Cloud.com CloudStack 2.2.11
Release Notes

Revised September 1, 2011

Contents

1 Overview

These Release Notes provide a brief description of new features and known issues for the 2.2.11 release of Cloud.com CloudStack.

Please read Known Issues on page 26 before installing. The Installation Guide provides step by step instructions for installation.

Upgrades from 2.2.0, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8, 2.2.9, and 2.2.10 to 2.2.11 are supported. See page 27.

Upgrades from 2.1.8, 2.1.9, and 2.1.10 to 2.2.4+ are now supported. Customers that are at a release prior to 2.1.8 will need to upgrade to 2.1.8 or later 2.1.x before upgrading to 2.2.4+. See page 29.

We would like to hear your feedback. You may submit feedback to us at support@cloud.com.

2 2.2.11

2.1 Issues Fixed in 2.2.11

System VMs can now start properly when upgrading.

2.2 New Features in 2.2.11

There are no new features in 2.2.11.

3 2.2.10

3.1 Issues Fixed in 2.2.10

10680	Changing xen.guest.network.device in global configuration will now change existing hosts.
<many>	Template and volume download functionality is much more reliable.
10750	vSphere: a separate port group is used for the virtual router and the guests. This allows setting different bandwidth limits on the two.
10763	vSphere: the root disk size now shows correctly.
10764	vSphere: changing the service offering will keep the CPU cap in place.
10766	vSphere: a VM doing a clean shutdown will no longer be powered off.
10843	vSphere: the network statistics in the UI have been removed from the web UI. vSphere does not provide the data needed to provide this statistic.
10844	The outbound network traffic of statically NATed guests will correctly show the additional static NAT IP as the source.
10922	vSphere: attaching of additional disks is reliable.
10907	vSphere: the CloudStack uses vCenter more efficiently to avoid API timeouts.
10489	API calls to list large numbers of VMs have improved performance.
11027	Idle management servers will no longer lose a connection to MySQL.

3.2 New Features in 2.2.10

9953	KVM: Beta support for RHEL 6.1 has been added.
4706	The API call to deploy a VM allows setting the guest IP address.
9681	The virtual router may be destroyed and recreated via the API using restartNetwork.

10659	In basic zones, an elastic load balancer function is available.
10748	The CloudStack's DNS service may be bypassed. With this set in global configuration the CloudStack's DHCP reply will send the guest to the external DNS server.
10561	Firewall Access Rules. Rules to selectively open firewall ports can be created separately from port forwarding rules via the API or by enabling a new UI tab. You can optionally specify one or more CIDRs to filter the source IPs.
11260	Allow different configuration of public network traffic for virtual routers via System Service Offerings
<many>	Improved VMware stability and performance.

4 2.2.9

4.1 Issues Fixed in 2.2.9

10860	In upgrading to 2.2.8, it was possible for the premium upgrade to fail to run. This has been fixed.
10714	A limitation on the number of templates per zone (roughly 300) has been removed.
10842	vSphere: a bug that could prevent starting a VM with an attached disk has been fixed.
<many>	The CloudStack can manage up to 20,000 physical hosts.
10681	If a secondary storage unmount fails, the CloudStack will no longer delete secondary storage contents.
10929	Under some error circumstances, it was possible for VMs to transition to the Error state incorrectly. This could lead to the erroneous deletion of the VMs. This has been fixed.
10867	VPN support has been restored.

4.2 New Features in 2.2.9

There are no new features in 2.2.9.

5 2.2.8

5.1 Issues Fixed in 2.2.8

9866	Copying a VHD from secondary storage now sets the size properly.
9367	listUsers will now return the API key and secret key.
9371	Multiple console proxies will not be started unnecessarily.
9981	The direct network behavior between XenServer and vSphere is now consistent.
9507	It is now possible to create a template from a snapshot of a deleted volume.
9604	Networks can now be renamed.
9543	Cloud-setup-management will no longer fail with updated sudoers file.
8183	sourceId and sourceType are set on volume creation.
9445	Host status is set to 'Storage down' when a storage failure occurs.
9356	Updating console proxy certificates works correctly.
9519	A performance problem with a large number of usage events has been fixed.
9138	Template limits now work correctly.
10414	Host status changes initiated from vCenter are tracked correctly.
10513	Disable accounts will work correctly.
4387	The agent protocol is more robust in the face of bad data.
9059	Host detail information now considers stopped VMs.
9470	Line breaks for events are now properly escaped.

6442	VMs that were transitioned during an HA event will have usage information tracked properly.
9750	listVolumes for the domain administrator will no longer return the virtual router's volume.
10028	When a host is removed the cluster capacity will be updated correctly.
9959	Special characters in passwords are handled properly in the UI.
9182	Newline characters in volume detach descriptions are handled properly.
9920	The SSVM properly handles a much larger amount of templates for a single user.
9655	The same subnet may be made available in multiple VLANs.
9568	On host restarts and in general the hosts are balanced across multiple management servers.
9771	Metadata is now available at the "standard" URL location. The previous location is still provided for backwards compatibility.
9828	Metadata is recreated when the virtual router is recreated.

5.2 New Features in 2.2.8

3224	Multiple NFS servers may be used to provide secondary storage for a zone.
4942	Networking metering may be performed on direct networks. This is in conjunction with InMon Traffic Sentinel and sFlow/NetFlow enabled switches.
6451	XenServer host passwords may be changed using the CloudStack API.
6873	Clusters, Pods and Zones may be put into a maintenance mode. In this mode no new VM allocations will be made to them. Administrators can still create VMs on this hardware.
7507	KVM now supports local disk for primary storage.

7553	The virtual router is now sized according to a system VM service offering. This allows for increasing virtual hardware available to some users' routers.
8115	Source IP filtering is now available in the virtual router.
8146	SRX devices can be used in basic networking zones.
8208	The CloudStack supports bare metal provisioning. Images are placed on host disks without a hypervisor.
8280	SRX devices in advanced zones can use interface NAT.
8350	The software load balancer in the virtual router has been tuned for performance.
8830	The parent template ID is provided for templates created from snapshot. This allows for template usage tracking.
8901	The CloudStack UI will give indication that a snapshot is in progress.
9109	Japanese keymapping is supported for the console viewer.
9158	It is now possible to list instances that are associated with a particular primary storage.
9250	A new guest OS type "Other PV" is available for XenServer. These are other types of templates that are paravirtualized.
9534	In service offerings it is now possible to enforce a hard cap in CPU consumption.
9579	It is now possible to add a custom DNS suffix per direct network.
9651	Multiple cloud guest networks may be added. Then direct networks may be associated with the administrator's choice of guest network.
9724	The listEvents API has been extended to allow specifying hours and minutes on queries.
10152	XenServer 5.6 SP2 is supported, except when used with security groups.

6 2.2.7

6.1 Issues Fixed in 2.2.7

10456	Create template from volume will work correctly.
10334	The default security group is assigned to VMs correctly.

6.2 New Features in 2.2.7

10435	The VPN feature has been removed from the CloudStack. We expect to make the VPN feature available again in approximately one month.

7 2.2.6

7.1 Issues Fixed in 2.2.6

<many>	Several upgrade bugs from 2.1.x were fixed.
10093	vSphere: Metadata now works correctly on guest VMs.
10068	vSphere: taking a snapshot will no longer break volume tracking.
10091	Volume deletion will correctly delete associated snapshots from primary storage.
10094	XenServer: HA may fail to restart some VMs when multiple hosts fail simultaneously or primary storage fails (causing multiple hosts to reboot simultaneously).
10118	vSphere: a guest shutdown request will be a clean shutdown if VMware tools are installed in the guest.
10200	vSphere: an attached data disk will be detached before VM destroy is processed.
9896	KVM: Windows 2008 R2 can now attach data disks.

7.2 New Features in 2.2.6

There are no new features in 2.2.6.

8 2.2.5

8.1 Issues Fixed in 2.2.5

9873	VMs are now assigned to the default security group.
9891	Upgrade from 2.2.3 to 2.2.4 no longer fails on usage_stats.
Many	The upgrade from 2.2.1 to 2.2.2 then to 2.2.4 now works properly.
9941	After upgrade to 2.2.5, the UI will now show all available volumes.
Many	The detection and use of the cloud.version table now works correctly. This fixes many upgrade bugs.
8990	Upgrade when augeas 0.8 is installed now works.

8.2 New Features in 2.2.5

There are no new features in 2.2.5.

9 2.2.4

Important: the behavior of storage allocation is more conservative in 2.2.4 than in 2.1.7 and prior releases or 2.2.0-2.2.3. The CloudStack will no longer create volumes on primary storage resources that have a storage percentage used higher than that defined by "storage.capacity.threshold" in global configuration. Previously the CloudStack would allocate a primary storage resource up to 100% full. This space reservation is required as a fix to cases where snapshots of VMs could not be taken when the storage had been allocated to 100% full. The use of a threshold setting allows the administrator to reserve space for snapshots in progress for existing volumes. **Deployments with primary storage that is close to full should examine the value of this parameter before upgrading.** If all primary storage resources are more full than storage.capacity.threshold no new volumes can be created after upgrade.

9.1 Issues Fixed in 2.2.4

9702	KVM: VM live migration will work reliably.
9152	Space is reserved on each primary storage volume for snapshots.
8103	Attempts to remove a host with running VMs will correctly fail.
8816	Listing system VM IP addresses will distinguish link local from private IP addresses.
8898	The service offering upgrade option is now always shown to users. Attempts to upgrade the service offering for a running VM will fail with a clear error message.
9079	Login problems with Safari have been fixed.
9087	Attach/detach of a data disk in a multi-cluster deployment will work correctly. Previously the data disk could be deleted.
9140	ISOs that are not bootable may now be uploaded.
8955	KVM: Userdata and instance metadata now work correctly.
8666	The guest network CIDR must be a RFC1918 address.
8959	Port forwarding with the virtual router will now work with IP addresses from multiple VLANs.
9106	The VM's metered running time is now correct.

9369	IP address releases will not intermittently fail.
9370	XenServer: the network throttling values are now correctly applied.
9460	vSphere: a reboot of a guest VM will first attempt a soft shutdown. If that fails a hard shutdown (power off) will be performed.
8802	Windows password management scripts work correctly in the presence of external network elements.
8911	A security vulnerability that allowed download of some files from the console proxy VM has been fixed.
8954	End users are no longer allowed access to the console of their virtual router.
9130	Security groups are no longer present in the UI in Advanced Networking zones.
9192	Performance of the listVirtualMachines API call in the presence of many VMs has been improved significantly.
9247	vSphere: Attaching an ISO works correctly.
9663	A security issue that could allow end users to snapshot another user's volume has been fixed.
9243	XenServer: a stop VM request will forcefully stop the VM even if qemu has crashed on the XenServer host.
7723	Host tagging now works correctly.
7935	Usage clients have a path to determining the OS type of a guest booted from a blank VM.
8532	KVM: HA failover works correctly with OCFS2.
8714	Users may again create four parallel snapshot schedules.
8967	vSphere: network bandwidth limiting works correctly.

8994	vSphere: user data and instance metadata now work correctly.
9180	XenServer: local storage now works correctly.
9539	CPU over-provisioning now works correctly.
8897	Zone delete now works correctly.
8902	Cluster delete now works correctly.
Many	Several bugs around resource limit tracking have been fixed.
9093	Firefox 4 and IE 9 are supported browsers.

9.2 New Features in 2.2.4

7424	Network throttling may be disabled altogether.
8932	The listTemplates API call will return an MD5 sum of the template.
3316	Virtual machines may be manually live-migrated by the administrator. The administrator may pick a VM and the host that the VM should be placed on.
8831	A network may be dedicated to a domain. Only users in that domain and its children will have access to the network.
8945	The global configuration parameter default.page.limit has been added. This sets the maximum number of results that will be returned by list* API calls. Default is 500.
9098	The UI has been changed to provide clearer monitoring of snapshot progress.
9635	The Java process's heap size has been increased from 128 MB to 1024 MB.
9653	Tagged private network is now supported in VMware. The CloudStack private network will share the vCenter management network and inherit its configuration. If the vCenter management network is tagged through a VLAN, the CloudStack private network will be tagged as well.

10 2.2.3

10.1 Issues Fixed in 2.2.3

8951	vSphere host capacity numbers now match the physical capacity of the host.
8977	The default route for the secondary storage VM will correctly use the public network gateway.

10.2 New Features in 2.2.3

There are no new features in 2.2.3.

11 2.2.2

11.1 Issues Fixed in 2.2.2

8614	The storage allocator now functions correctly.
8731	Console view of guests on vSphere hosts now works correctly.
8865	It is now possible to start VMs whose networks were shutdown when using 2.2.0.
8635	Direct network VM creation will work correctly in the CloudStack UI wizard.
8514	The OS type dropdown is correctly populated when creating a template from a volume.
8892	The DNS server for guests in direct tagged networks is now set properly.
8912	Password management scripts now work correctly with multiple NIC guests in all cases as well as external firewall configurations.
8604	Adding a second management server will work reliably.
7935	There is a mechanism to bill differently for guests of different hypervisor type when the guests are started from ISO images.
8530	Adding vSphere hosts to an existing cluster will work reliably.
7762	The snapshot and volume copy logic for vSphere hosts has been moved into the Secondary Storage VM.
8806	The set of hypervisors present in the cloud is now represented correctly by the API and UI.
Many	Several bugs in HA functionality across hypervisors and storage types have been fixed.
Many	Several bugs in internationalization and localization have been fixed.
8632	The dashboard view or domain administrators is now correct.

8104	If the secondary storage VM is down, booting a guest off ISO will work.
Many	Several logging improvements have been made. Logging is less verbose in some cases and more descriptive in others.

11.2 New Features in 2.2.2

8349	Routers may be listed by network ID.
8250	KVM: Security groups will work with direct tagged networks.
8664	A maximum page size is enforced. This limits server memory impact from large queries.
8263	A domain specific zone may have its scope adjusted to be public.

12 2.2.1

12.1 Issues Fixed in 2.2.1

8574	Account deletion could fail leaving resources orphaned.
8631	The DHCP server would not start in the case of external firewall integration.

12.2 New Features in 2.2.1

There are no new features in 2.2.1.

13 New Features in 2.2

Issue Number	Issue Description
591	Virtual Machines may have multiple NICs.
6802	Service offerings and disk offerings may be made private to a domain.
1974	The Virtual Router memory may be changed.
2461	A user may VPN into their virtual network using IPSec/L2TP.
3120	1:1 NAT of public IPs is possible.
3346	There is a command line interface (CLI) tool for the CloudStack. It is called cloudadm. This tool is in a beta state and its syntax may change substantially in future releases.
3386	Zones may be dedicated to domains. This allows for hardware dedication and a higher level of isolation.
3676	Multiple hypervisor types may exist in the same CloudStack cloud. An individual cluster consists of nodes of the same hypervisor type.
4286	Templates may be extracted via HTTP download or HTTP POST.
4774	ISOs may be public.
4836	Limits may be set on a domain basis. This allows an administrator to prescribe aggregate limits that apply to a set of accounts.
5060	Disk offerings can have arbitrary sizes.
5147	Primary storage devices may be placed into a maintenance mode. Then they may be taken offline and later returned to service.
5190,5191	The URL used by the Console Proxy code and its associated SSL certificate may be configured and changed.
5507	VMware vSphere ESX/ESXi are supported as hypervisor types. The CloudStack can

	manage vCenter clusters or standalone nodes.
5559	Snapshots are supported for local disk storage.
5592	The DNS domain for guests may be configured.
5688	KVM CloudStack nodes now support VLANs for isolation.
5784	KVM CloudStack now supports snapshots.
5800	KVM CloudStack supports cluster functionality, analogous to vSphere and XenServer.
6103	The "look back period" for which the system considers a stopped VM to still be consuming resources is configurable.
6994	XenServer: administrators may add pre-existing SRs as primary storage to CloudStack. This enables support for FiberChannel storage.
7871	KVM: Shared mountpoint storage is available. This enables the use of clustered filesystems like OCFS2 as primary storage.
8495	Support Juniper SRX as a managed router for guest virtual networks.
8496	Support F5 load balancer as a managed device for load balancing in virtual networks.
<many>	There have been many API enhancements, including the ability to show the lineage of a volume, show a volume's attachment time, determine a cloud's capabilities, find the OS type of a virtual machine, search for deleted templates, and more.

14 API Changes

The API has had several enhancements for 2.2. There are a large number of small changes to the API. The API was significantly improved and made more consistent. As a result most applications developed against the API will need to be adapted to be compatible with 2.2.

2.2.11 API documentation is available at:

Global Admin: http://download.cloud.com/releases/2.2.0/api_2.2.10/TOC_Global_Admin.html

Domain Admin: http://download.cloud.com/releases/2.2.0/api_2.2.10/TOC_Domain_Admin.html

User: http://download.cloud.com/releases/2.2.0/api_2.2.10/TOC_User.html

15 Known Issues

Issue Number	Issue Description
8105	KVM: NFS v4 for primary storage may not work. Use v3.
8076	KVM: Unable to process quoted strings in ifcfg-eth0 when setting up the CloudStack Agent.
8486	XenServer: putting a host into maintenance mode will fail if some guests do not have PV drivers.
7145	Basic mode networking: if the Secondary Storage VM's private and public IP ranges are in the same subnet the SSVM will not function properly.
10507	The SSVM does not get assigned a route to the internal DNS server.
5573	KVM: editing the name of a Pod will prevent VMs from starting.
<many>	The internationalization feature of the CloudStack is immature. Some strings have not been extracted and will still render in English.

16 Upgrade

WARNING: The CloudStack upgrade does not preserve UI customizations. Customers with customizations should save altered files before applying the upgrade. Then create a script that will re-apply the changes after the upgrade. Any customizations should be tested on a staging environment prior to upgrade to a new version.

16.1 Upgrade from 2.2.0, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8, 2.2.9, or 2.2.10 to 2.2.11

Perform the following to upgrade from 2.2.0, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8, 2.2.9, or 2.2.10 to 2.2.11.

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

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

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

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

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

```
# mysqldump cloud > cloud-backup.dmp
# mysqldump cloud_usage > cloud-usage-backup.dmp
```

4. Untar the tgz download and cd into the resulting directory. Then update the software on each Management Server.

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

   Choose "U" to update the packages.

5. Start one Management Server. Do not start the other Management Servers.

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

6. Wait until the UI is accessible.
7. If upgrading from 2.2.8 or earlier and using vSphere, perform the following. Otherwise, skip to step **Error! Reference source not found.**.

   The CloudStack 2.2.9 release added flexibility in naming the vCenter management network. This flexibility introduces two new global configuration parameters that must be configured to match the values in vCenter. In deployments with multiple vCenters, each vCenter must be configured with the same management network label. CloudStack defaults these configuration variables to match the defaults provided by vCenter. If you have changed the vCenter defaults, you will need to configure CloudStack with the correct values. CloudStack will assume a management network label of “Management Network” for all ESXi hosts and “Service Console” for all ESX hosts. If you have configured a different name, change the global configuration parameters “vmware.management.portgroup” for ESXi hosts and “vmware.service.console” for ESX hosts to match your deployment's specific name.

8. If you modified configuration parameters in step 7, restart the Management Server.

```
# service cloud-management restart
```

9. Start the other Management Servers. Perform this on each Management Server host.

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

Note: the CloudStack Management Server logs may contain warnings like the following. These will stop when the upgrade is completed.
java.io.IOException: SSL: Fail to init SSL! java.io.IOException: Connection closed with -1 on reading size

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

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

11. In the CloudStack Administrator UI, check the status of the hosts. All hosts should come to Up state (except for those that you know to be offline). You may need to wait 20 or 30 minutes depending on the number of hosts you have. 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.
12. If you are upgrading from version 2.2.7 or earlier, and using VMware ESX hosts, you need to extend the range of firewall ports that the console proxy works with on those hosts. This is to enable the console proxy to work with VMware-based VMs. The default additional port range is 59000-60000. To extend the port range:

a. In the CloudStack UI, choose Configuration – Global Settings, and set the following parameters:

- vmware.additional.vnc.portrange.size = 1000
- vmware.additional.vnc.portrange.start = 59000

b. On each ESX host, log in to the VMware ESX service console and run the following commands:

```
esxcfg-firewall -o 59000-60000,tcp,in,vncextras
esxcfg-firewall -o 59000-60000,tcp,out,vncextras
```

13. Stop, then start, all Secondary Storage VMs, Console Proxy VMs, and virtual routers. A script is provided to implement this. Run the script once on one management server. The script requires the IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the "-a" argument.

For example:

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

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

16.1.1 KVM Hosts

Additional steps are required for each KVM host. These steps should be performed after the Management Server upgrade above. These steps will not impact running guests in the cloud. These steps are required only for clouds using KVM as hosts and only on the KVM hosts.

On each KVM host:

1. Copy the 2.2.11 tgz download to the host, untar it, and cd into the resulting directory.
2. Stop the running agent.

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

3. Update the agent software.

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

   Choose "U" to update the packages.

4. Start the agent.

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

5. If the operating system on the host is RHEL/CentOS 6.0:

   a. cd into the directory 2.2.11/oss/.

   b. Run the following command:

```
rpm -Uvh "cloud*" --nodeps --force
```

   c. Run the following command:

```
cp /usr/bin/cloud-qemu-img  /usr/bin/qemu-img
```

16.2 Upgrade from 2.1.8, 2.1.9, or 2.1.10 to 2.2.11

Important: **Upgrades from versions 2.1.0-2.1.7 directly to 2.2.11 will fail.** The CloudStack must first be upgraded to 2.1.8 or later. Please see the 2.1.8+ Release Notes for information about this procedure.

The database transformation between 2.1.x releases to 2.2.x releases is complex. In order to ensure your successful production upgrade, Cloud.com is offering all customers free professional services to assist with the upgrade. Cloud.com will, at no expense to the customer, assist with running the upgrade on the customer's production system. Assistance will be remote, provided from Cloud.com's offices. Please contact support@cloud.com if you would like to take advantage of this offer. You will be asked to make a production database dump (as in step 9 below) available to the support team. Cloud.com will run the database segment of the upgrade and report back to you. Any errors will be fixed and a patch will be implemented and provided to you to insure a successful production upgrade.

The steps to upgrade a 2.1.8, 2.1.9 or 2.1.10 system to 2.2.11 are as follows:

1. Schedule a time with Cloud.com support so that we are on alert when you attempt the production upgrade.
2. While running the 2.1.x system, make sure you will not encounter the effects of a bug from 2.1.x. After entering mysql, run this query:

```
mysql> select * from ip_forwarding where forwarding=1 and (private_port!=concat('',
0+private_port) or public_port!=concat('', 0+public_port));
```

   This will return 0 or more rows. If there are 0 rows returned then you may proceed to the next step. If rows are returned, note the id of each returned row. Then, for each such id, delete it with this command:

```
mysql> DELETE from ip_forwarding where id=<id>;
```

3. If you are using advanced networking zones, check the value of the global configuration parameter direct.attach.untagged.vlan.enabled. This value must be set to false for deployments with advanced zones. If this value is true and you have advanced zones, set it to false.

4. While running the 2.1.x system, add a new System VM template through the admin UI. Fields MUST be the following (do not change these):

   Name: systemvm-xenserver-2.2.4
   Display Text: systemvm-xenserver-2.2.4
   URL: http://download.cloud.com/releases/2.2.0/systemvm.vhd.bz2
   Zone: All Zones
   OS Type: CentOS 5.4(64-bit)
   Format: VHD
   Password Enabled:no
   Public: no
   Featured: no

5. Watch the screen to be sure that the template downloads successfully. Do not proceed until this is successful.
6. Edit /etc/sudoers. Make sure that "default requiretty" is commented out. Do this by placing a "#" character at the beginning of the line with "default requiretty".
7. Enter mysql. Run the following SQL command.

```
mysql> select count(*) from cloud.vm_template where name='systemvm-xenserver-
2.2.4' AND removed is null;
```

   That command should return 1 as its result. If some other value is returned, cancel the upgrade and contact technical support. The upgrade will not succeed. Do not proceed until this command returns 1.

   Exit mysql.

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

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

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

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

10. 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.

```
# mysqldump cloud > cloud-backup.dmp
# mysqldump cloud_usage > cloud-usage-backup.dmp
```

11. Untar the tgz download and cd into the resulting directory. Then update the software on each Management Server.

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

    Choose "U" to update the packages.

12. Start one management server. Do not start other management servers. The database upgrade will run.

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

    This will take approximately 1 minute per 4000 rows in the vm_instance table to run.

13. You will not be able to access the UI until the database upgrade finishes. Wait for the database upgrade to finish. Tail the management server log (/var/log/cloud/management/management-server.log) and look for errors. If the database upgrade fails, the server will exit.

    Important: if the database upgrade fails, contact support and provide the entire management server log. Do not proceed with the upgrade.

14. If you modified configuration parameters in step 3, restart the Management Server.

```
# service cloud-management restart
```

15. When you can access the UI, start the remaining management servers. These should start quickly.

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

16. Start the usage servers.

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

17. In the CloudStack Administrator UI, check the status of the hosts. All hosts should come to Up state (except for those that you know to be offline). You may need to wait 20 or 30 minutes, depending on the number of hosts you have. Do not proceed to the next step until the hosts show in Up state. If the hosts do not come to the Up state, contact support.
18. Stop, then start, all Secondary Storage VMs, Console Proxy VMs, and virtual routers. A script is provided to implement this. Run the script once on one management server. The script requires the IP address of the MySQL instance, the MySQL user to connect as, and the password to use for that user. In addition to those parameters, provide the "-a" argument. For example:

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

    This might take up to an hour to run, depending on the number of accounts in the system.
    Important: in previous upgrades, this step could be delayed. In this upgrade, it is imperative that this step be done immediately.

19. You may need to edit your service offerings. In 2.1.x, the service offerings included network as well as computing resources. For example, you may have one service offering that is "small with direct networking" and another that is "small with virtual networking". In 2.2.x, the choice of computing resource and network model is separated. As a result, we recommend deleting one of a pair of service offerings when the only difference is the network type. Then you may need to edit the description of the remaining service offering. For example, in the case previously mentioned, delete "small with virtual networking" and rename "small with direct networking" to just "small".
20. You may need to edit global configuration values regarding limits. With the 2.2 series, there are global configuration values that are used as the default for resource limits consumed by users when there are no account-specific limits set. These values all default to "20". You should review these values. If you have users that are already consuming more than 20 of any of these, you should increase the corresponding value to something that will not impact their ability to provision new resources. The global configuration parameters for limits are shown in the following table.

max.account.public.ips	The default maximum number of public IPs that can be consumed by an account.
max.account.snapshots	The default maximum number of snapshots that can be created for an account.
max.account.templates	The default maximum number of templates that can be deployed for an account.
max.account.user.vms	The default maximum number of user VMs that can be deployed for an account.
max.account.volumes	The default maximum number of volumes that can be created for an account.

21. If you modified configuration parameters in step 20, restart the Management Server(s).

```
# service cloud-management restart
```

22. You may need to edit resource limits on domains. In CloudStack 2.1, the domain resource limits provide defaults for accounts in the domain. In 2.2, the domain resource limits are enforced on an aggregate limit. A domain's limit provides a maximum on the count of such resources on all accounts in that domain and all its subdomains. For example, if the ROOT domain has a VM limit of 20, the CloudStack will prohibit the creation of a 21st VM across the entire cloud. If you have implemented domain limits on 2.1 it is likely you will need to increase them, perhaps significantly. A limit of "-1" indicates that no limit is in place.

    If a VM will not start after the upgrade, check global configuration, domain, and account resource limits.

23. You may need to edit the default virtual network offering. If your deployment uses only virtual networking or uses only basic zones (direct untagged), you may skip this step. If your deployment uses direct tagged networking, set the availability to optional. Go to Configuration -> Network Offerings -> DefaultVirtualizedNetworkOffering. In Actions, choose Edit, then change the Availability to Optional. You may also set Virtual Networking availability to "Unavailable". This is useful if you want to require that users create VMs on only direct tagged networks.