Citrix CloudPlatform (powered by Apache CloudStack) 4.2.1-6 Maintenance Release Notes

Revised July 17, 2014 02:00 pm IST

Citrix CloudPlatform (powered by Apache CloudStack) 4.2.1-6 Maintenance Release Notes
Revised July 17, 2014 02:00 pm IST

Release notes for Citrix CloudPlatform version 4.2.1-6 Maintenance Release.

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 4.2.1-6 Maintenance Release. Most earlier OS and hypervisor versions are also still supported for use with 4.2.1-6 Maintenance Release For a complete list, see the System Requirements section of the CloudPlatform 4.2.1-6 Maintenance Release Installation Guide.

2.1. Supported OS Versions for Management Server

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

2.2. Supported Hypervisor Versions

The following hypervisors are supported:

- XenServer versions 5.6 SP2, 6.0, 6.0.2, 6.1, and 6.2
- KVM versions 5.5, 6.6, 5.7, 6.1, and 6.3
- VMware versions 4.1, 5.0.1 Update B, 5.0, and 5.1 Update 2
- 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 VPX and MPX versions 9.3 and 10.e
- Netscaler SDX version 9.3
- SRX (Model srx100b) versions 10.3 or higher
- F5 10.1.0 (Build 3341.1084)

2.4. Supported Browsers

- Internet Explorer versions 8 and 9

- Firefox version 25
- Google Chrome versions 17 and 20.0.1132.47m
- Safari 5

Upgrade Instructions

3.1. Upgrading from 4.2.x-x to 4.2.1-6

Perform the following to upgrade from version 4.2.x-x to version 4.2.1-6.

1. Download the latest System VM templates:

   The System VM templates includes fixes for the OpenSSL vulnerability issues reported in *http://support.citrix.com/article/CTX140876*.

Hypervisor	Description
XenServer	Name: systemvm-xenserver-4.2.1-b Description: systemvm-xenserver-4.2.1-b URL (if using 32-bit system VM template): *http://download.cloud.com/templates/4.2/systemvmtemplate-2014-06-17-master-xen.vhd.bz2* URL (if using 64-bit system VM template): *http://download.cloud.com/templates/4.2/64bit/systemvmtemplate64-2014-06-23-master-xen.vhd.bz2* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the XenServer zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit and 64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.2.1-b Description: systemvm-kvm-4.2.1-b URL (if using 32-bit system VM template): *http://download.cloud.com/templates/4.2/systemvmtemplate-2014-06-17-master-kvm.qcow2.bz2* URL (if using 64-bit system VM template): *http://download.cloud.com/templates/4.2/64bit/systemvmtemplate64-2014-06-23-master-kvm.qcow2.bz2*

Hypervisor	Description
	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-4.2.1-b Description: systemvm-vmware-4.2.1-b URL (if using 32-bit system VM template on earlier VMware version): *http://download.cloud.com/templates/4.2/systemvmtemplate-2014-06-17-master-vmware.ova* URL (if using 64-bit system VM template): *http://download.cloud.com/templates/4.2/64bit/systemvmtemplate64-2014-06-23-master-vmware.ova* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running VMware, choose All Zones to make the template available in all the VMware zones. Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

2. By using the prepareTemplate API, download the latest System VM to all the primary storages.
3. Check whether you already have the templates given at *http://support.citrix.com/article/CTX200024*.

The article include the necessary Python scripts to update the version format entires to x.x.x.x in the database to successfully perform the SystemVM upgrade. If you are not using the tempates, follow the instructions:

The systemVM template upgrade considers only the first 3 digits in the release number, and therefore the template versions are considred the same for 4.2.0.0 and 4.2.0.1, which is incorrect. To make the necessary database changes to accept the four digit version format, x.x.x.x, run the Python script as given below.

a. Download the Python script from *http://support.citrix.com/article/CTX200024*.

b. Stop all the Management Servers.

c. Take a backup of the database.

d. Execute the following python script on the Management Servers to update DB entries:

```
# python sys-tmpl-upgrade-4.2.1.py -i <db host name/ip> -u <db user name> -p <db
password>
```

e. Start all the Management Servers.

f. In the CloudPlatform UI, stop and start all the SSVM.

4. (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 4.2.1-6 RHEL 6.3 binaries from *https://www.citrix.com/English/ss/downloads/*

   b. Extract the binaries:

```
# cd /root
# tar xvf CloudPlatform-4.2.1-6-rhel6.3.tar.gz
```

   c. Create a CloudPlatform 4.2.1-6 qemu repo:

```
# cd CloudPlatform-4.2.1-6-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-4.2.1-6-rhel6.3/6.3
enabled=1
gpgcheck=0
```

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

```
yum upgrade
```

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

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

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

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

7. 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
```

8. (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
```

9. Download CloudPlatform 4.2.1 onto the management server host where it will run. Get the software from the following link:

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

   You need a *My Citrix Account*[1].

10. Upgrade the CloudPlatform packages. You should have a file in the form of “CloudPlatform-4.2.1-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-4.2.1-N-OSVERSION.tar.gz
# cd CloudPlatform-4.2.1-N-OSVERSION
# ./install.sh
```

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

11. Choose "U" to upgrade the package

```
>U
```

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

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

12. 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 4.2.1.

Note

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

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

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

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

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

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

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

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

13. Repeat steps *8* - *12* on each management server node.

14. 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.

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

```
# service cloudstack-usage 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 4.2.1-6.tgz download to the host, untar it, and change to the resulting directory.

    b. Stop the running agent.

```
# service cloudstack-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. (VMware only) Log in to the CloudPlatform UI.
19. Destroy both the Secondary Storage VM (SSVM) and Console Proxy VM (CPVM).
20. (VMware) Run the following script to destroy and re-create all remaining System VMs.

    a. Run the script once on one management server. Substitute your own IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the "-n" and "-v" arguments. For example:

    ```
    # nohup cloudstack-sysvmadm -d 192.168.1.5 -u cloud -p password -n -v > sysvm.log
     2>&1 &
    ```

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

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

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

    The content should be like the following:

    ```
    nohup: ignoring input
    Restarting 4 networks...
    Done restarting networks.
    Restarting 2 vpcs...
    INFO: Restarting vpc with id 2
    INFO: Restarting vpc with id 1
    INFO: Successfully restarted vpc with id 1
    INFO: Successfully restarted vpc with id 2
    Done restarting vpcs.
    ```

21. (XenServer or KVM) Run the following script to stop, then start, all System VMs including Secondary Storage VMs, Console Proxy VMs, and virtual routers.

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

    For example:

    ```
    # nohup cloudstack-sysvmadm -d 192.168.1.5 -u cloud -p password -a > sysvm.log 2>&1 &
    ```

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

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

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

The content should be like the following:

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

22. (XenServer only) If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudPlatform 4.2.1 and apply any required hotfixes. Instructions for upgrading XenServer software and applying hotfixes can be found in *Section 3.7, “Upgrading and Hotfixing XenServer Hypervisor Hosts”*.

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

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

b. Set vmware.use.dvswitch to true.

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

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

For example: dvSwitch18,,vmwaredvs

VLANID is optional.

d. Stop the Management server.

e. Start the Management server.

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

Post Upgrade Tasks

Consider the following:

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

- (XenServer) A cluster-level global parameter, *xen.vm.vcpu.max*, has been added to configure the number of non-Windows VMs in a cluster. After upgrade, the parameter takes the default value of 16. However, you can change the default value by using the Global Settings or Cluster Settings tab in the UI if you manually apply the following database schema:

```
INSERT IGNORE INTO `cloud`.`configuration` VALUES ('Advanced', 'DEFAULT', 'management-
server',
'xen.vm.vcpu.max', '16', 'Maximum number of VCPUs that VM can get in XenServer.');
```

Warning

The schema change might break the future CloudPlatform upgrades. Therefore, back port the changes in 4.2.1 before upgrading.

- Manually update systemvm.iso as given in Section 3.5, “Updating SystemVM.ISO”.

  In the previous 4.x releases, the Management Server version stored in the database version table is in x.x.x format. For example, 4.2.0 and 4.2.0.1 are stored as 4.2.0 as only the first 3 digits are considered as release version. Therefore, because the Management Server version number is the same for both the releases, the latest systemvm.iso files are not pushed after upgrade. Therefore, you must manually push systemvm.iso after upgrade.

3.2. Upgrading from 3.0.x to 4.2.1-6

Perform the following to upgrade from version 3.0.5, 3.0.6, or 3.0.7 Patch E to version 4.2.1-6.

1. While running the 3.0.x system, log in to the UI as root administrator.
2. 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-4.2.1-b Description: systemvm-xenserver-4.2.1-b URL (if using 32-bit system VM template): *http://download.cloud.com/templates/4.2/systemvmtemplate-2014-06-17-master-xen.vhd.bz2* URL (if using 64-bit system VM template): *http://download.cloud.com/templates/4.2/64bit/systemvmtemplate64-2014-06-23-master-xen.vhd.bz2* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the XenServer zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit and 64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.2.1-b Description: systemvm-kvm-4.2.1-b URL (if using 32-bit system VM template): *http://download.cloud.com/templates/4.2/systemvmtemplate-2014-06-17-master-kvm.qcow2.bz2* URL (if using 64-bit system VM template): *http://download.cloud.com/templates/4.2/64bit/systemvmtemplate64-2014-06-23-master-kvm.qcow2.bz2* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running KVM, choose All Zones to make the template available in all the KVM zones. Hypervisor: KVM Format: QCOW2

Hypervisor	Description
	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-4.2.1-b Description: systemvm-vmware-4.2.1-b URL (if using 32-bit system VM template on earlier VMware version): *http://download.cloud.com/templates/4.2/systemvmtemplate-2014-06-17-master-vmware.ova* URL (if using 64-bit system VM template): *http://download.cloud.com/templates/4.2/64bit/systemvmtemplate64-2014-06-23-master-vmware.ova* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running VMware, choose All Zones to make the template available in all the VMware zones. Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

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.

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 4.2.1-6 RHEL 6.3 binaries from *https://www.citrix.com/English/ss/downloads/*

      Extract the binaries:

      ```
      # cd /root
      # tar xvf CloudPlatform-4.2.1-6-rhel6.3.tar.gz
      ```

   b. Create a CloudPlatform 4.2.1-6 qemu repo:

      ```
      # cd CloudPlatform-4.2.1-6-rhel6.3/6.3
      # createrepo
      ```

   c. 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-4.2.1-6-rhel6.3/6.3
      enabled=1
      gpgcheck=0
      ```

   d. 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 4.2.1 onto the management server host where it will run. Get the software from the following link:

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

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

9. Upgrade the CloudPlatform packages. You should have a file in the form of “CloudPlatform-4.2.1-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-4.2.1-N-OSVERSION.tar.gz
# cd CloudPlatform-4.2.1-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 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 4.2.1.

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)

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

```
# 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
```

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 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
```

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 4.2.1-6.tgz download to the host, untar it, and cd into the resulting directory.

b. Stop the running agent.

```
# service cloudstack-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
```

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. (VMware only) Log in to the CloudPlatform UI. Destroy both the Secondary Storage VM (SSVM) and Console Proxy VM (CPVM).

19. (VMware) Run the following script to destroy and re-create all remaining System VMs.

    a. Run the script once on one management server. Substitute your own IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the "-n" and "-v" arguments. For example:

    ```
    # nohup cloudstack-sysvmadm -d 192.168.1.5 -u cloud -p password -n -v > sysvm.log
     2>&1 &
    ```

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

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

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

    The content should be like the following:

    ```
    nohup: ignoring input
    Restarting 4 networks...
    Done restarting networks.
    Restarting 2 vpcs...
    INFO: Restarting vpc with id 2
    INFO: Restarting vpc with id 1
    INFO: Successfully restarted vpc with id 1
    INFO: Successfully restarted vpc with id 2
    Done restarting vpcs.
    ```

20. (XenServer or KVM) Run the following script to stop, then start, all System VMs including Secondary Storage VMs, Console Proxy VMs, and virtual routers.

    a. Run the script once on one management server. Substitute your own IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the "-a" argument. For example:

    ```
    # nohup cloudstack-sysvmadm -d 192.168.1.5 -u cloud -p password -a > sysvm.log 2>&1 &
    ```

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

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

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

The content should be like the following:

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

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 4.2.1-6 Mon April 21 15:10:04 PST 2014
```

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 4.2.1-6 Mon Feb 24 15:10:04 PST 2014
```

22. 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.

23. (XenServer only) If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudPlatform 4.2.1-6 and apply any required hotfixes. Instructions for

upgrading XenServer software and applying hotfixes can be found in *Section 3.7, "Upgrading and Hotfixing XenServer Hypervisor Hosts"*.

24. (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. Upgrading from 2.2.x to 4.2.1-6

Direct upgrade from 2.2.x to 4.2.1-6 is not supported. You must first upgrade to 4.2.1:

1. Upgrade to 4.2.1:

a. 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 4.2.1, any existing IP address usage records in the old format will no longer be available.

b. If you are using version 2.2.0 - 2.2.14, first upgrade to 2.2.16 by using the instructions in the *2.2.14 Release Notes*[3].

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 4.2.1.

c. 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.

d. 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-4.2.1-b

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

Hypervisor	Description
	Description: systemvm-xenserver-4.2.1-b URL (if using 32-bit system VM template): *http://download.cloud.com/templates/4.2/systemvmtemplate-2014-06-17-master-xen.vhd.bz2* URL (if using 64-bit system VM template): *http://download.cloud.com/templates/4.2/64bit/systemvmtemplate64-2014-06-23-master-xen.vhd.bz2* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running XenServer, choose All Zones to make the template available in all the XenServer zones. Hypervisor: XenServer Format: VHD OS Type: Debian GNU/Linux 7.0 (32-bit and 64-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no
KVM	Name: systemvm-kvm-4.2.1-b Description: systemvm-kvm-4.2.1-b URL (if using 32-bit system VM template): *http://download.cloud.com/templates/4.2/systemvmtemplate-2014-06-17-master-kvm.qcow2.bz2* URL (if using 64-bit system VM template): *http://download.cloud.com/templates/4.2/64bit/systemvmtemplate64-2014-06-23-master-kvm.qcow2.bz2* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running KVM, choose All Zones to make the template available in all the KVM zones. Hypervisor: KVM Format: QCOW2 OS Type: Debian GNU/Linux 7.0 (32-bit and 64-bit) (or the highest Debian release number available in the dropdown) Extractable: no

Hypervisor	Description
	Password Enabled: no Public: no Featured: no
VMware	Name: systemvm-vmware-4.2.1-b Description: systemvm-vmware-4.2.1-b URL (if using 32-bit system VM template on earlier VMware version): *http://download.cloud.com/templates/4.2/systemvmtemplate-2014-06-17-master-vmware.ova* URL (if using 64-bit system VM template): *http://download.cloud.com/templates/4.2/64bit/systemvmtemplate64-2014-06-23-master-vmware.ova* Zone: Choose the zone where this hypervisor is used. If your CloudPlatform deployment includes multiple zones running VMware, choose All Zones to make the template available in all the VMware zones. Hypervisor: VMware Format: OVA OS Type: Debian GNU/Linux 7.0 (32-bit) (or the highest Debian release number available in the dropdown) Extractable: no Password Enabled: no Public: no Featured: no

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.

e. (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 4.2.1-6 RHEL 6.x binaries from *https://www.citrix.com/English/ss/downloads/*.

   b. Extract the binaries:

```
# cd /root
# tar xvf CloudPlatform-4.2.1-6-rhel6.x.tar.gz
```

   c. Create a CloudPlatform 4.2.1 qemu repo:

```
# cd CloudPlatform-4.2.1-6-rhel6.x
# createrepo .
```

   d. Prepare the yum repo for upgrade. Edit the file /etc/yum.repos.d/rhel6x.repo. For example:

```
[upgrade]
name=rhel6x
baseurl=url-of-your-rhel6.x-repo
enabled=1
gpgcheck=0
[cloudstack]
name=cloudstack
baseurl=file:///root/CloudPlatform-4.2.1-6-rhel6.x/6.x
enabled=1
gpgcheck=0
```

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

```
yum upgrade
```

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

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

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

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

h. 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
```

i. (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
```

j. Download CloudPlatform 4.2.1-6 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].

k. Upgrade the CloudPlatform packages. You should have a file in the form of "CloudPlatform-4.2.1-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-4.2.1-N-OSVERSION.tar.gz
# cd CloudPlatform-4.2.1-N-OSVERSION
# ./install.sh
```

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

l. Choose "U" to upgrade the package.

```
> U
```

m. 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 4.2.1.

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
```

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

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
```

n. 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.

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

p. 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.

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

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

r. (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 4.2.1-6.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
```

s. 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.

t. (VMware only) Log in to the CloudPlatform UI. Destroy both the Secondary Storage VM (SSVM) and Console Proxy VM (CPVM).

u. (VMware) Run the following script to destroy and re-create all remaining System VMs.

   a. Run the script once on one management server. Substitute your own IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the "-n" and "-v" arguments. For example:

```
# nohup cloudstack-sysvmadm -d 192.168.1.5 -u cloud -p password -n -v > sysvm.log
 2>&1 &
```

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

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

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

   The content should be like the following:

```
nohup: ignoring input
Restarting 4 networks...
Done restarting networks.
Restarting 2 vpcs...
INFO: Restarting vpc with id 2
INFO: Restarting vpc with id 1
INFO: Successfully restarted vpc with id 1
INFO: Successfully restarted vpc with id 2
Done restarting vpcs.
```

v. (XenServer or KVM) Run the following script to stop, then start, all System VMs including Secondary Storage VMs, Console Proxy VMs, and virtual routers.

   a. Run the script once on one management server. Substitute your own IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the "-a" argument. For example:

```
# nohup cloudstack-sysvmadm -d 192.168.1.5 -u cloud -p password -a > sysvm.log
 2>&1 &
```

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

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

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

   The content should be like the following:

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

```
Done restarting router(s).
```

w. 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 4.2.1 Mon April 21 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 4.2.1 Fri April 18 15:10:04 PST 2012
```

x. (XenServer only) If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudPlatform 4.2.1 and apply any required hotfixes. Instructions for upgrading and applying hotfixes can be found in *Section 3.7, “Upgrading and Hotfixing XenServer Hypervisor Hosts”*.

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".

2. Upgrade from 4.2.1 to 4.2.1-6.

   For more information, see *Section 3.1, “Upgrading from 4.2.x-x to 4.2.1-6”*.

3.4. Upgrading from 2.1.x to 4.2.1-6

Direct upgrades from version 2.1.0 - 2.1.10 to 4.2.1-6 are not supported. CloudPlatform must first be upgraded to version 2.2.16, then to 4.2.1. From 4.2.1, you can upgrade to 4.2.1-6. For information on how to upgrade from 2.1.x to 2.2.16, see the CloudPlatform 2.2.14 Release Notes.

3.5. Upgrading 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 4.2.1.

1. Log in as root to the host or virtual machine running the Baremetal PXE server and DHCP server.
2. Download CloudPlatform 4.2.1 onto the PXE or DHCP server. Get the software from the following link:

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

   You need a *My Citrix Account*[5].
3. Upgrade the CloudPlatform packages. You should have a file in the form of “CloudPlatform-4.2.1-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-4.2.1-N-OSVERSION.tar.gz
   # cd CloudPlatform-4.2.1-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

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

```
>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
```

3.6. Updating SystemVM.ISO

- On CloudPlatform versions 3.0.5.x and 3.0.7.x **`systemvm.iso`** will get propagated automatically; therefore, no separate procedure is required.
- On CloudPlatform versions 4.2.1.x, perform the following based on the hypervisor that you use:
  - XenServer: No action is required.
  - KVM
    a. On the KVM host, stop the CloudPlatform agent.
    b. Upgrade the CloudPlatform agent.
    c. Restart the CloudPlatform agent.
    d. Stop and Start SystemVMs.
  - VMware
    a. Stop all the Management Servers.
    b. Remove the old **`systemvm<version>.iso`** file from the **`systemvm`** directory, **`\<secondary_storage_path>\systemvm\`**.

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

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

3.7. Upgrading and Hotfixing XenServer Hypervisor Hosts

In CloudPlatform 4.2.1, 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.

3.7.1. Upgrading to a New XenServer Version

To upgrade XenServer hosts when running CloudPlatform 4.2.1:

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

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

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

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

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.

3.7.2. 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 start
```

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: XS602E004.xsupdate, XS602E005.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).

About This New Release

CloudPlatform 4.2.1-6 Maintenance release mainly focuses on closing the issues around replacing the domain, realhostip.com, with custom defined domain name. This release includes no API changes.

4.1. What's New in 4.2.1-6 Maintenance Release

The CloudPlatform 4.2.1-6 Maintenance Release includes the following:

- Support for VMware 5.1 Update 2 and NFSv4
- Realhost IP changes
- SystemVM templates with fixes for the OpenSSL vulnerability issues reported in *http://support.citrix.com/article/CTX140876*.

4.1.1. Replacing Realhostip with Custom Domain

Prior to CloudPlatform version 4.2, the console viewing functionality for SystemVMs used a dynamic DNS service under the domain name realhostip.com. This domain name assists in providing SSL security to console sessions. The domain, realhostip.com, has been depreciated. CloudPlatform deployments prior to version 4.2 that have not been reconfigured to use a DNS domain other than realhostip.com for Console Proxy or Secondary Storage must make changes to for the SystemVMs to continue functioning. To use one SSL certificate across all the instances among different deployments, CloudPlatform provides a global parameter based mechanism. To achieve that you need the following:

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

Note

Self-signed certificates are not supported.

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

4.1.1.1. Prerequisites and Considerations

- Specify the same domain name in the following:
  - SSL certificates you upload

- *consoleproxy.url.domain*
- *secstorage.ssl.cert.domain*

4.1.1.2. Procedure

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

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

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

3. Once the Management Server and SystemVM agents are upgraded successfully, follow the instructions given in *Section 4.1.1.3, “Console Proxy”* and *Section 4.1.1.4, “Secondary Storage VM”*.

4. Restart the Management Server.

5. Update **systemvm.iso**.

   See *Section 3.6, “Updating SystemVM.ISO”*.

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

   See *Section 4.1.1.5.2, “Uploading Custom Certificates”*.

4.1.1.3. Console Proxy

For Console Proxy sessions, you can use the HTTPS with wildcard certificate mode. For this mode, you need to set the global parameter, *consoleproxy.url.domain*to different forms of IP address, which can later be resolved by your DNS server.

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

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

2. Set up your zone in your DNS server.

   If you are using BIND 9:

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

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

   For example, a range such as 55.66.77.100 to 55.66.77.200.

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

```
etc..

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

4. Update CloudPlatform with the new domain name:

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

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

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

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

Console Proxy Mode	Global Parameter Settings	Console Proxy URL
HTTPS with wildcard certificate	Set *consoleproxy.url.domain* to yourdomain.com	http://yourdomain.com/xxxxx Each public IP entered in CloudPlatform is converted to a DNS name, for example, 77.88.99.11 and maps to yourdomain.com/xxxxx, where xxxxx is the secure token. When the browser connects to this URL, it try to match to wildcard cert yourdomain.com. For more information on generating wildcard certificates, see the CloudPlatform Administrator Guide.

5. Restart the Management Server.

4.1.1.4. Secondary Storage VM

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

Note

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

4.1.1.5. Using Custom Certificates

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

4.1.1.5.1. Prerequisites

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

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

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

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

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

4.1.1.5.2. Uploading Custom Certificates

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

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

2. Before uploading the next certificate, ensure that all the SystemVM agents are up and running.

3. (optional) Upload the intermediate certificate by using the uploadCustomCertificate API. For example:

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

4. Using the CloudPlatform UI, upload the server certificate and private key:

   a. In the left navigation pane, click Infrastructure.

   b. Click SSL Certificate.

      The SSL Certificate window is displayed.

   c. In the SSL Certificate window, specify the following:

      - The server certificate.
      - Private key in PKCS#8 format.
      - DNS Domain suffix. For example, .yourdomain.com.

5. Click OK.

   If the certificate is successfully uploaded, you see the "Update SSL certificate succeeded" message.

6. Restart the SystemVMs for the changes to take effect.

7. To verify, perform the following:

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

4.1.2. Fixed Issues

Issue ID	Description
CS-20527	High availability works as expected in Dedicated Zone.

Issue ID	Description
CS-20481	VM Snapshot usage records as expected for a domain. The value is the total size of the volume snapshot chain of all the ROOT volumes in the primary storage.
CS-20460	[XenServer] VCPUs settings are corrected for Linux VMs.
CS-20108	The listUsers API with keyword parameter is fixed.
CS-20477	[VMware] Post upgrade, clusters can now be successfully added to a legacy Zone.
CS-20358	The global parameter, custom.diskoffering.size.max is now honored.
CS-20272	Usage service starts as expected after updating to java 1.7.
CS-20257	High Availability functionality works as expected when an uploded volume is attached to a VM.
CS-20251	Network Offerings can now be successfully created from the CloudPlatform UI.
CS-20247	SSVM continues to use NFSv3 by default for secondary storage. SSVM no longer defaults to use NFSv4.
CS-20186	Java memery loss no longer occurs on the Management Server.
CS-20174	A network with no VMs can now be deleted.
CS-20163	The listCapacity API shows all the types for zones.
CS-20157	[VMware] Snapshot no longer fails with the CreatedOnPrimary error.
CS-20151	The listnetworks API no longer fails with the Incorrect number exception.
CS-20147	Creating a VM by using jclouds works as expected.
CS-20099	The Domain administrator can now successfully delete other domain administrators under the same domain.
CS-20042	Resizing volume no longer reports incorrect size in the usage database.
CS-20026/ CS-20027	[KVM] Virtual NIC capacity has been improved on guest VMs.
CS-20019	A new global parameter, xen.vm.vcpu.max, has been introduced.
CS-19990	The listUsageRecords API works as expected after upgrade.
CS-19982	Network usage is now recorded correctly.

Issue ID	Description
CS-19980	Connection count for an IP has now been set to an higher value on the VR.
CS-19976	The metadata API is now accessable on the VMs after the upgrade.
CS-19971	Multiple VMs can now be stopped parallely with no errors.
CS-19960	A VM can now be deployed to multiple Advanced network with Security Groups.
CS-19958	The listUsageRecords API works as expected across domains.
CS-19945	[VMware] VM Sync no longer shows running VMs' in Stopped state on the host.
CS-19854	The security policy and firewall filter term are no longer removed When a VM with a Static NAT bound is destroyed.
CS-19776	Cleanup download URLs now refers to correct timestamp for volume store.
CS-19666	VMs can be created with multiple core CPUs.
CS-18728	Recopying templates to other zones now works as expected.
CS-19935	[VMware] VMs are now successfully started after a failed storage migration attempt.
CS-19814	[KVM] SSL timeout issue has been fixed after setting the value for direct.agent.load.size to 60. KVM hosts now suceessfully reconnect back to the Management Server.
CS-19805	SSL keystore reference inconsistencies are fixed now.
CS-19802	[KVM] VMs now start after upgrading to version 4.2.1-4.
CS-19799	Port forwarding rule no longer fails due to unplugged VIFs.
CS-19775	The show/hide cross zone check box in the Acquire IP dialog works as expected.
CS-19756	Domain admin or user can now register a template by using S3/Swift object store.
CS-19725	Multiple networks with the same VLAN ID cannot be created in a cluster.
CS-19721	Virtual host is now supported in EventBus.
CS-19720	SSL is now supported in EventBus.
CS-19620	VMs can now be deployed in a mixed IPv4/IPv6 network.
CS-19464	Guest NIC now is replugged to the VPC VR upon restarting the VPC VR.

Issue ID	Description
CS-19226	DNS resolution service provided by the VR for a shared network no longer allows DNS resolution by using the public IP address of the VR.
CS-18930	RHEL guests VMs are created under correct OS type.
CS-18869	Value of cpuallocated is no longer twice the expected value.
CS-18604	Secondary Storage server no longer attempts to mount incorrect Secondary Storage NAS.

4.1.3. 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-17509	VM deployment fails with the Unable to acquire lock on VMTemplateStoragePool error. **Workaround**: Increase the default value of *`storage.pool.max.waitseconds`* as per the performance of your storage device. In this case, copying templates took more than 60 minutes due to slow storage. Increasing the value of the global parameter to more than 60 minutes would solve the issue.
CS-18409	(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**: To bring up the hosts, manually restart cloud-agent on the KVM hosts.
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. Workaround: **Workaround**: Restart the VM.

Issue ID	Description
CS-18561	(VMware) After upgrading from 3.0.x to 4.2 and higher versions, restoring an 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-18605	Order of templates and ISOs are not honored by UI or API.
CS-18752	In a Basic zone, an API error is thrown when you click the Add guest network option.
CS-18789	The listAsyncJobs API does not parse *startdate* parameter for some timezones.
CS-19067, CS-19066	DeleteRemoteAccessVpnCmd does not disable remote VPN access on an IP address.
CS-19110	Async response from addAccountToProject doesn't contain useful information.
CS-19105	No check to prevent invalid IP getting assigned to virtual router.
CS-19164	Storage migration between cluster-wide and zone-wide storage does not work as expected.
CS-19177	Private interface of a external LB devices and guest VMs are on the same network.
CS-19248	Upgrading to 4.2 leave cloud-agent-scripts on system without getting removed.
CS-19639	Attaching a data disk to an existing RHEL 6.x VM created in CloudPlatform 4.2.1-3 on vSphere does not work as expected. **Workaround**: Workaround is applicable to all the RHEL 6.x VMs created from version 4.2.1-3 to the version with the fix for this defect. 1. Stop the VM in CloudPlatform.

Issue ID	Description
	2. Open the vSphere client or vSphere web client. 3. Edit the setting of the VM: a. Change the SCSI controller sub-type of each SCSI controller from VMware Paravirtual to LsiLogic Parallel. b. Click OK to save the SCSI controller type changes. 4. Start the VM.
CS-19707	[VMware] Legacy Windows VMs cannot be restarted after attaching a DATA volume. This issue is observed only when the value for vmware.root.disk.controller is changed from ide to osdefault, which in turn results in losing the previous controller information. **Workaround**: 1. Set root.vmware.disk.controller value to ide. 2. Stop and start the Management server. 3. Start the failed VMs.
CS-19882	VMs are not deployed with 64-bit SSVM template of size 256 MB. **Workaround**: Scale SSVM memory to 512 MB. To achieve this, create a new System offering for SSVM with a size of 512 MB, then upgrade the existing SSVM offering to the new one.
CS-19885	[Realhostip] Certificates uploaded in 4.x versions without realhostip-related fixes fail after upgrading to a version with those defect fixes. **Workaround**: After the upgrade, upload the certificate again in the correct order with supplying all the parameters.
CS-19895	[Realhostip] The certificate for a custom domain can't be reverted after it's uploaded. To use the realhostip domain, upload the realhostip certificate and key again.
CS-20498	SSVMs of default size 256 MB cannot be created from the 64-bit VMware template. **Workaround**:

Issue ID	Description
	1. Update the *service_offering* table in the database. Set the value of *ram_size* to 512 for row. Set the value for *vm_type* to secondarystoragevm and default_use to 1. 2. Stop and start SSVM. Restarting System VM does not apply any changes to the VM settings; therefore, you must stop and start SSVM for the updated memory value to take effect.
CLOUDSTACK-1717	Local region entry that gets added by default should not include "/api" for its end_point. Also the endpoint should have the actual hostname instead of localhost.
CLOUDSTACK-1960	The euro symbol € does not work while accessing the guest virtual machine consoles on a UK keyboard by using console proxy.
CLOUDSTACK-1964	In Simplified Chinese, some combination keys used to switch IME cannot work well. **Workaround**: For "Ctrl+Shift" and "Ctrl+Space", click the input style of IME to select the input style and switch keyboard layout. For "Ctrl+Dot", click the “Chinese/Western Punctuation (Ctrl +.)” in the IME Toolbar to switch the punctuation between full-width and half-width.
CLOUDSTACK-1986	The Japanese keyboard keys ¥_,\ |, Muhenkan, Henkan, and Hiragana/Katakana are not working even after possible key translations tried. **Workaround**: For keys: | _ Set the console proxy keyboard layout to "Standard (US) Keyboard". Add English Keyboard layout to the Japanese guest VM from "Regional Setting" option from Control Panel (in case of Windows). Set the Japanese guest OS keyboard layout to "EN". Try the keyboard keys | _ using Japanese keyboard in localized environment. For Muhenkan key: You can use F6, F7 and F8 instead of the Muhenkan key. F6 key converts the string into Hiragana. F7 key converts the string into Katakana. F8 key converts the string into Hankaku-Katakana. Muhenkan keys toggles the string Hiragana, Katakana and Hankaku-Katakana.

Issue ID	Description
	Henkan key: You can use space bar (key) instead of the Henkan key. Hiragana/Katakana key: We have to use IME menu below to change IME input mode in case the Hiragana/Katakana key is unavailable.
CLOUDSTACK-2112	VM will go into stopped state after live migration failed during a scale up VMs operation. Need to be manually restarted.
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 runninng in KVM Hypervisor.
CLOUDSTACK-3212	Default guest network can now have multiple subnets per VLAN, but the IP range list page does not display the netmask and gateway for each subnet. **Workaround**: Use the API listVlanIPRanges to get the complete details.
CLOUDSTACK-3317	Management and storage network traffic cannot be configured to use VMware Distributed vSwitch (DVS). Continue to use standard vSwitch.
CLOUDSTACK-3466	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://*

Issue ID	Description
	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.
CLOUDSTACK-4402	Cannot delete primary storage 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

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

Issue ID	Description
	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. 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.

4.2. API Changes in 4.2.1-6 Maintenance Release

No API changes are introduced in 4.2.1-6 Maintenance Release.