Apache CloudStack

Apache CloudStack 4.0.1-incubating Release Notes

Revised December 15, 2012 05:49 UTC

cloudstack
open source cloud computing

Apache CloudStack

Apache CloudStack Apache CloudStack 4.0.1-incubating Release Notes
Revised December 15, 2012 05:49 UTC

Author   Apache CloudStack

Apache CloudStack is an effort undergoing incubation at The Apache Software Foundation (ASF).

Incubation is required of all newly accepted projects until a further review indicates that the infrastructure, communications, and decision making process have stabilized in a manner consistent with other successful ASF projects. While incubation status is not necessarily a reflection of the completeness or stability of the code, it does indicate that the project has yet to be fully endorsed by the ASF.

Release notes for the Apache CloudStack 4.0.1-incubating release.

Submitting Feedback and Getting Help

The Apache CloudStack project has mailing lists for users and developers. These are the official channels of communication for the project and are the best way to get answers about using and contributing to CloudStack. It's a good idea to subscribe to the cloudstack-users mailing list if you've deployed or are deploying CloudStack into production, and even for test deployments.

The CloudStack developer's mailing list (cloudstack-dev) is for discussions about CloudStack development, and is the best list for discussing possible bugs in CloudStack. Anyone contributing to CloudStack should be on this mailing list.

You can also report bugs in CloudStack using the *Apache Defect Tracking System*[1].

To posts to the lists, you'll need to be subscribed. See the *CloudStack Web site*[2] for instructions.

---

[1] https://issues.apache.org/jira/secure/CreateIssue!default.jspa

[2] http://incubator.apache.org/cloudstack/mailing-lists.html

Upgrade Instructions

2.1. Upgrade from 4.0.0-incubating to 4.0.1-incubating

Perform the following to upgrade from version 4.0.0-incubating to version 4.0.1 incubating. Note that some of the steps here are only required if you're using a specific hypervisor. The steps that are hypervisor-specific are called out with a note.

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

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

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

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

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

    In the following commands, it is assumed that you have set the root password on the database, which is a CloudStack recommended best practice. Substitute your own MySQL root password.

    ```
    # mysqldump -u root -pmysql_password cloud > cloudstack_backup.dmp
    # mysqldump -u root -pmysql_password cloud_usage > usage_backup.dmp
    ```

4. Either build RPM/DEB packages as detailed in the Installation Guide, or use one of the community provided yum/apt repositories to gain access to the CloudStack binaries.

5. After you have configured an appropriate yum or apt repository, you may execute the one of the following commands as appropriate for your environment in order to upgrade CloudStack:

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

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

    You will, of course, have to agree to the changes suggested by Yum or APT.

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

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

    ```
    # service cloud-management start
    ```

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

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

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

   ```
   # service cloud-usage start
   ```

8.
> **Note**
>
> Additional steps are required for each KVM host. These steps will not affect running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.

   a. Configure a yum or apt respository containing the CloudStack packages as outlined in the Installation Guide.

   b. Stop the running agent.

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

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

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

      ```
      # apt-get update
      ```

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

   d. Start the agent.

      ```
      # service cloud-agent start
      ```

   e. Edit **/etc/cloud/agent/agent.properties** to change the resource parameter from "com.cloud.agent.resource.computing.LibvirtComputingResource" to "com.cloud.hypervisor.kvm.resource.LibvirtComputingResource".

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

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

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

Do not proceed to the next step until the hosts show in Up state.

2.2. Upgrade from 3.0.2 to 4.0.1-incubating

Perform the following to upgrade from version 3.0.2 to version 4.0.1-incubating. Note that some of the steps here are only required if you're using a specific hypervisor. The steps that are hypervisor-specific are called out with a note.

1. Ensure that you query your IP address usage records and process them or make a backup. During the upgrade you will lose the old IP address usage records.

   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. > **Note**
   >
   > The following upgrade instructions apply only if you're using VMware hosts. If you're not using VMware hosts, skip this step and move on to step 3: stopping all usage servers.

   In each zone that includes VMware hosts, you need to add a new system VM template.

   a. While running the existing 3.0.2 system, log in to the UI as root administrator.

   b. In the left navigation bar, click Templates.

   c. In Select view, click Templates.

   d. Click Register template.

      The Register template dialog box is displayed.

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

Field	Value
Name	systemvm-vmware-3.0.0
Description	systemvm-vmware-3.0.0

Field	Value
URL	http://download.cloud.com/templates/burbank/burbank-systemvm-08012012.ova
Zone	Choose the zone where this hypervisor is used
Hypervisor	VMware
Format	OVA
OS Type	Debian GNU/Linux 5.0 (32-bit)
Extractable	no
Password Enabled	no
Public	no
Featured	no

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

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

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

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

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

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

   In the following commands, it is assumed that you have set the root password on the database, which is a CloudStack recommended best practice. Substitute your own MySQL root password.

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

6. Either build RPM/DEB packages as detailed in the Installation Guide, or use one of the community provided yum/apt repositories to gain access to the CloudStack binaries.

7. After you have configured an appropriate yum or apt repository, you may execute the one of the following commands as appropriate for your environment in order to upgrade CloudStack:

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

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

   You will, of course, have to agree to the changes suggested by Yum or APT.

> **Note**
>
> If the upgrade output includes a message similar to the following, then some custom content was found in your old components.xml, and you need to merge the two files:
>
> ```
> warning: /etc/cloud/management/components.xml created as /etc/cloud/management/
> components.xml.rpmnew
> ```
>
> Instructions follow in the next step.

8. If you have made changes to your copy of **/etc/cloud/management/components.xml** the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 4.0.1-incubating.

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

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

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

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

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

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

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

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

   ```
   # service cloud-management start
   ```

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

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

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

    ```
    # service cloud-usage start
    ```

11.
> **Note**
>
> Additional steps are required for each KVM host. These steps will not affect running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.

    a. Configure a yum or apt respository containing the CloudStack packages as outlined in the Installation Guide.

    b. Stop the running agent.

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

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

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

       ```
       # apt-get update
       ```

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

    d. Start the agent.

       ```
       # service cloud-agent start
       ```

    e. Edit **/etc/cloud/agent/agent.properties** to change the resource parameter from "com.cloud.agent.resource.computing.LibvirtComputingResource" to "com.cloud.hypervisor.kvm.resource.LibvirtComputingResource".

    f. Start the cloud agent and cloud management services.

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

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

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

Do not proceed to the next step until the hosts show in Up state.

13. If you are upgrading from 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 cloud-sysvmadm script at the end of the upgrade procedure. For information about how to set this parameter, see "Setting Global Configuration Parameters" in the Installation Guide.

    b. Restart the Management Server.

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

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

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

    # tail -f sysvm.log
    ```

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

15. If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudStack 4.0.1-incubating. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudStack 4.0.1-incubating Installation Guide.

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

    a. Disconnect the XenServer cluster from CloudStack.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

`# xe vm-list`

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

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

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

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

```
# xe host-list
```

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

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

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

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

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

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

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

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

- Extract the file:

```
# tar xf xenserver-cloud-supp.tgz
```

- Run the following script:

```
# xe-install-supplemental-pack xenserver-cloud-supp.iso
```

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

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

i. Reboot this XenServer host.

j. Run the following:

```
/opt/xensource/bin/setupxenserver.sh
```
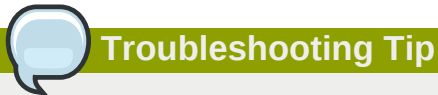
> **Note**
>
> If the message "mv: cannot stat `/etc/cron.daily/logrotate': No such file or directory" appears, you can safely ignore it.

k. Run the following:

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

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

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

2.3. Upgrade from 2.2.14 to 4.0.1-incubating

1. Ensure that you query your IPaddress usage records and process them; for example, issue invoices for any usage that you have not yet billed users for.

   Starting in 3.0.2, the usage record format for IP addresses is the same as the rest of the usage types. Instead of a single record with the assignment and release dates, separate records are generated per aggregation period with start and end dates. After upgrading to 4.0.1-incubating, any existing IP address usage records in the old format will no longer be available.

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

> ⚠ **KVM Hosts**
>
> If KVM hypervisor is used in your cloud, be sure you completed the step to insert a valid username and password into the host_details table on each KVM node as described in the 2.2.14 Release Notes. This step is critical, as the database will be encrypted after the upgrade to 4.0.1-incubating.

3. While running the 2.2.14 system, log in to the UI as root administrator.

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

   a. In the left navigation bar, click Templates.

   b. In Select view, click Templates.

   c. Click Register template.

   The Register template dialog box is displayed.

   d. In the Register template dialog box, specify the following values depending on the hypervisor type (do not change these):

Hypervisor	Description
XenServer	Name: systemvm-xenserver-3.0.0
	Description: systemvm-xenserver-3.0.0
	URL: http://download.cloud.com/templates/acton/acton-systemvm-02062012.vhd.bz2
	Zone: Choose the zone where this hypervisor is used
	Hypervisor: XenServer
	Format: VHD
	OS Type: Debian GNU/Linux 5.0 (32-bit)
	Extractable: no
	Password Enabled: no
	Public: no
	Featured: no
KVM	Name: systemvm-kvm-3.0.0
	Description: systemvm-kvm-3.0.0
	URL: http://download.cloud.com/templates/acton/acton-systemvm-02062012.qcow2.bz2

Hypervisor	Description
	Zone: Choose the zone where this hypervisor is used
	Hypervisor: KVM
	Format: QCOW2
	OS Type: Debian GNU/Linux 5.0 (32-bit)
	Extractable: no
	Password Enabled: no
	Public: no
	Featured: no
VMware	Name: systemvm-vmware-3.0.0
	Description: systemvm-vmware-3.0.0
	URL: http://download.cloud.com/templates/burbank/burbank-systemvm-08012012.ova
	Zone: Choose the zone where this hypervisor is used
	Hypervisor: VMware
	Format: OVA
	OS Type: Debian GNU/Linux 5.0 (32-bit)
	Extractable: no
	Password Enabled: no
	Public: no
	Featured: no

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

6. **WARNING**: If you use more than one type of hypervisor in your cloud, be sure you have repeated these steps to download the system VM template for each hypervisor type. Otherwise, the upgrade will fail.

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

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

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

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

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

In the following commands, it is assumed that you have set the root password on the database, which is a CloudStack recommended best practice. Substitute your own MySQL root password.

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

10. Either build RPM/DEB packages as detailed in the Installation Guide, or use one of the community provided yum/apt repositories to gain access to the CloudStack binaries.

11. After you have configured an appropriate yum or apt repository, you may execute the one of the following commands as appropriate for your environment in order to upgrade CloudStack:

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

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

You will, of course, have to agree to the changes suggested by Yum or APT.

12. If you have made changes to your existing copy of the file components.xml in your previous-version CloudStack installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 4.0.1-incubating.

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

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

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

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

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

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

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

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

13. If you have made changes to your existing copy of the **/etc/cloud/management/ db.properties** file in your previous-version CloudStack installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 4.0.1-incubating.

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

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

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

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

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

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

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.

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

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

    • (Optional) For encryption_type, use file or web to indicate the technique used to pass in the database encryption password. Default: file.

    • (Optional) For management_server_key, substitute the default key that is used to encrypt confidential parameters in the properties file. Default: password. It is highly recommended that you replace this with a more secure value

    • (Optional) For database_key, substitute the default key that is used to encrypt confidential parameters in the CloudStack database. Default: password. It is highly recommended that you replace this with a more secure value.

15. Repeat steps 10 - 14 on every management server node. If you provided your own encryption key in step 14, use the same key on all other management servers.

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

    ```
    # service cloud-management start
    ```

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

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

```
# service cloud-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.

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

    b. Stop the running agent.

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

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

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

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

    d. Start the agent.

    ```
    # service cloud-agent start
    ```

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

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

    f. Start the cloud agent and cloud management services.

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

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

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

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

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

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

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

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

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

The content should be like the following:

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

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

The output should be like the following:

```
Cloudstack Release 4.0.1-incubating Mon Oct 9 15:10:04 PST 2012
```

ESXi

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

Run the following commands on the Management Server:

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

The output should be like the following:

```
Cloudstack Release 4.0.1-incubating Mon Oct 9 15:10:04 PST 2012
```

22. If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudStack 4.0.1-incubating. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudStack 4.0.1-incubating Installation Guide.

23. Apply the XenServer hotfix XS602E003 (and any other needed hotfixes) to XenServer v6.0.2 hypervisor hosts.

    a. Disconnect the XenServer cluster from CloudStack.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    ```
    # xe vm-list
    ```

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

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

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

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

```
# xe host-list
```

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

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

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

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

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

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

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

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

- Extract the file:

  ```
  # tar xf xenserver-cloud-supp.tgz
  ```

- Run the following script:

  ```
  # xe-install-supplemental-pack xenserver-cloud-supp.iso
  ```

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

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

i. Reboot this XenServer host.

j. Run the following:

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

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

k. Run the following:

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

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

Version 4.0.1-incubating

3.1. What's New in 4.0.1-incubating

Apache CloudStack 4.0.1-incubating is a bugfix release and includes no new features.

3.2. Issues Fixed in 4.0.1-incubating

The following issues have been fixed in 4.0.1-incubating:

Defect	Description
CLOUDSTACK-359[1]	PropagateResourceEventCommand failes in cluster configuration.
CLOUDSTACK-374[2]	When running cloud-setup-databases, it auto chooses the highest priority nic(lowest number ie: eth0).
CLOUDSTACK-389[3]	Install Guide: Section 4.5.5 (Prepare NFS Shares): Confusing statement about iSCSI
CLOUDSTACK-395[4]	Primary Storage and Secondary Storage sections missing sub-sections
CLOUDSTACK-415[5]	restartNetwork call causes VM to be unreachable when Nicira based SDN is used.
CLOUDSTACK-422[6]	XSL files missing license header.
CLOUDSTACK-426[7]	SetVPCStaticNatRules unimplemented for KVM.
CLOUDSTACK-448[8]	SSVM bootstrap failure on XenServer hosts with E3 CPU.
CLOUDSTACK-465[9]	French language file quotes are dropping javascript syntax errors.
CLOUDSTACK-473[10]	API Doc for uploadCustomCertificate doesn't explain how to use the optional parameters well.
CLOUDSTACK-480[11]	Installation Documentation error: Section 4.5.5.2 needs to mention nfs-kernel-server.
CLOUDSTACK-498[12]	Missing dependency in RPM of KVM Agent.
CLOUDSTACK-502[13]	VPC router needs to resolve its hostname.
CLOUDSTACK-505[14]	CloudStack logs the private key in plaintext.
CLOUDSTACK-507[15]	fix api docs for listSSHKeyPairs.

---

[1] https://issues.apache.org/jira/browse/CLOUDSTACK-359

[2] https://issues.apache.org/jira/browse/CLOUDSTACK-374

[3] https://issues.apache.org/jira/browse/CLOUDSTACK-389

[4] https://issues.apache.org/jira/browse/CLOUDSTACK-395

[5] https://issues.apache.org/jira/browse/CLOUDSTACK-415

[6] https://issues.apache.org/jira/browse/CLOUDSTACK-422

[7] https://issues.apache.org/jira/browse/CLOUDSTACK-426

[8] https://issues.apache.org/jira/browse/CLOUDSTACK-448

[9] https://issues.apache.org/jira/browse/CLOUDSTACK-465

[10] https://issues.apache.org/jira/browse/CLOUDSTACK-473

[11] https://issues.apache.org/jira/browse/CLOUDSTACK-480

[12] https://issues.apache.org/jira/browse/CLOUDSTACK-498

[13] https://issues.apache.org/jira/browse/CLOUDSTACK-502

[14] https://issues.apache.org/jira/browse/CLOUDSTACK-505

[15] https://issues.apache.org/jira/browse/CLOUDSTACK-507

Defect	Description
CLOUDSTACK-515[16]	NVP Installation.
CLOUDSTACK-536[17]	remove citrix cloudpatform from 4.0 build - CloudStack is ASF project.
CLOUDSTACK-560[18]	Usage server doesn't work in 4.0.0 due to missing db changes.
CLOUDSTACK-591[19]	Wrong vnet in iptables on KVM hypervisors after VM reboot.
CLOUDSTACK-622[20]	In the add primary storage dialog in the ui the RBD fields don't disappear when changing from RBD to another protocol.

3.3. Known Issues in 4.0.1-incubating

Issue ID	Description
CLOUDSTACK-301[21]	Nexus 1000v DVS integration is not functional This source code release includes some partial functionality to support the Cisco Nexus 1000v Distributed Virtual Switch within a VMware hypervisor environment. The functionality is not complete at this time.
CLOUDSTACK-368[22]	OVM - cannot create guest VM This source code release has regressed from the CloudStack 2.2.x code and is unable to support Oracle VM (OVM).
CLOUDSTACK-279[23]	Deleting a project fails when executed by the regular user. This works as expected for root/domain admin. To workaround, perform either of the following: • Use the account cleanup thread which will eventually complete the project deletion. • Execute the call as the root/domain admin on behalf of the regular user.

---

[16] https://issues.apache.org/jira/browse/CLOUDSTACK-515

[17] https://issues.apache.org/jira/browse/CLOUDSTACK-536

[18] https://issues.apache.org/jira/browse/CLOUDSTACK-560

[19] https://issues.apache.org/jira/browse/CLOUDSTACK-591

[20] https://issues.apache.org/jira/browse/CLOUDSTACK-622

[21] https://issues.apache.org/jira/browse/CLOUDSTACK-301

[22] https://issues.apache.org/jira/browse/CLOUDSTACK-368

[23] https://issues.apache.org/jira/browse/CLOUDSTACK-279

API Changes from 4.0.0-incubating to 4.0.1-incubating

4.1. New API Commands in 4.0.1-incubating

CloudStack 4.0.1-incubating is a bugfix release, and thus there are no new API commands.

4.2. Changed API Commands in 4.0.1-incubating

CloudStack 4.0.1-incubating is a bugfix release, and there are no changed API commands.