Apache CloudStack

Version 4.0.0-incubating Release Notes

Revised October 17, 2012 19:49 UTC

cloudstack

open source cloud computing

Apache CloudStack

Apache CloudStack Version 4.0.0-incubating Release Notes Revised October 17, 2012 19:49 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 4.0.0-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 3.0.2 to 4.0.0-incubating

Perform the following to upgrade from version 3.0.2 to version 4.0.0-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-3.0.5
Description	systemvm-vmware-3.0.5
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

Field	Value
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-*
```

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 4.0.0-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 4.0.0-incubating. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudStack 4.0.0-incubating Installation Guide.

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.

2.2. Upgrade from 2.2.14 to 4.0.0-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 4.0.0-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 4.0.0-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 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-3.0.5 Description: systemvm-vmware-3.0.5 URL: http://download.cloud.com/templates/burbank/burbank-systemvm-08012012.ova Zone: Choose the zone where this hypervisor is used Hypervisor: VMware Format: OVA

Hypervisor	Description
	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-*
```

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 4.0.0-incubating.

Note

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

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

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

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

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

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

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

   ```
   # vi /etc/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 4.0.0-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 4.0.0-incubating Mon Oct 9 15:10:04 PST 2012
```

ESXi

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

Run the following commands on the Management Server:

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

The output should be like the following:

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

22. If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudStack 4.0.0-incubating. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudStack 4.0.0-incubating Installation Guide.

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 4.0.0-incubating

3.1. What's New in 4.0.0-incubating

Apache CloudStack 4.0.0-incubating includes the following new features:

3.1.1. Inter-VLAN Routing

Inter-VLAN Routing is the capability to route network traffic between VLANs. This feature enables you to set up Virtual Private Clouds (VPC) that can hold multi-tier applications. These tiers are deployed on different VLANs that can communicate with each other. You can provision VLANs to the tiers your create, and VMs can be deployed on different tiers, such as Web, Application, or Database. The VLANs are connected to a virtual router, which facilitates communication between the VMs. In effect, you can segment VMs by means of VLANs into different networks that can host multi-tier applications. Such segmentation by means of VLANs logically separate application VMs for higher security and lower broadcasts, while remaining physically connected to the same device.

This feature is supported on XenServer and VMware hypervisors.

3.1.2. Site-to-Site VPN

A Site-to-Site VPN connection helps you establish a secure connection from an enterprise datacenter to the cloud infrastructure. This allows users to access the guest VMs by establishing a VPN connection to the virtual router of the account from a device in the datacenter of the enterprise. Having this facility eliminates the need to establish VPN connections to individual VMs.

The supported endpoints on the remote datacenters are:

- Cisco ISR with IOS 12.4 or later
- Juniper J-Series routers with JunOS 9.5 or later

3.1.3. Local Storage Support for Data Volumes

You can now create data volumes on local storage. The data volume is placed on the same XenServer host as the VM instance that is attached to the data volume. These local data volumes can be attached to virtual machines, detached, re-attached, and deleted just as with the other types of data volume. In earlier releases of CloudStack, only the root disk could be placed in local storage.

Local storage is ideal for scenarios where persistence of data volumes and HA is not required. Some of the benefits include reduced disk I/O latency and cost reduction from using inexpensive local disks.

In order for local volumes to be used, the feature must be enabled for the zone.

You can create a data disk offering for local storage. When a user creates a new VM, they can select this disk offering in order to cause the data disk volume to be placed in local storage.

You can not migrate a VM that has a volume in local storage to a different host, nor migrate the volume itself away to a different host. If you want to put a host into maintenance mode, you must first stop any VMs with local data volumes on that host.

Local storage support for volumes is available for XenServer, KVM, and VMware hypervisors.

3.1.4. Tags

A tag is a key-value pair that stores metadata about a resource in the cloud. Tags are useful for categorizing resources. For example, you can tag a user VM with a value that indicates the user's city of residence. In this case, the key would be "city" and the value might be "Toronto" or "Tokyo." You can then request CloudStack to find all resources that have a given tag; for example, VMs for users in a given city.

You can tag a user virtual machine, volume, snapshot, guest network, template, ISO, firewall rule, port forwarding rule, public IP address, security group, load balancer rule, project, VPC, network ACL, or static route. You can not tag a remote access VPN.

You can work with tags through the UI or through the new API commands createTags, deleteTags, and listTags. You can define multiple tags for each resource. There is no limit on the number of tags you can define. Each tag can be up to 255 characters long. Users can define tags on the resources they own, and administrators can define tags on any resources in the cloud.

A new optional input parameter, "tags," has been added to many of the list* API commands. The following example shows how to use this new parameter to find all the volumes having tag region=canada OR tag city=Toronto:

```
command=listVolumes
&listAll=true
&tags[0].key=region
&tags[0].value=canada
&tags[1].key=city
&tags[1].value=Toronto
```

The following API commands have the new "tags" input parameter:

- listVirtualMachines
- listVolumes
- listSnapshots
- listNetworks
- listTemplates
- listIsos
- listFirewallRules
- listPortForwardingRules
- listPublicIpAddresses
- listSecurityGroups
- listLoadBalancerRules
- listProjects
- listVPCs
- listNetworkACLs
- listStaticRoutes

3.1.5. AWS API Changes for Tags

Some changes have been made to the Amazon Web Services API compatibility support in order to accommodate the new tagging feature.

New APIs:

New API	Description
ec2-create-tags	Add tags to one or more resources.
ec2-delete-tags	Remove tags from one or more resources.
ec2-describe-tags	Show currently defined tags.

Changed APIs:

Changed API	Description
ec2-describe-images	Output now shows tags defined for each image.
ec2-describe-instances	Output now shows tags defined for each image. The following filters can now be passed in to limit the output result set: tag-key, tag-value and tag:key
ec2-describe-snapshots	Output now shows tags defined for each image. The following filters can now be passed in to limit the output result set: tag-key, tag-value and tag:key
ec2-describe-volumes	Output now shows tags defined for each image. The following filters can now be passed in to limit the output result set: tag-key, tag-value and tag:key

3.1.6. Secure Console Access on XenServer

With the addition of Secure Console feature, users can now securely access the VM consoles on the XenServer hypervisor. You can either SSH or use the View Console option in the Management Server to securely connect to the VMs on the XenServer host. The Management Server uses the xapi API to stream the VM consoles. However, there is no change in the way you can access the console of a VM. This feature is supported on XenServer 5.6 and 6.0 versions.

3.1.7. Stopped VM

This release supports creating VMs without starting them on the backend. You can determine whether the VM needs to be started as part of the VM deployment. A VM can be deployed in two ways: create and start a VM (the default method); create a VM and leave it in the stopped state.

A new request parameter, startVM, is introduced in the deployVm API to support the stopped VM feature. The possible values are:

- true - The VM starts as a part of the VM deployment
- false - The VM is left in stopped state at the end of the VM deployment

3.1.8. Uploading an Existing Volume to a Virtual Machine

Existing data can now be made accessible to a virtual machine. This is called uploading a volume to the VM. For example, this is useful to upload data from a local file system and attach it to a VM. Root administrators, domain administrators, and end users can all upload existing volumes to VMs. The upload is performed by using HTTP. The uploaded volume is placed in the zone's secondary storage.

This functionality is supported for the following hypervisors:

- Hypervisor : Disk Image Format
- XenServer : VHD
- VMware : OVA
- KVM : QCOW2

3.1.9. Dedicated High-Availability Hosts

One or more hosts can now be designated for use only by high-availability (HA) enabled VMs that are restarted due to a host failure. Setting up a pool of such dedicated HA hosts as the recovery destination for all HA-enabled VMs make it easier to determine which VMs are restarted as part of the high-availability function. You can designate a host as a dedicated-HA restart node only if the Dedicated HA Hosts feature is enabled by setting the appropriate global configuration parameter.

3.1.10. Support for Amazon Web Services API

This release supports Amazon Web Services APIs, including Elastic Compute Cloud (EC2) API. Fidelity with the EC2 API and the installation experience for this functionality are both enhanced. In prior releases, users were required to install a separate component called CloudBridge, in addition to installing the Management Server. For new installations of CloudStack 4.0.0-incubating, this software is installed automatically along with CloudStack and runs in a more closely integrated fashion. The feature is disabled by default, but can be easily enabled by setting the appropriate global configuration parameter and performing a few setup steps.

3.1.11. The Nicira NVP Plugin

The Nicira NVP plug-in allows CloudStack to use the Nicira solution for virtualized network as a provider for CloudStack networks and services. In CloudStack 4.0.0-incubating this plug-in supports the Connectivity service. This service is responsible for creating Layer 2 networks supporting the networks created by guests. When a tenant creates a new network, instead of a traditional VLAN, a logical network will be created by sending the appropriate calls to the Nicira NVP Controller. The plug-in has been tested with Nicira NVP versions 2.1.0, 2.2.0 and 2.2.1.

3.1.12. Support for CAStor Cluster

CloudStack 4.0.0-incubating supports using a CAStor cluster as the back-end storage system for a CloudStack S3 front-end. The CAStor back-end storage for CloudStack extends the existing storage classes and allows the storage configuration attribute to point to a CAStor cluster. This feature makes use of the CloudStack server's local disk to spool files before writing them to CAStor when handling the PUT operations. However, a file must be successfully written into the CAStor cluster prior to the return of a success code to the S3 client to ensure that the transaction outcome is correctly reported.

The S3 multipart file upload is not supported in this release. You are prompted with proper error message if a multipart upload is attempted.

3.1.13. Clustered Logical Volume Manager Support for KVM

This release adds Clustered Logical Volume Manager (CLVM) storage support for KVM hosts. With this support, you can use CLVM as primary storage.

The CLVM support for KVM allows root and data disks (primary storage) to reside on Linux logical volumes. The administrators are required to configure CLVM on the KVM hosts independent of CloudStack. When the volume groups are available, an administrator can simply add primary storage of type CLVM, providing the volume group name. Then CloudStack creates and manages logical volumes as needed.

CLVM also supports Snapshots. CloudStack creates an LVM snapshot, copy the applicable logical volume to the secondary storage in the qcow2 format, and then delete the LVM snapshot.

3.1.14. Rados Block Device Support for KVM

You can now use Rados Block Device (RBD) to run instances on Apache CloudStack 4.0.0-incubating. This can be done by adding a RBD pool as primary storage. Before using RBD, ensure that Qemu is compiled with RBD enabled, and the libvirt version is at least 0.10 with RBD enabled on the KVM host

Create a disk offering for RBD so that you can ensure that StoragePoolAllocator chooses the RBD pool to deploy instances.

3.2. Issues Fixed in 4.0.0-incubating

Many bugs include a defect number that reflects the bug number that was held in the bug tracker run by Citrix (bugs.cloudstack.org). The Apache CloudStack project now uses *Jira*[1] to manage its bugs, so some of the bugs that are referenced here may not be available to view. However, we are still including them for completeness.

Defect	Description
Many	vSphere 5.0 now has GA support. Formerly only Beta support was provided.
CS-16135	Creating volumes after upgrading from snapshot taken in 2.2.14 no longer deletes the snapshot physically from the secondary storage.
CS-16122	In a site-to-site VPN setup, alerts are generated when the VPC virtual router is rebooted with multiple vpn connections.
CS-16022	If host connection fails due to a database error, host now disconnects and the Managerment Server id is removed.
CS-16011	Name of network offering is no longer truncated due to too-narrow field width in Add Guest Network dialog box.
CS-15978	When the virtual router and its host go down, the high availability mechanism now works for the virtual router.
CS-15921	The 2.2.x security group script now accounts for the VMs created in the version 2.1 timeframe.
CS-15919	A level parameter is added to the listVolumes command; therefore queries return the response more quickly.
CS-15904	Upgrade from version 2.2.14 to CloudStack-3.0.5-0.2944-rhel5 works as expected. The upgrade script, /usr/share/cloud/setup/db/schema-2214to30-cleanup.sql, works as expected.

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

Defect	Description
CS-15879	The database upgrade from version 3.0.4 to 3.0.5 works as expected.
CS-15807	Network label for OVM now available in UI.
CS-15779	When the thumbnail is requested, the console session will not be terminated.
CS-15778	Fetching a VM thumbnail now gets a thumbnail of appropriate visual dimensions.
CS-15734	KVM Snapshots no longer shows incorrect disk usage.
CS-15733	The domainId parameter for the listNetworks command now lists the resources belonging to the domain specified.
CS-15676	Stopping the router no longer fails with the null pointer exception.
CS-15648	If creating a volume from a snapshot fails, the error is reported on the UI but the volume is stuck in the creating state.
CS-15646	createFirewallRule API no longer causes null pointer exception.
CS-15628	In a KVM host, the high availability mechanism no longer takes a long time to migrate VMs to another KVM host if there are multiple storage pools.
CS-15627	Metadata instance-id and vm-id for existing VMs stays the same after upgrade.
CS-15621	Solved difficulty with allocating disk volumes when running multiple VM deployment in parallel.
CS-15603	CloudStack now stop the VMs when destroyVM command is called.
CS-15586	Public Vlan for an account no longer fails if multiple physical networks are present.
CS-15582	The dns-name filter is now supported for ec2-describe-instances in the Amazon Web Services API compatibility commands. The filter maps to the name of a user VM.
CS-15503	An IP address which has static NAT rules can now be released. Subsequently, restarting this network after it was shutdown can succeed.
CS-15464	Can now delete static route whose state is set to Revoke.
CS-15443	Creating a firewall rule no longer fails with an internal server error.
CS-15398	Corrected technique for programming DNS on the user VMs.
CS-15356	Internal DNS 2 entry now correctly shown in UI.
CS-15335	The CloudBridge S3 Engine now connects to the database by using the deciphered password in the db.properties file.
CS-15318	UI now correctly prevents the user from stopping a VM that is in the Starting state.
CS-15307	Fixed Japanese localization of instance statuses in the Instances menu.
CS-15278	The deployment planner no longer takes long time to locate a suitable host to deploy VMs when large number of clusters are present.

Defect	Description
CS-15274	Creating a VLAN range using Zone ID without network ID now succeeds.
CS-15243	Now check to be sure source NAT and VPN have same provider.
CS-15232	Ensure that networks using external load balancer/firewall in 2.2.14 or earlier can properly upgrade.
CS-15200	No exception when trying to attach the same volume while attaching the first volume is in progress.
CS-15173	Additional cluster can no longer be added with same VSM IP address as another cluster.
CS-15167	AWS API calls now honor the admin account's ability to view or act on the resources owned by the regular users.
CS-15163	The minimum limit is not honored when there is not enough capacity to deploy all the VMs and the ec2-run-instances command with the -n >n1 -n2> option is used to deploy multiple VMs.
CS-15157	Can now add/enable service providers for multiple physical networks through the UI.
CS-15145	AWS API call ec2-register has better error handling for negative cases.
CS-15122	Filters now supported for AWS API call ec2-describe-availability-zones.
CS-15120	Actions column in UI of Volume page now shows action links.
CS-15099	Buttons no longer overlap text on Account Deletion confirmation page in UI.
CS-15095	Ensures you can not create a VM with a CPU frequency greater than the host CPU frequency.
CS-15094	CPU cap now set properly in VMware.
CS-15077	NullPointerException is no longer observed while executing the command to list the public IP in a basic zone created with the default shared NetScaler EIP and ELB network offering.
CS-15044	UI now provides option to view the list of instances which are part of the guest network.
CS-15026	UI in Deploy VM dialog now lists only templates or ISOs depending on which is selected in previous dialog.
CS-14989	In KVM, the Create Instance wizard now shows only templates from the current (KVM) zone.
CS-14986, CS-14985	Listing filters works as expected in the ec2-describe-volumes and ec2-describe-snapshots commands.
CS-14964	Automatically starting the Console Proxy no longer fails due to its missing volume on the primary storage
CS-14907	User is now correctly prevented from trying to download an uploaded volume which has not yet been moved to primary storage.
CS-14879	When a user VM is stopped or terminated, the static NAT associated with this VM is now disabled. This public IP address

Defect	Description
	is no longer owned by this account and can be associated to any other user VM.
CS-14854	Only the admin user can change the template permission to Public, so this option is removed from the UI for domain Admins and regular Users.
CS-14817	While checking if network has any external provider, CloudStack will consider all providers in the network.
CS-14796	When deploying a VM with ec2-run-instances, userdata is now encoded.
CS-14770	The API returns the keypair information when a VM is deployed with sshkey. This affects the API commands related to virtual machines (deployVirtualMachine, listVirtualMachines, ... *VirtualMachine), as well as the corresponding AWS APIs.
CS-14724	UI no longer displays the dropdown list of isolation method choices if sdn.ovs.controller is false.
CS-14345	Logout API returns XML header.
CS-14724	Host IPs now associated with appropriate IPs according to traffic type.
CS-14253	Can now delete and re-create port forwarding rule on same firewall.
CS-14724	UI no longer displays the dropdown list of isolation method choices if sdn.ovs.controller is false.
CS-14452	Data disk volumes are now automatically copied from one cluster to another.
CS-13539	Windows VM can get IP after reboot.
CS-13537	When user tries to delete a domain that contains sub-domains, an error message is now sent to convey the reason for the delete failure.
CS-13153	System VMs support HTTP proxy.
CS-12642	Added Close button to Select Project list view popup in UI.
CS-12510	Deleting and reinserting host_details no longer causes deadlocks.
CS-12407	F5 and Netscaler - when dedicated is selected, capacity field is disabled.
CS-12111	Email validation for edit user form.
CS-10928	Network read/write values now always positive numbers.
CS-15376, CS-15373	The AWS APIs (EC2 and S3) now listen on the 7080 port and send request to CloudStack on the 8080 port just as any other clients of CloudStack.
CS-13944	The CloudStack 2.2.x to 3.0.x database upgrade for multiple physical networks is now supported.
CS-15300	The admin accounts of a domain now honour the limits imposed on that domain just like the regular accounts do. A domain admin now is not allowed to create an unlimited number of instances, volumes, snapshots, and so on.

Defect	Description
CS-15396	The CloudStack database now contain the UUD information after the 2.2.14 to 3.0.4 upgrade.
CS-15450	Upgrade from 2.2.14 to 3.0.4 no longer fails on a VMware host.
CS-15449	Running cloudstack-aws-api-register no longer fails with the "User registration failed with error: [Errno 113] No route to host" error.
CS-15455	The iptable rules are configured to open the awsapi port (7080) as part of the installation.
CS-15429	While creating an instance with data volume, disk offering also is considered while checking the account limit on volume resources.
CS-15414	After the 2.2.14 to 3.0.4 upgrade, the value of the global parameter xen.guest.network.device is now decrypted before setting the traffic label.
CS-15382	During 2.2.14 to 3.0.4 upgrade, the hosts no longer go to the Alert state if destroyed networks existed with non-existent tags prior to upgrade.
CS-15323	CloudStack supports the following Citrix XenServer hotfixes: XS602E003, XS602E004, and XS602E005.
CS-15430	Create snapshot now fails if creating a snapshot exceeds the snapshot resource limit for a domain admin or a user account.
CS-14256	Virtual Router no longer remains in starting state for subdomain or user on a KVM 3.0.1 prerlease host on RHEL 6.2.
CS-7495	Implemented a variety of Xen management host improvements.
CS-8105	NFS v4 for primary storage now works as expected on KVM hosts.
CS-9989	The error messages returned during VM deployment failure will have much more details than before.
CS-12584	You can no longer add security groups not supported by the hypervisor in use.
CS-12705	When creating a Network offering by using SRX as the service provider for SourceNAT servcies, an option is given in the CloudStack UI now to set the source_nat type to "per Zone"/"per account".
CS-12782	Assigning a VM from Basic to Advanced zone no longer ignores the network ID. A warning message is displayed for VM movements across zones.
CS-12591	Broadcast Address on the Second Public IP NIC is now corrected.
CS-13272	When a user is deleted, all the associated properties, such as IPs and virtual routers, are now deleted.
CS-13377	Creating template from a root disk of a stopped instance now provides an option to make it a "Featured template".
CS-13500	Reaching the first guest VM by using its public IP from the second guest VM no longer fails.
CS-13853	The default gateway can no longer be 0.0.0.0 in the Secondary Storage VM (SSVM).

Defect	Description
CS-13863	The queryAsyncJobResult command in XML format now returns the correct UUIDs.
CS-13867	Corrected CSP xenserver-cloud-supp.tgz for XenServer 5.6 and 6.0.
CS-13904	Labels and values for the service offerings CPU and memory are now consistent.
CS-13998	The SSVM kernel panic issue is fixed on XenServer.
CS-14090	The issue is fixed where running the VMware snapshots randomly fails with the ArrayIndexOutOfBoundsException error.
CS-14021	The java.lang.OutOfMemoryError is fixed on the Management Server.
CS-14025	The Python Eggs are provided to easily package the test client for each branch of CloudStack.
CS-14068	Resetting the VM password through the CloudStack UI no longer causes any error.
CS-14156	The pod which has the administrator's virtual router is no longer selected while creating the virtual routers for guests.
CS-14182	The users can now delete their ISOs as normal users.
CS-14185	The listOSTypes API now filters out the types of operating system by using the keywords.
CS-14204	The cloud-setup-bonding.sh command no longer generates the "command not found" error.
CS-14214	The Specify VLAN option cannot be enabled now for an isolated Network offering with SourceNAT enabled.
CS-14234	Sending project invite email to an account now requires SMTP configured in CloudStack.
CS-14237	The garbage collector of the primary storage no longer fails when the first host in the cluster is not up.
CS-14241	Custom Volume Disk Offering is now matching the Global configuration value.
CS-14270	The listNetworks API no longer assumes that the broadcast type is always VLAN.
CS-14319	The internal name of the VM is no longer present in the error message that is displayed to a domain administrator.
CS-14321	The listVolumes API call now returns a valid value for the isExtractable parameter for the ISO-derived disk and data disk volumes.
CS-14323	Invalid API calls will now give valid response in json/xml format.
CS-14339	Custom Disk Size will now allow values larger than 100GB.
CS-14357	The ConsoleProxyLoadReportCommand is no longer fired continuously.
CS-14421	Fixed the issue of virtual router deployments. The DHCP entries can now be assigned to the router.

Defect	Description
CS-14555	Unzipped downloaded template MD5SUM will no longer override the zipped template MD5SUM in the database.
CS-14598	The complete screen of the running VM is now displayed in the console proxy.
CS-14600	Windows or Linux based consoles are no longer lost upon rebooting VMs.
CS-14784	Multiple subnets with the same VLAN now work as expected.
CS-13303, 14874, 13897, 13944, 14088, 14190	A variety of upgrade issues have been fixed in release 3.0.3.
CS-15080	Setting a private network on a VLAN for VMWare environment is now supported.
CS-15168	The console proxy now works as expected and no exception is shown in the log after upgrading from version 2.2.14 to 3.0.2.
CS-15172	Version 3.0.2 now accepts the valid public key.

3.3. Known Issues in 4.0.0-incubating

Issue ID	Description
CLOUDSTACK-301	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	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	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.
CS-16067	The command=listTags&key=city command does not work as expected. The command does not return tags for the resources of the account with the tag, city
CS-16063	The current values of volumes and snapshots are incorrect when using KVM as a host. To fix this, the database upgrade codes, volumes.size and snapshots.size, should be changed to show the virtual sizes.
CS-16058	Null pointer Exception while deleting the host after moving the host to maintenance state.

Issue ID	Description
CS-16045	Only the root administrator can handle the API keys. The domain administrators are not allowed to create, delete, or retrieve API keys for the users in their domain.
CS-16019	CIDR list in the Add VPN Customer Gateway dialog does not prompt the user that they can provide a comma separated CIDRs if multiple CIDRs have to be supplied.
CS-16015	Deleting a network is not supported when its network providers are disabled.
CS-16012	Unable to delete a zone in the UI because the necessary cleanup cannot be completed. When the hosts are removed, the expunge process fails to delete the volumes as no hosts are present to send the commands to. Therefore, the storage pool removal fails, and zone can't be cleaned and deleted.
CS-16011	Name of network offering might be truncated due to too-narrow field width in Add Guest Network dialog box.
CS-15789	Invalid global setting prevents management server to restart. For example, if you configure the "project.invite.timeout" parameter to "300" and attempt to restart management server, it fails without throwing a warning or setting the value to the default.
CS-15749	Restarting VPC is resulting in intermittent connection loss to the port forwarding and StaticNAT rules.
CS-15690	The IpAssoc command failed as a part of starting the virtual router, but the final start result is reported as succes.
CS-15672, CS-15635	The FQDN of the VM is not configured if it is deployed as a part of default shared network and isolated guest network (DefaultIsolatedNetworkOfferingWithSourceNatService).
CS-15634	The FQDN of a VM that is deployed as a part of both a shared network and default isolated guest network has the suffix of the shared network instead of the default isolated guest network.
CS-15576	Stopping a VM on XenServer creates a backlog of API commands. For example, the Attach volume calls become delayed while waiting for the stopVirtualMachine command to be executed.
CS-15569	Misleading error message in the exception when creating a StaticNAT rule fails in a VPC.
CS-15566	External device such as Netscaler is not supported in VPC.
CS-15557	Intermittent traffic loss in the VPN connection if Juniper is the remote router and the life time is 300 seconds.
CS-15361	Egress rules are not working in NetScaler loadbalancer.
CS-15163	The minimum limit is not honored when there is not enough capacity to deploy all the VMs and the ec2-run-instances command with the -n >n1 -n2> option is used to deploy multiple VMs.
CS-15105	The cloud-sysvmadm script does not work if the integration.api.port parameter is set to any port other than 8096.
CS-15092	Connecting to the guest VMs through SSH is extremely slow, and it results in connection timeout.

Issue ID	Description
CS-15037	Hairpin NAT is not supported when NetScaler is used for EIP.
CS-15009	The port_profile table will not be populated with port profile information. In this release, CloudStack directly connects to the VSM for all the port profile operations; therefore, no port profile information is cached.
CS-14939	Adding a VMware cluster is not supported when the Management Network is migrated to the Distributed Virtual Switch environment.
CS-14780	You are allowed to ping the elastic IP address of the VM even though no ingress rule is set that allows the ICMP protocol.
CS-14756	Installing KVM on RHEL 6.2 will result in unreliable network performance. Workaround: blacklist vhost-net. Edit /etc/modprobe.d/blacklist-kvm.conf and include vhost-net.
CS-14346	The UpdateVirtualMachine API call does not check whether the VM is stopped. Therefore, stop the VM manually before issuing this call.
CS-14303 (was 14537)	The IP addresses for a shared network are still being consumed even if no services are defined for that network.
CS-14296 (was 14530)	OVM: Network traffic labels are not supported.
CS-14291 (was 14523)	The EIP/ELB network offering for basic zones does not support multiple NetScalers.
CS-14275 (was 14506)	F5: Unable to properly remove a F5 device.
CS-14201 (was 14430)	VMWare: Template sizes are being reported different depending on whether the primary storage is using ISCSI or NFS.
CS-13758 (was 13963)	vSphere: template download from templates created off of the root volume does not work properly.
CS-13733 (was 13935)	vSphere: detaching an ISO from a restored VM instance fails.
CS-13682 (was 13883)	Multiple NetScalers are not supported in Basic Networking.
CS-13599 (was 13359)	Programming F5/NetScaler rules can be better optimized.
CS-13337 (was 13518)	Security Groups are not supported in Advanced Networking
CS-13173 (was 13336)	vSphere: cross cluster volume migration does not work properly.
CS-12714 (was 12840)	Capacity view is not available for pods or clusters.
CS-12624 (was 12741)	vSphere: maintenance mode will not live migrate system VM to another host.
CS-15476	The 2.2.14 to 4.0.0-incubating upgrade fails if multiple untagged physical networks exist before the upgrade.
CS-15407	After the 2.2.14 to 4.0.0-incubating upgrade, VLAN allocation on multiple physical networks does not happen as expected. To workaround this issue, follow the instructions given below: 1. Revert to your 2.2.14 setup. 2. Stop all the VMs with the isolated virtual networks in your cloud setup.

<table>
<tr><th>Issue ID</th><th>Description</th></tr>
<tr><td></td><td>

3. Run following query to find if any networks still have the NICs allocated:

    a. Check if any virtual guest networks have the NICs allocated:

    ```
    #SELECT DISTINCT op.id from `cloud`.`op_networks`
     op JOIN `cloud`.`networks` n on op.id=n.id WHERE
     nics_count != 0 AND guest_type = 'Virtual';
    ```

    b. If this returns any network IDs, then ensure the following:

        i. All the VMs are stopped.

        ii. No new VM is started.

        iii. Shutdown the Management Server.

    c. Remove the NICs count for the virtual network IDs returned in step (a), and set the NIC count to 0:

    ```
    UPDATE `cloud`.`op_networks` SET nics_count = 0
     WHERE id = enter id of virtual network
    ```

    d. Restart the Management Server, and wait for all the networks to shut down.

    Note

    Networks shutdown is determined by the network.gc.interval and network.gc.wait parameters.

4. Ensure that all the networks are shut down and all the guest VNETs are free.

5. Run the upgrade script.

    This allocates all your guest VNET ranges to the first physical network.

6. By using the updatePhysicalNetwork API, reconfigure the VNET ranges for each physical network as desired.

7. Start all the VMs.

</td></tr>
<tr><td>CS-14680</td><td>

CloudStack and LDAP user validation cannot happen simultaneously because the user password is hashed and stored in the database, and LDAP requires the passwords in plain text.

To work with the LDAP user, the MD5 hash should be disabled in the login process by commenting the following variable in

</td></tr>
</table>

Issue ID	Description
	sharedFunctions.js file available at /usr/share/cloud/management/webapps/client/scripts, and restart the cloud-management service. `var md5HashedLogin = false;` However, if md5HashedLogin is set to false, the end user can login with the LDAP credentials but not with the CloudStack user credentials.
CS-14346	The UpdateVirtualMachine API call does not check whether the VM is stopped. Therefore, stop the VM manually before issuing this call.
CS-15130	Data disk volumes are not automatically copied from one cluster to another.
CS-14780	You are allowed to ping the elastic IP address of the VM even though no ingress rule is set that allows the ICMP protocol.
CS-14939	Adding a VMware cluster is not supported when the Management Network is migrated to the Distributed Virtual Switch environment.
CS-15009	The port_profile table will not be populated with port profile information. In this release, CloudStack directly connects to the VSM for all the port profile operations; therefore, no port profile information is cached.
CS-15037	Hairpin NAT is not supported when NetScaler is used for EIP.
CS-15092	Connecting to the guest VMs through SSH is extremely slow, and it results in connection timeout.
CS-15105	The cloud-sysvmadm script does not work if the integration.api.port parameter is set to any port other than 8096.
CS-15163	The minimum limit is not honored when there is not enough capacity to deploy all the VMs and the ec2-run-instances command with the -n >n1 -n2> option is used to deploy multiple VMs.

Chapter 4.

API Changes from 3.0.2 to 4.0.0-incubating

4.1. New API Commands in 4.0.0-incubating

- createCounter (Adds metric counter)
- deleteCounter (Deletes a counter)
- listCounters (List the counters)
- createCondition (Creates a condition)
- deleteCondition (Removes a condition)
- listConditions (List Conditions for the specific user)
- createTags. Add tags to one or more resources. Example:

  ```
  command=createTags
  &resourceIds=1,10,12
  &resourceType=userVm
  &tags[0].key=region
  &tags[0].value=canada
  &tags[1].key=city
  &tags[1].value=Toronto
  ```

- deleteTags. Remove tags from one or more resources. Example:

  ```
  command=deleteTags
  &resourceIds=1,12
  &resourceType=Snapshot
  &tags[0].key=city
  ```

- listTags (Show currently defined resource tags)
- createVPC (Creates a VPC)
- listVPCs (Lists VPCs)
- deleteVPC (Deletes a VPC)
- updateVPC (Updates a VPC)
- restartVPC (Restarts a VPC)
- createVPCOffering (Creates VPC offering)
- updateVPCOffering (Updates VPC offering)
- deleteVPCOffering (Deletes VPC offering)
- listVPCOfferings (Lists VPC offerings)
- createPrivateGateway (Creates a private gateway)

- listPrivateGateways (List private gateways)
- deletePrivateGateway (Deletes a Private gateway)
- createNetworkACL (Creates a ACL rule the given network (the network has to belong to VPC))
- deleteNetworkACL (Deletes a Network ACL)
- listNetworkACLs (Lists all network ACLs)
- createStaticRoute (Creates a static route)
- deleteStaticRoute (Deletes a static route)
- listStaticRoutes (Lists all static routes)
- createVpnCustomerGateway (Creates site to site vpn customer gateway)
- createVpnGateway (Creates site to site vpn local gateway)
- createVpnConnection (Create site to site vpn connection)
- deleteVpnCustomerGateway (Delete site to site vpn customer gateway)
- deleteVpnGateway (Delete site to site vpn gateway)
- deleteVpnConnection (Delete site to site vpn connection)
- updateVpnCustomerGateway (Update site to site vpn customer gateway)
- resetVpnConnection (Reset site to site vpn connection)
- listVpnCustomerGateways (Lists site to site vpn customer gateways)
- listVpnGateways (Lists site 2 site vpn gateways)
- listVpnConnections (Lists site to site vpn connection gateways)
- markDefaultZoneForAccount (Marks a default zone for the current account)
- uploadVolume (Uploads a data disk)

4.2. Changed API Commands in 4.0.0-incubating

API Commands	Description
copyTemplate prepareTemplate registerTemplate updateTemplate createProject activateProject suspendProject	The commands in this list have a single new response parameter, and no other changes. New response parameter: tags(*)

API Commands	Description
updateProject listProjectAccounts createVolume migrateVolume attachVolume detachVolume uploadVolume createSecurityGroup registerIso copyIso updateIso createIpForwardingRule listIpForwardingRules createLoadBalancerRule updateLoadBalancerRule createSnapshot	**Note** Many other commands also have the new tags(*) parameter in addition to other changes; those commands are listed separately.
rebootVirtualMachine attachIso detachIso listLoadBalancerRuleInstances resetPasswordForVirtualMachine changeServiceForVirtualMachine recoverVirtualMachine startVirtualMachine migrateVirtualMachine deployVirtualMachine assignVirtualMachine updateVirtualMachine restoreVirtualMachine stopVirtualMachine	The commands in this list have two new response parameters, and no other changes. New response parameters: keypair, tags(*)

API Commands	Description
destroyVirtualMachine	
listSecurityGroups listFirewallRules listPortForwardingRules listSnapshots listIsos listProjects listTemplates listLoadBalancerRules	The commands in this list have the following new parameters, and no other changes. New request parameter: tags (optional) New response parameter: tags(*)
listF5LoadBalancerNetworks listNetscalerLoadBalancerNetworks listSrxFirewallNetworks updateNetwork	The commands in this list have three new response parameters, and no other changes. New response parameters: canusefordeploy, vpcid, tags(*)
createZone updateZone	The commands in this list have the following new parameters, and no other changes. New request parameter: localstorageenabled (optional) New response parameter: localstorageenabled
listZones	New response parameter: localstorageenabled
rebootRouter changeServiceForRouter startRouter destroyRouter stopRouter	The commands in this list have two new response parameters, and no other changes. New response parameters: vpcid, nic(*)
updateAccount disableAccount listAccounts markDefaultZoneForAccount enableAccount	The commands in this list have three new response parameters, and no other changes. New response parameters: vpcavailable, vpclimit, vpctotal
listRouters	New request parameters: forvpc (optional), vpcid (optional) New response parameters: vpcid, nic(*)
listNetworkOfferings	New request parameters: forvpc (optional)

API Commands	Description
	New response parameters: forvpc
listVolumes	New request parameters: details (optional), tags (optional) New response parameters: tags(*)
addTrafficMonitor	New request parameters: excludezones (optional), includezones (optional)
createNetwork	New request parameters: vpcid (optional) New response parameters: canusefordeploy, vpcid, tags(*)
listPublicIpAddresses	New request parameters: tags (optional), vpcid (optional) New response parameters: vpcid, tags(*)
listNetworks	New request parameters: canusefordeploy (optional), forvpc (optional), tags (optional), vpcid (optional) New response parameters: canusefordeploy, vpcid, tags(*)
restartNetwork	New response parameters: vpcid, tags(*)
enableStaticNat	New request parameter: networkid (optional)
createDiskOffering	New request parameter: storagetype (optional) New response parameter: storagetype
listDiskOfferings	New response parameter: storagetype
updateDiskOffering	New response parameter: storagetype
createFirewallRule	Changed request parameters: ipaddressid (old version - optional, new version - required) New response parameter: tags(*)
listVirtualMachines	New request parameters: isoid (optional), tags (optional), templateid (optional) New response parameters: keypair, tags(*)
updateStorageNetworkIpRange	New response parameters: id, endip, gateway, netmask, networkid, podid, startip, vlan, zoneid
reconnectHost	A new response parameter is added: hahost.
addCluster	The following request parameters are added: • vsmipaddress (optional) • vsmpassword (optional) • vsmusername (optional) The following parameter is made mandatory: podid

API Commands	Description
listVolumes	A new response parameter is added: status
migrateVolume	A new response parameter is added: status
prepareHostForMaintenance	A new response parameter is added: hahost.
addSecondaryStorage	A new response parameter is added: hahost.
enableAccount	A new response parameter is added: defaultzoneid
attachVolume	A new response parameter is added: status
cancelHostMaintenance	A new response parameter is added: hahost
addSwift	A new response parameter is added: hahost
listSwifts	A new response parameter is added: hahost
listExternalLoadBalancers	A new response parameter is added: hahost
createVolume	A new response parameter is added: status
listCapabilities	A new response parameter is added: customdiskofferingmaxsize
disableAccount	A new response parameter is added: defaultzoneid
deployVirtualMachine	A new request parameter is added: startvm (optional)
deleteStoragePool	A new request parameter is added: forced (optional)
updateAccount	A new response parameter is added: defaultzoneid
addHost	A new response parameter is added: hahost
updateHost	A new response parameter is added: hahost
detachVolume	A new response parameter is added: status
listAccounts	A new response parameter is added: defaultzoneid
listHosts	A new response parameter is added: hahost A new request parameter is added: hahost (optional)