ID	Description
CS-18930	Handling RHEL guests works as expected.
CS-18860	Capacity calculation is now correct when a host which has HA enabled guest VMs goes down.
CS-18896	CreateVolumeFromSnapshot no longer skips using the suitable storage pool found. It works as expected.
CS-18807	JSVC package is included in RHEL 6.4 builds
CS-18823	[VMware] root disk is on IDE and secondary disks are SCSI
CS-18927	HA works as expected. SSL handshake timeout is introduced.
CS-18929	Virtual router no longer deployed in disabled pod.
CS-18984	The rootdisksize text box is removed from the Deploy VM wizard in the UI.
CS-18987	Source NAT ipaddress of a Advanced zone with source NAT enabled network detail page now includes Configuration tab to allow PF and LB rule creation.
CS-19003/ CS-19204	Attaching volumes no longer fails on existing windows VM. Existing windows VM can now be restarted after resetting VM.
CS-19042	The dnsmasq race condition no longer results in dnsmasq failing to hand out IP addresses.
CS-19062	Live migration works as expected between two pods on advanced isolated network.
CS-19101	Creating new shared network with overlapping CIDR of another shared network works as expected even when a different VLAN ID is used.
CS-19116	[Hyper-V] System VMs now starts when untagged public VLAN is specified.
CS-19140	System Offering id is now set for virtual Router when creating a network offering.
CS-19124	Cluster can be added when VMware data center name contains space in between.
CS-19133	[XenServer]When master host is down, both user VMs and System VMs on this host are reported as being in Running state. This is by design. Note that when the master host is down, the whole cluster is not functional. Therefore, all the slave hosts will also not function as expected. This behavior is true only for XenServer Versions prior to 6.2 SP1 Hotfix XS62ESP1004.
CS-19165	Local data disk with tag no longer goes to a wrong local storage pool.

Issue ID	Description
CS-19180	Console proxy no longer connects to a different VM instance under certain timeout conditions.
CS-19193/ CS-19426	An IP can now be assigned to a VM at deploy time.
CS-19300	Guest network ACL is applied on VPC restart.
CS-19372	[KVM] The s3.singleupload.max.size option not applicable for backup snapshot.
CS-19388	Restarting user VMs works as expected if they are created when global parameter, vmware.root.disk.controller, is set to scsi.
CS-19448	Assign Instance to Another Account icon is added back.
CS-19464	Guest NIC can now be replugged to the VPC VR upon its restart.
CS-19538	No exception when attaching data disk to RHEL VM on vSphere.
CLOUDSTACK-2562	When a virtual router on a VMware ESX is restarted out of band by VMware HA, CloudPlatform now re-program the port forwarding, NAT, and load balancer rules.
CLOUDSTACK-3154	When a VMware data center is deleted from the Zone, the data center is deleted, and the UI screen no longer stays in processing state.
CLOUDSTACK-3252	A VM deployed by using explicit or implicit dedication now generates a usage event.
CLOUDSTACK-4861	Selection of physical network to implement guest network is now work as expected if guest traffic spans across multiple physical networks.
CLOUDSTACK-5145/ CS-18725	The ListNetworkACL API lists all the ACLs.

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-18615	[Hyper-V] SMB share passwords are visible in the logs.
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.

Issue ID	Description
CS-18604	Secondary Storage Server attempting to mount wrong Secondary Storage NAS.
CS-18726	CloudPlatform does not accept 2-byte code for Account first and last name.
CS-18651	Null pointer exception while running usage jobs.
CS-18743	[XenServer] VM state is incorrectly reflected in CloudPlatform if VM is deleted outside of CloudPlatform. In this case, the VM state is 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-18832	[Hyper-V] No Console access after a VM live migration.
CS-18834	[Hyper-V] More than 13 disks cannot be attached to a guest VM.
CS-18889	Upgrading some routers failed with Null Pointer Exception when execute.in.sequence.hypervisor.commands is set to true.
CS-18902	[XenServer] On a 6.2 SPI host, creating template from snapshot does not work because vhd.util is not found on expected location.
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 experiencing the issue from the vCenter or bring it back up. 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-18979	When publishing events are enabled using RabbitMQEventBus, certain operations such as LB rule deletion fails.
CS-19037	Template files are deleted from secondary storage after download.
CS-19066	Re-enabling Remote VPN access on the IP address does not work as expected.

Issue ID	Description
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-19136	Downloading templates does not work when 3 SSVMs are present in one zone.
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.
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-19600	Restart of VPC may result in VPC private gateway loss and loss of VR public interfaces.
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

Issue ID	Description
	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(21,'roo`
CS-19796	MySQL connector jar is not available in the Usage Server classpath. **Workaround**: Run the following on the Usage Server: `# ln -s /usr/share/java/mysql-connector-java.jar /usr/share/cloudstack-usage/lib/mysql-connector-java.jar`
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. 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 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.

Issue ID	Description
	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. **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.

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

Issue ID	Description
CLOUDSTACK-4402	Primary storage cannot be deleted if the associated host is already removed. **Workaround**: Unmount the primary storage first before deleting the host.
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 the CIDR to be the superset of Network CIDR for that VPC tier.
CLOUDSTACK-5262	Few of the snapshot creation from the root volume fails when concurrent snapshot creation is in progress.
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.

Issue ID	Description

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 lhe 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-5561, CLOUDSTACK-5814	[Hyper-V] Limited support for multiple NICs for VR running on Hyper-V hosts: APIs, such as createVlanIpRange will not work. NIC hot plug-in does not work if public IP is acquired from a different VLAN.
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.