

Citrix CloudPlatform (powered by Apache CloudStack) Version 3.0.5 Release Notes

Revised November 9, 2012 12:45 pm Pacific

WARNING: Security Vulnerability Reported.
Immediate Action Advised. See [Security Vulnerability](#).



Citrix CloudPlatform (powered by Apache CloudStack) Version 3.0.5 Release Notes

Revised November 9, 2012 12:45 pm Pacific: **WARNING: Security Vulnerability Reported. Immediate Action Advised. See [Security Vulnerability](#).**

© 2012 Citrix Systems, Inc. All rights reserved. Specifications are subject to change without notice. Citrix Systems, Inc., the Citrix logo, Citrix XenServer, Citrix XenCenter, and CloudPlatform are trademarks or registered trademarks of Citrix Systems, Inc. All other brands or products are trademarks or registered trademarks of their respective holders.

Release notes for CloudPlatform version 3.0.5.

1. Security Vulnerability Reported: Immediate Action Advised	1
2. Submitting Feedback and Getting Help	3
3. Upgrade Instructions	5
3.1. Upgrade from 3.0.x to 3.0.5	5
3.2. Upgrade from 2.2.x to 3.0.5	11
3.3. Upgrade from 2.1.x to 3.0.5	20
4. What's New in 3.0.5	21
4.1. Inter-VLAN Routing	21
4.2. Site-to-Site VPN	21
4.3. NetScaler Autoscaling	21
4.4. Local Storage Support for Data Volumes	21
4.5. Tags	22
4.6. AWS API Changes for Tags	23
4.7. Changing the AWS API Port	23
5. Issues Fixed in 3.0.5	25
6. Known Issues in 3.0.5	29
7. API Changes from 3.0.4 to 3.0.5	33
7.1. New API Commands in 3.0.5	33
7.2. Changed API Commands in 3.0.5	35

Security Vulnerability Reported: Immediate Action Advised

We have received a report of a serious security vulnerability in CloudStack and CloudPlatform. The vulnerability allows an attacker to use a system account to issue any CloudStack API command as an administrator. The attacker could, for example, delete all VMs in the system.



Warning

This is a serious vulnerability that requires your immediate attention and action.

We have verified that this vulnerability exists on all CloudStack and CloudPlatform versions. At this time, we believe knowledge of the vulnerability is limited to a few individuals. No known exploits have occurred. However, we still recommend urgent action, particularly for public clouds.

Action Required

The vulnerability can be fixed with a single MySQL command.

1. Log in to MySQL:

```
[root@host] # mysql -u cloud -p your-password -h host-ip-address
```

2. Add a random password to the system account:

```
Mysql> update `cloud`.`user` set password=RAND() where id=1;
```


Submitting Feedback and Getting Help

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

¹ <http://support.citrix.com/cms/kc/cloud-home/>

Upgrade Instructions

3.1. Upgrade from 3.0.x to 3.0.5

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

1. If you are upgrading from 3.0.0 or 3.0.1, ensure that you query your IP address usage records and process them; for example, issue invoices for any usage that you have not yet billed users for.

Starting in 3.0.2, the usage record format for IP addresses is the same as the rest of the usage types. See [bug CS-8222¹](#)). 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. (VMware only) In each zone that includes VMware hosts, you need to add a new system VM template.
 - a. While running the existing 3.0.x 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
Public	no
Featured	no

3. Watch the screen to be sure that the template downloads successfully and enters the READY state. Do not proceed until this is successful.
4. Stop all Usage Servers if running. Run this on all Usage Server hosts.

¹ <http://bugs.cloudstack.org/browse/CS-8222>

Chapter 3. Upgrade Instructions

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

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

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

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

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

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

7. Download CloudPlatform 3.0.5 onto the management server host where it will run. Get the software from the following link:

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

You need a [My Citrix Account](#)².

8. Upgrade the CloudPlatform packages. You should have a file in the form of "CloudStack-3.0.5-N-OSVERSION.tar.gz". Untar the file, then run the install.sh script inside it. Replace the file and directory names below with those you are using:

```
# tar xzf CloudStack-3.0.5-N-OSVERSION.tar.gz
# cd CloudStack-3.0.5-N-OSVERSION
# ./install.sh
```

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

9. Choose "U" to upgrade the package

```
>U
```

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

10. If you have made changes to your existing copy of the file components.xml in your previous-version CloudPlatform installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 3.0.5.

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

**Note**

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

11. Repeat steps 7 - 10 on each management server node.

12. 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.

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

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

14. 12. (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.

Chapter 3. Upgrade Instructions

- a. Copy the CloudPlatform 3.0.5 tar file to the host, untar it, and change directory to the resulting directory.
- b. Stop the running agent.

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

- c. Update the agent software.

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

- d. Choose "U" to update the packages.
- e. Start the agent.

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

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



Note

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

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

16. If you are upgrading from 3.0.1 or 3.0.2, perform the following:
 - a. Ensure that the admin port is set to 8096 by using the "integration.api.port" global parameter.

This port is used by the cloud-sysvmadm script at the end of the upgrade procedure. For information about how to set this parameter, see "Edit the Global Configuration Settings" in the Advanced 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

17. Run the following script to stop, then start, all Secondary Storage VMs, Console Proxy VMs, and virtual routers. Run the script once on one management server. Substitute your own IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the "-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.

18. If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudPlatform 3.0.5. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudPlatform 3.0.5 Advanced Installation Guide.
19. Now apply the XenServer hotfix XS602E003 (and any other needed hotfixes) to XenServer v6.0.2 hypervisor hosts.
 - a. Disconnect the XenServer cluster from CloudPlatform.

In the left navigation bar of the CloudPlatform 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 CloudPlatform 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 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 CloudPlatform Management Server to the host.

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

- 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://download.cloud.com/support/csp/56710/xenserver-cloud-supply.tgz>
For hotfix XS602E007: <http://download.cloud.com/support/csp/57824/xenserver-cloud-supply.tgz>
- Extract the file:

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

- Run the following script:

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

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

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

- Reboot this XenServer host.
- 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.

- Run the following:

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

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



Note

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

3.2. Upgrade from 2.2.x to 3.0.5

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. See [CS-8222](#)³. Instead of a single record with the assignment and release dates, separate

³ <http://bugs.cloudstack.org/browse/CS-8222>

records are generated per aggregation period with start and end dates. After upgrading to 3.0.5, 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.



Note

(KVM only) If KVM hypervisor is used in your cloud, be sure you completed the step to insert a valid username and password into the host_details table on each KVM node as described in the 2.2.14 Release Notes. This step is critical, as the database will be encrypted after the upgrade to 3.0.5.

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

Hypervisor	Description
	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-3.0.0 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
```

Chapter 3. Upgrade Instructions

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

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

10. Download CloudPlatform 3.0.5 onto the management server host where it will run. Get the software from the following link:

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

You need a [My Citrix Account](#)⁴.

11. Upgrade the CloudPlatform packages. You should have a file in the form of "CloudStack-3.0.5-N-OSVERSION.tar.gz". Untar the file, then run the install.sh script inside it. Replace the file and directory names below with those you are using:

```
# tar xzf CloudStack-3.0.5-N-OSVERSION.tar.gz
# cd CloudStack-3.0.5-N-OSVERSION
# ./install.sh
```

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

12. Choose "U" to upgrade the package.

```
> U
```

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

13. If you have made changes to your existing copy of the file components.xml in your previous-version CloudPlatform installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 3.0.5.



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:

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

```
# 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
```

14. If you have made changes to your existing copy of the `/etc/cloud/management/db.properties` file in your previous-version CloudPlatform installation, the changes will be preserved in the upgrade. However, you need to do the following steps to place these changes in a new version of the file which is compatible with version 3.0.5.

- 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
```

15. 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 CloudPlatform database. Default: `password`. It is highly recommended that you replace this with a more secure value.

Chapter 3. Upgrade Instructions

16. Repeat steps 10 - 15 on every management server node. If you provided your own encryption key in step 15, use the same key on all other management servers.
17. 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.

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

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

19. (KVM only) Additional steps are required for each KVM host. These steps will not affect running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.



Note

After the 2.2.13 to 3.0.x upgrade on a KVM machine, Ctrl+Alt+Del button on the console view of a VM doesn't work. Use Ctrl+Alt+Insert to log in to the console of the VM.

- a. Copy the CloudStack 3.0.5 .tgz download to the host, untar it, and cd into the resulting directory.
- b. Stop the running agent.

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

- c. Update the agent software.

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

- d. Choose "U" to update the packages.
- e. Start the agent.

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

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

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

21. 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).
```

22. If you would like additional confirmation that the new system VM templates were correctly applied when these system VMs were rebooted, SSH into the System VM and check the version.

Use one of the following techniques, depending on the hypervisor.

XenServer or KVM:

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

Run the following commands on the XenServer or KVM host on which the system VM is present:

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

The output should be like the following:

```
Cloudstack Release 3.0 Mon Feb 6 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
```

Chapter 3. Upgrade Instructions

```
# cat /etc/cloudstack-release
```

The output should be like the following:

```
Cloudstack Release 3.0 Mon Feb 6 15:10:04 PST 2012
```

23. If needed, upgrade all Citrix XenServer hypervisor hosts in your cloud to a version supported by CloudPlatform 3.0.5. The supported versions are XenServer 5.6 SP2 and 6.0.2. Instructions for upgrade can be found in the CloudPlatform 3.0.3 - 3.0.5 Installation Guide.
24. Apply the XenServer hotfix XS602E003 (and any other needed hotfixes) to XenServer v6.0.2 hypervisor hosts.
 - a. Disconnect the XenServer cluster from CloudPlatform.

In the left navigation bar of the CloudPlatform 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 CloudPlatform 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 CloudPlatform Management Server to the host.

Copy from here...	...to here
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/xenserver60/NFSSR.py	/opt/xensource/sm/NFSSR.py
/usr/lib64/cloud/agent/scripts/vm/hypervisor/xenserver/setupxenserver.sh	/opt/xensource/bin/setupxenserver.sh
/usr/lib64/cloud/agent/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://download.cloud.com/support/csp/56710/xenserver-cloud-supply.tgz>

For hotfix XS602E007: <http://download.cloud.com/support/csp/57824/xenserver-cloud-supply.tgz>

- Extract the file:

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

- Run the following script:

```
# xe-install-supplemental-pack xenserver-cloud-supply.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."

3.3. Upgrade from 2.1.x to 3.0.5

Direct upgrades from version 2.1.0 - 2.1.10 to 3.0.5 are not supported. It must first be upgraded to version 2.2.14. For information on how to upgrade from 2.1.x to 2.2.14, see the version 2.2.14 Release Notes.

What's New in 3.0.5

CloudPlatform 3.0.5 includes the following new features:

4.1. 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 you 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.

4.2. 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

4.3. NetScaler Autoscaling

AutoScaling allows you to scale your back-end services or application VMs up or down seamlessly and automatically according to the conditions, schedules, and health checks you define. With AutoScaling enabled, you can ensure that the number of VMs you are using seamlessly scale up when demand increases, and decreases automatically when demand subsides. Thus it helps you save compute costs by terminating underused VMs automatically and launching new VMs when you need them, without the need for manual intervention.

Conditions for triggering a scale-up or scale-down action can vary from a simple use case like monitoring the CPU usage of a server to a complex use case of monitoring a combination of server's responsiveness and its CPU usage. For example, you can instruct AutoScaling to launch an additional VM whenever CPU usage exceeds 80 percent for ten minutes, or to terminate half of your Web site's instances when traffic is expected to be low.

CloudPlatform uses the NetScaler 10.0 load balancer to monitor all aspects of a system's health and work in unison with CloudPlatform to initiate scale-up or scale-down actions.

4.4. 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 CloudPlatform, 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.

4.5. 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 CloudPlatform 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

4.6. 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

4.7. Changing the AWS API Port

CloudPlatform listens for AWS-compatible API requests on port 7080. If you prefer to listen on another port, you can change it as follows:

1. Edit the files `/etc/cloud/management/server.xml`, `/etc/cloud/management/server-nonssl.xml`, and `/etc/cloud/management/server-ssl.xml`.
2. In each file, find the tag `<Service name="Catalina7080">`. Under this tag, locate `<Connector executor="tomcatThreadPool-internal" port= ...>`.

3. Change the port to whatever port you want to use, then save the files.
4. Restart the Management Server.



Note

If you re-install CloudPlatform, the port setting will return to 7080, so you will need to make these changes again.

Issues Fixed in 3.0.5

Issue Number	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 Management 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.
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.

Chapter 5. Issues Fixed in 3.0.5

Issue Number	Description
CS-15603	CloudPlatform 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.
CS-15274	Creating a VLAN range using Zone ID without network ID now succeeds.
CS-15256	If adding a cluster fails the first time, now able to associate cluster with Nexus VSM upon retry.
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.

Issue Number	Description
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-14952	The vCenter IP Address and the datacenter information are now present in the "virtual_supervisor_module" table. The Nexus virtual switch credentials are now encrypted.
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 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, CloudPlatform 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.

Chapter 5. Issues Fixed in 3.0.5

Issue Number	Description
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.

Known Issues in 3.0.5

Issue ID	Description
CS-16601, CS-15316	Japanese keyboard is not supported.
CS-16289	Adding an egress rule to a virtual private cloud (VPC) does not block egress to other IP addresses.
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.
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<space>" 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 success.
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-15664	A typo in the component.xml file that blocks Nicira NVP integration: <pre><pluggableservice name="NiciraNvpElementService" key="com.coud.network.element.NiciraNvpElementService" class="com.cloud.network.element.NiciraNvpElement" /></pre>

Issue ID	Description
	<p>The line should be:</p> <pre data-bbox="560 309 1334 421" style="border: 1px solid gray; padding: 5px;"> <pluggableservice name="NiciraNvpElementService" key="com.cloud.network.element.NiciraNvpElementService" class="com.cloud.network.element.NiciraNvpElement" /> </pre>
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-15218	You might find the term "CloudStack" when you expect "CloudPlatform" in scripts, file names, etc. The use of the new product name CloudPlatform is not yet fully implemented.
CS-15198	Peak bandwidth (PIR) and burst size shaping policies are not applied on Nexus 1000v virtual switch interface.
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-15124	Mixed switch environment is not supported. The zone can either be deployed as Standard vSwitch based or Nexus virtual switch based.
CS-15118	In a deployment with Nexus 1000v virtual switch, zone VLAN range is not validated against the reserved list of VLANs for Nexus 1000v.
CS-15117	In a deployment with Nexus 1000v virtual switch, disable/enable operation of the Nexus virtual switch is not working as expected. The Nexus 1000v virtual switch continues to be used to create network or edit network operations even after disabling the switch.
CS-15105	The cloud-sysvadm 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.
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, CloudPlatform directly connects to the VSM for all the port profile operations; therefore, no port profile information is cached.

Issue ID	Description
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-11514 (was 11535)	In-line mode for load balancer is not supported for all external devices.

API Changes from 3.0.4 to 3.0.5

7.1. New API Commands in 3.0.5

- 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)
- createAutoScalePolicy (Creates an autoscale policy for a provision or deprovision action, the action is taken when the all the conditions evaluates to true for the specified duration. The policy is in effect once it is attached to a autscale vm group.)
- createAutoScaleVmProfile (Creates a profile that contains information about the virtual machine which will be provisioned automatically by autoscale feature.)
- createAutoScaleVmGroup (Creates and automatically starts a virtual machine based on a service offering, disk offering, and template.)
- deleteAutoScalePolicy (Deletes a autoscale policy.)
- deleteAutoScaleVmProfile (Deletes a autoscale vm profile.)
- deleteAutoScaleVmGroup (Deletes a autoscale vm group.)
- listAutoScalePolicies (Lists autoscale policies.)
- listAutoScaleVmProfiles (Lists autoscale vm profiles.)
- listAutoScaleVmGroups (Lists autoscale vm groups.)
- enableAutoScaleVmGroup (Enables an AutoScale Vm Group)
- disableAutoScaleVmGroup (Disables an AutoScale Vm Group)
- updateAutoScalePolicy (Updates an existing autoscale policy.)
- updateAutoScaleVmProfile (Updates an existing autoscale vm profile.)
- updateAutoScaleVmGroup (Updates an existing autoscale vm group.)
- 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
```

Chapter 7. API Changes from 3.0.4 to 3.0.5


- 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)

7.2. Changed API Commands in 3.0.5

API Commands	Description
copyTemplate prepareTemplate registerTemplate updateTemplate createProject activateProject suspendProject updateProject listProjectAccounts createVolume migrateVolume attachVolume detachVolume uploadVolume createSecurityGroup registerIso copyIso updateIso createIpForwardingRule listIpForwardingRules createLoadBalancerRule updateLoadBalancerRule createSnapshot	<p>The commands in this list have a single new response parameter, and no other changes.</p> <p>New response parameter: tags(*)</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>Many other commands also have the new tags(*) parameter in addition to other changes; those commands are listed separately.</p> </div>
rebootVirtualMachine attachIso	<p>The commands in this list have two new response parameters, and no other changes.</p> <p>New response parameters: keypair, tags(*)</p>

Chapter 7. API Changes from 3.0.4 to 3.0.5

API Commands	Description
detachIso listLoadBalancerRuleInstances resetPasswordForVirtualMachine changeServiceForVirtualMachine recoverVirtualMachine startVirtualMachine migrateVirtualMachine deployVirtualMachine assignVirtualMachine updateVirtualMachine restoreVirtualMachine stopVirtualMachine destroyVirtualMachine	
listSecurityGroups listFirewallRules listPortForwardingRules listSnapshots listIps listProjects listTemplates listLoadBalancerRules	<p>The commands in this list have the following new parameters, and no other changes.</p> <p>New request parameter: tags (optional)</p> <p>New response parameter: tags(*)</p>
listF5LoadBalancerNetworks listNetscalerLoadBalancerNetworks listSrxFirewallNetworks updateNetwork	<p>The commands in this list have three new response parameters, and no other changes.</p> <p>New response parameters: canusefordeploy, vpcid, tags(*)</p>
createZone updateZone	<p>The commands in this list have the following new parameters, and no other changes.</p> <p>New request parameter: localstorageenabled (optional)</p> <p>New response parameter: localstorageenabled</p>
listZones	<p>New response parameter: localstorageenabled</p>
rebootRouter	<p>The commands in this list have two new response parameters, and no other changes.</p>

API Commands	Description
changeServiceForRouter startRouter destroyRouter stopRouter	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) 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)

Chapter 7. API Changes from 3.0.4 to 3.0.5

API Commands	Description
	New response parameters: keypair, tags(*)
updateStorageNetworkIpRange	New response parameters: id, endip, gateway, netmask, networkid, podid, startip, vlan, zoneid