Upgrading Cisco VTS

This chapter provides information about how to upgrade to Cisco VTS 2.6.7.

Note Cisco VTS 2.6.7 release will replace the Cisco VTS 2.6.6 version. You can directly upgrade to Cisco VTS 2.6.7 from Cisco VTS 2.6.5. If you are running a version other than Cisco VTS 2.6.5, you have to first upgrade to Cisco VTS 2.6.5 before you upgrade to Cisco VTS 2.6.7.

Also if you have VTSR, make sure to complete the upgrade of VTC, VTSR, reinstall VMM plugins, VTS agent and VTF before performing any CRUD operation.

This chapter has the following sections:

Upgrading VTC

Before you upgrade, ensure that:

- Cisco VTS is running version 2.6.5.
- The admin has taken the backups for Day Zero and Day One configurations for all the switches managed by Cisco VTS.

  See Device documentation for the procedure about how to copy Day Zero configuration locally.
- In an HA set up, HA status is checked on both the VMs. On the Cisco VTS GUI, check HA status under **Administration > High Availability** Or, you may use the following command:

  ```
  # sudo crm status
  ```
- In an HA setup, both VTCs are online, and one is set as Master and other is set as Slave.
- In an HA setup, *service nso status* of both VTCs is in *active (running)* state.

- In an HA setup, VTS is reachable using the VIP IP address (the IP address used to log in to the Cisco VTS GUI).
- The VTS virtual machines have enough disk-space before starting the upgrade. See Prerequisites chapter for details.
- All the devices in the inventory are reachable and accessible via Cisco VTS. Use the check-sync functionality to make sure all devices are in sync (**Inventory > Network Inventory** GUI).
- For devices that you want to be in *unmanaged* state, you set the devices to *unmanaged* mode:

```
set devices device [device_name] [device_extension]:device-info device-use unmanaged
commit
```

Examples:

```
set devices device asr-dci1 asr9k-extension:device-info device-use unmanaged

set devices device n9k-leaf n9k-extension:device-info device-use unmanaged
```

When a device is specified as *unmanaged*, Cisco VTS will not sync with these devices as part of the upgrade process. Hence, if before upgrade, you use the above command to mark the devices that are not managed by Cisco VTS, then VTS will not sync with these devices and this will not cause a failure during the upgrade.

- Devices are in unlocked state (check **Inventory > Network Inventory** GUI).
- You back up the current VTC VMs (Master and Slave) as snapshots which will need to be used to rollback if there is any problem found during the upgrade.

Note VTC and VTS are interchangeable.

"Source VTC/VTS System" can be in 2.6.5.

If there are service extensions or device template is configured, then follow steps mentioned in VTS Service Extension and Device Templates Migration section.

Step 1 Take the snapshot of the existing VTC VM. See Backing up VTC VMs as Snapshots, on page 3 for details.

Step 2 Download *vts-backup.sh* from Cisco.com, to your VTC VM (Master VTC in an HA setup).

Step 3 Go to root user using **sudo su** - from admin user login.

Step 4 Run the following command on the source VTC system.

```
show_tech_support -t -a
```

This command backs up log files, including device configuration, and generates a tar file. Copy the tar file outside of the VTC host. This file will be required for troubleshooting purpose. This needs to be done on both VTC nodes in case of an HA setup.

Step 5 Run the backup script to take a backup of the database, credential files, and templates of source VTC. This copies the backup tar file to a local directory and the home directory of the remote server you specify.

```
./vts-backup.sh
Remote server IP : <remote_server>
Remote server user: <user>
Remote server password: <password>
```

Step 6 Shutdown the current VTC VM (both Master and Slave in case of HA).

Step 7 Bring up the new VTC VM with the 2.6.7 image, with the same management IP address (both Master and Slave VTC VM in case of HA).

Step 8 Copy the *vts-backup.tgz* backup file created on 2.6.5 VM from a remote location to current VTC.

Step 9 Copy the upgrade ISO file from cisco.com to a local directory on VTC VM.

Step 10 Log in to VTC VM (Master VTC in case of HA) as root user using sudo su - from admin user login.

Step 11 Create a mount directory.

```
mkdir /mnt/vts-upgrade
```

Step 12 Mount the ISO which is copied to the local directory to /mnt/vts-upgrade

```
mount -o loop /tmp/VTS-docker-upgrade-2.6.7.iso /mnt/vts-upgrade
```

Step 13 Enter into the mount directory.

```
cd /mnt/vts-upgrade
```

Step 14 Run the upgrade script as *./upgrade.sh <backup tar file with path>*.

```
./upgrade.sh /tmp/vts-backup.tgz
```

- After Upgrade is done on VTC1 it will ask details for HA setup.
- The upgrade will setup VTCs in HA (no manual steps needed).

If you have out of band template configuration in Cisco VTS source system, follow the procedure detailed in section Preserving Out of Band Template Configuration, on page 4. If the upgrade fails, you need to perform a rollback to revert to source vtc version. See Performing a Rollback, on page 12 for details. You must rerun the upgrade procedure to upgrade to version 2.6.7 again.

Step 15 Run the following command, as root user.

```
show_tech_support -t -a
```

This command backs up log files, including device configuration, and generates a tar file. Copy the tar file outside of the VTC host. This file will be required for troubleshooting purpose. This needs to be done on both VTC nodes in case of an HA setup.

Note During the upgrade process, when you do show_tech_support after you run the upgrade script, L2 High Availability gets broken. If you face this issue, follow the steps listed in the message, and reboot the Master and Slave nodes.

Step 16 Log in to VIP and do sync-to to all devices, except for VTSR.

Backing up VTC VMs as Snapshots

Saving VTC snapshots involves:

- On vCenter—Need to be done for all VTC VMs (Master and Slave):
  1. Power Off the VTC VM (recommended)
  2. Right click on the VTC VM, select **Snapshot**, and then select **Take Snapshot...**.
  3. Enter Name and Description for snapshot and click **Ok**.

4. Power on the VTC VM.

- On OpenStack—Need to be done for all VTC VMs (Master and Slave):

1. Shutdown the VTC VMs to take snapshot using virsh save utility. VTC VMs will no longer be available in running state.

   Run **virsh list**, which shows the VTC domain ID, name, and status. Use Domain ID to save VTC VMs.

   ```
   root@vts-controller-110 ]# virsh list
    Id          Name             State
   ------------------------------------
   236          VTC1             running
   237          VTC2             running
   ```

   ```
   virsh save <id> <file>
   ```

   For example:

   ```
   virsh save <VTC Domain ID> <file>
   ```

   ```
   virsh save 236 vtc1.txt
   virsh save 237 vtc2.txt
   ```

2. Take vtc.qcow2 image backup which was used to bring up Master and Slave.

   ```
   tar –cvf vtc1.qcow2.tar vtc1.qcow2
   tar –cvf vtc2.qcow2.tar vtc2.qcow2
   ```

3. Copy tar images to external drive (vtc1.qcow2.tar ,vtc2.qcow2.tar are VTC snapshots, which will be used to rollback).

4. Restore VTC VMs which will bring VTC VMs back to running state.

   ```
   virsh restore vtc1.txt
   virsh restore vtc2.txt
   ```

5. Verify if Master and Slave are up and running in HA mode. Verify GUI login using VIP IP.

Preserving Out of Band Template Configuration

If you have out of band template configuration in 2.6.5 and want to upgrade to 2.6.7, do the following to ensure that the out of band template configuration is preserved after you upgrade to 2.6.7 without any interruption to the data plane.

Step 1 Upgrade to 2.6.7 without doing a sync-to.

```
cd /mnt/upgrades/python
python upgrade.py upgrade -ip <vip-ip> -p <password> -b <backup dir>
```

Step 2 Run sync-to dry-run.

```
cd /mnt/upgrades/python/scripts
./sync_to_dry_run.script
```

Step 3 Check /opt/vts/run/upgrade/ folder with files having non-zero size.

Step 4 If there are files with non-zero size, then Southbound lock all the devices.

```
cd /mnt/upgrades/python/scripts
./southbound_lock_managed_devices.script
```

Step 5 Create templates that contain the out of band configuration and apply the templates. Configuration with - sign will be removed from device configuration. Configuration with + sign will be added to device configuration.

Step 6 Unlock all the devices.

```
cd /mnt/upgrades/python/scripts
./unlock_managed_devices.script
```

Step 7 Do a sync-to to all the devices.

```
cd /mnt/upgrades/python/scripts
./synch_to.script
```

Upgrading VTSR

To upgrade VTSR VM, do the following:

Step 1 Get the default site ID from the VTS GUI Home page to generate a new VTSR ISO before upgrading to new VTSR.

Step 2 Delete the existing VTSR VM and bring up the new VM using the new image. See Installing VTSR for details.

Step 3 If you opt to enable Monit feature, run the following command to configure Monit details via VTS CLI. This is required to update the VTC database with Monit details. For example:

Note This has to be done after VTSR gets registered with the VTC.

```
If VTC is being upgraded from 2.6.5 then change the monit configuration as below from VTC.
If it is VTSR HA then apply the same config on both the vtsr.admin@VTC1:/opt/vts/bin$ sudo ./vts-cli.sh
 -monitConfig vtsr-monit
admin@VTC-OSPD-131-MASTER:/opt/vts/bin$ sudo ./vts-cli.sh -monitConfig vtsr-monit
[sudo] password for admin:
command monitConfig executing with input vtsr-monit ...
Enter Site Name: <site name>
 Enter VTSR Monit user: <monit username>
 Enter VTSR Monitpassword:<monit password>
 Enter salt for VTSR Monit password encryption: <key for slat encryption>
 Enter VTSR Monit process monitoring interval(in seconds): <seconds>
 Applying Monit config in VTS DB for vtsr01...
 Changing device vtsr01 state to southbound-locked...
 Applying Monit credentials on vtsr01...
 Applying Monit process monitoring interval vtsr01...Enter VTSR Monit user: admin
 Changing device vtsr01 state to unlocked...
 Successfully applied Monit config on vtsr01 in VTS DB
```

Step 4 If VTC is being upgraded from 2.6.5 (where VTS and VTF password encryption is not supported) to 2.6.7, then do the following:

a) Obtain encrypted VTC/VTF/VTSR AUTH ENCRYPTED password from VTSR:

1. SSH to any VTSR device.
2. Run bash.
3. **docker exec -it vtsr bash**
4. **confd_cli -u admin -C**

5. **show running-config vtsr-day0-config | include** "vts-auth password"
   vtsr-day0-config vts-auth password-hash ENCRYPTED_PASSWORD_SHOWN

   For example, the output will look like below:

   ```
   vtsr01# show running-config vtsr-day0-config | inc "vts-auth password"
   vtsr-day0-config vts-auth password-hash YLdKnf3qSsKA2JWQT9a0Sg==
   ```

6. **show running-config vtsr-day0-config | inc** "vtf-auth password"
   vtsr-day0-config vtf-auth password-hash ENCRYPTED_PASSWORD_SHOWN

   For example, the output will look like below:

   ```
   vtsr01# show running-config vtsr-day0-config | inc "vtf-auth password"
   vtsr-day0-config vtf-auth password-hash YLdKnf3qSsKA2JWQT9a0Sg==
   ```

7. **show running-config vtsr-day0-config | inc** "vtsr-day0-config password"
   vtsr-day0-config password ENCRYPTED_PASSWORD_SHOWN

   For example, the output will look like below:

   ```
    vtsr01# show running-config vtsr-day0-config | include "vtsr-day0-config password"
   vtsr-day0-config password G+QB+Rq/HyF1a/TDErBMgA==
   ```

b) Update VTS and VTF ENCRYPTED PASSWORD (got from above. Example: YLdKnf3qSsKA2JWQT9a0Sg== and ALdKnf3qBbKA2JWQT9a0Sg==) in NCS CDB.

1. **ncs_cli -u admin**
2. **config**
3. Set devices:

   device <vtsr device name> **state admin-state southbound-locked**

4. Set devices:

   device <vtsr device name> **config cisco-vtsr-day0:vtsr-day0-config vts-auth password-hash** <encrypted password>

5. Set devices:

   device <vtsr device name> **config cisco-vtsr-day0:vtsr-day0-config vtf-auth password-hash** <encrypted password>

6. Set devices:

   device <vtsr device name> **config cisco-vtsr-day0:vtsr-day0-config password** <encrypted password>

7. commit
8. Set devices:

   device <vtsr device name> **state admin-state unlocked**

9. commit

Step 5 Do a sync-to operation for VTSR(s) in order to sync the configuration from the VTC.

Upgrading VTF

VTF has to be uninstalled and installed after the VTC upgrade.

See Inband Installation of VTF on OpenStack and Installing VTF on vCenter for details about VTF installation and uninstallation.

Upgrading Cisco VTS under OSPD

VTS component upgrade involves the same steps as in *OSPD 10 Integration* section in the *Installing Cisco VTS Components in OpenStack using Red Hat Enterprise Linux OpenStack Director* document. The components will be automatically upgraded and the new configuration parameters applied, upon an overcloud update.

Post Upgrade Considerations

This section has certain important points you need to consider after you upgrade to Cisco VTS 2.6.7.

- A default site will be created after upgrade to VTS 2.6.7.
- After upgrade, run `chown -R nso:vts-log /opt/vts/log/nso` once on the VTS Slave. This is required so that the ssh user has access to nso logs.
- Upgrade from Cisco VTS 2.6.5 to Cisco VTS 2.6.7—Impact on SRIOV ports:

  OpenStack behavior for SRIOV ports is similar to that of OVS ports in that SRIOV ports, by default, get associated with tenant's default Security Group.

  When SRIOV ports get migrated from Cisco VTS 2.6.5 to Cisco VTS 2.6.7, Cisco VTS removes any Security Groups associated with them as they do not serve any purpose anyways.

  You must edit these SRIOV ports and associate them with either 'no security groups' or with a security group that does not use 'remote-sg'.

  If above action is not performed, any subsequent SRIOV ports updates from OpenStack would get rejected as Cisco VTS does not allow SRIOV ports to get associated with Security Groups containing remote-sg.
- After upgrade from Cisco VTS 2.6.5 to Cisco VTS 2.6.7 fabric static routes (for an overlay Router) which are designated for selective devices will not be device specific anymore. They will be applied to all network devices that have the overlay networks associated to the Router. As such, after upgrade, many devices will be going out-of-sync because of this and you have to decide if you want these static routes on those devices.
- After upgrade you need to go to **Site Administration > Virtual Machine Manager** page, and edit each OpenStack VMM and edit each Neutron Server and save. This is required to update J-Driver plugin.
- After upgrade, a default site will be created automatically.
- After upgrade you need to go to **Inventory > Host Inventory** page, and edit each host with OVS virtual switch type to trigger reinstallation of Host Agent.
- When you upgrade to VTS 2.6.7, each rule specified in the existing Security Groups gets reprogrammed on the VTFs with the reflexive attribute turned on. This may render some of the rules within the Security

Groups redundant. You need to remove any rules that are deemed redundant in the context of reflexive ACL feature.

- Cisco VTS will not be transitioning any of the BGP configuration that were part of L3 Service Extension templates when you upgrade to Cisco VTS 2.6.7, which supports BGP as a service. For migrating BGP to a service, you must:

  1. Create the appropriate Port Extension with BGP configuration and associate them respectively with all the necessary ports deployed. See *Creating Port Extensions* section in the *Cisco VTS User Guide*, for details.
  2. Validate whether the configuration being pushed to the devices are similar to those that had been pushed via the service templates.
  3. Disassociate the service templates from the devices and verify that there is no configuration or service loss.
  4. Repeat the process for all BGP configuration that can be transitioned.

Note It is not applicable for 2.6.3 to 2.6.4 upgrade, but still valid for other upgrade path.

Step 1 If there is a port-scope static route with BFD enabled in 2.6.5 and upgrade to 2.6.7, then VTC automatically pushes “no ip redirects” or “no ipv6 redirects” in 2.6.7 VTS cdb. After post upgrade if “check sync” is done then device will show as Out of sync saying that VTS 2.6.5 cdb has “no ip redirects” or “no ipv6 redirects” and not in device. This is expected in 2.6.7 and customer has to do “sync to” (from VTS CDB to Device) to push the config to device only if below matching configuration shows in check sync output.

```
devices {
     device tor6-pod2 {
         config {
             nx:interface {
                 Vlan 1001 {
                     ip {
-                        redirects false;
                     }
                     ipv6 {
-                        redirects false;
                     }
                 }
             }
         }
     }
}
```

Step 2 If the below configuration is pushed from VTS 2.6.5 to device (ASR9K as DCI/DCGW), do an upgrade to 2.6.7:

```
vrf admin-rtr-1
address-family ipv4 unicast
  import from default-vrf route-policy data-center-vrf-import-policy advertise-as-vpn
  import route-target
   200:30002 stitching
   201:45000
  300:30002 stitching
  !
```

```
export to default-vrf route-policy data-center-vrf-export-policy allow-imported-vpn
export route-target
 200:30002 stitching
 201:45000
 300:30002 stitching
!
```

- After upgrade to 2.6.7, the DCI device will go out of sync and “check sync” on VTC will show the the following configuration:

```
devices {
     device dc3-pod2 {
         config {
             cisco-ios-xr:vrf {
                 vrf-list admin-rtr-1 {
                     address-family {
                         ipv4 {
                             unicast {
                                 import {
                                     from {
                                         default-vrf {
-                                            route-polic
```

  Workaround for this issue is to do the “sync from” (DCI to VTS) only if the above configuration matches in check sync output.

- After upgrade, if all N7K and N9K devices (which has L3 configurations pushed by VTS) are Out-Of-Sync and the differences show that the changes are in default settings for maximum-paths and log-neighbor-changes under 'router bgp/vrf/address-family', then do the sync-to of N7K and N9K devices.

- In VTS 2.5.2 version, if the remote-as cli was pushed under the VRF configuration in ToR's by using device templates, and when the upgrade is performed from 2.5.2 to 2.6.2, 2.6.3 and 2.6.4 then, remote-as cli is impacted. Perform the following steps to resolve the issue:

```
==========================
Solution #1 (recommended)
==========================


Correct the templates that has remote-as as part of template migration process before upgrade.


================
Solution #2
================

If Solution #1 is not performed then,

After upgrading from 2.5.x to 2.6.2, 2.6.3 and 2.6.4, if a sync-from  (pulling the configurations
 from Device to VTC database)  is already done on ToR's, which has remote-as cli

#1 Make sure the VTS and devices (the device which has remote-as) are in sync. Click the “check
 sync” from VTS GUI.

#2 Edit the template, which has remote-as
 remove the remote-as
 add the inner-remote-as
 save the template.
    At this stage no configs are pushed to the device and the template is corrected with
inner-remote-as.

#3 to check there is no impact after #2 ,
 modify the template and save. remote-as will be in intact but changes will be applied to device.
```

```
===============
Solution #3
===============
#1 After the upgrade to 2.6.3 or 2.6.4 , perform the check sync on device (from GUI), which has
 remote-as configured, and the device will go out of sync (diffs below from cli)


nso:admin@vts-pod2-164 (config)# request devices device tor1-pod2 compare-config
diff
devices {
     device tor1-pod2 {
         config {
             nx:router {
                 bgp 300 {
                     vrf tnt1-pod2-rtr-1 {
                         neighbor 15.15.15.15 {
                             remote-as {
-                                as-number 65017;        >>>>>>>>>>>> VTS cdb has this config
                             }
                             inner-remote-as {
+                                remote-as 65017;        >>>>>>>>>>>> device has this config…
                             }
                         }
                     }
                 }
             }
         }
     }
}


device has below configs
=========================
router bgp 300
  router-id 15.15.1.1
  address-family ipv4 unicast
  address-family ipv6 unicast
  address-family l2vpn evpn
    maximum-paths ibgp 2
  neighbor 14.14.14.14
    remote-as 300
    update-source loopback1
    address-family l2vpn evpn
      send-community
      send-community extended
  vrf tnt1-pod2-rtr-1
    router-id 15.15.1.1
    address-family ipv4 unicast
      advertise l2vpn evpn
      redistribute direct route-map vts-subnet-policy
      maximum-paths ibgp 2
    neighbor 15.15.15.15
      bfd
      remote-as 65017. >>>>>>>>>>>>>>>>>>>>>>>>>>>>
      address-family ipv4 unicast
        next-hop-self



#2 Perform the sync to on VTS GUI, once the sync to is done. remote-as will be removed from
device.
```

```
<< 15-Oct-2019::22:40:22.834 SHOW
modified   /nx:interface/Ethernet[name='1/2']
default_se /nx:interface/Ethernet[name='1/2']/medium
modified   /nx:router/bgp[id='300']
modified   /nx:router/bgp[id='300']/vrf[name='tnt1-pod2-rtr-1']
modified   /nx:router/bgp[id='300']/vrf[name='tnt1-pod2-rtr-1']/neighbor[id='15.15.15.15']
deleted
/nx:router/bgp[id='300']/vrf[name='tnt1-pod2-rtr-1']/neighbor[id='15.15.15.15']/remote-as/as-number
value_set
/nx:router/bgp[id='300']/vrf[name='tnt1-pod2-rtr-1']/neighbor[id='15.15.15.15']/inner-remote-as/remote-as
 65017
>> 15-Oct-2019::22:40:23.008 INITIALIZE 0
<< 15-Oct-2019::22:40:23.008 SET_TIMEOUT
<< 15-Oct-2019::22:40:24.609 SET_TIMEOUT
<< 15-Oct-2019::22:40:24.610 INITIALIZED f94702b9363410efe5f1b895c379540d
>> 15-Oct-2019::22:40:24.611 PREPARE 0:
router bgp 300
vrf tnt1-pod2-rtr-1
  neighbor 15.15.15.15 remote-as 65017
   no remote-as 65017
  exit
!
!

<< 15-Oct-2019::22:40:24.611 SET_TIMEOUT


configs on device
=====================

router bgp 300
  router-id 15.15.1.1
  address-family ipv4 unicast
  address-family ipv6 unicast
  address-family l2vpn evpn
    maximum-paths ibgp 2
  neighbor 14.14.14.14
    remote-as 300
    update-source loopback1
    address-family l2vpn evpn
      send-community
      send-community extended
  vrf tnt1-pod2-rtr-1
    router-id 15.15.1.1
    address-family ipv4 unicast
      advertise l2vpn evpn
      redistribute direct route-map vts-subnet-policy
      maximum-paths ibgp 2
    neighbor 15.15.15.15
     bfd
      address-family ipv4 unicast
        next-hop-self                >>>>>>>>>>>> remote-as is deleted after sync to and again
compare configs show device out of sync


[edit]
nso:admin@vts-pod2-164 (config)# request devices device tor1-pod2 compare-config  [shows diffs]
diff
devices {
     device tor1-pod2 {
         config {
             nx:router {
                 bgp 300 {
```

```
                    vrf tnt1-pod2-rtr-1 {
                        neighbor 15.15.15.15 {
                            remote-as {
-                               as-number 65017;       >>>>>    (cdb has this config but device
 don't have the remote-as config)
                            }
                        }
                    }
                }
            }
        }
    }
}


#3 Southbound locks the device that has remote-as from VTS GUI


#4 from template, remove the remote-as and add the inner-remote-as and save the template.
   At this step configs will not be pushed to device, as device is in southbound locked.


#5 remove the southbound lock for device from VTS GUI, and do the sync to. At this stage it will
 push the configs back to device.


<< 15-Oct-2019::23:03:35.121 INITIALIZED 6c90c600be04eed24c0a8a284a8b78af
>> 15-Oct-2019::23:03:35.122 PREPARE 0:
router bgp 300
vrf tnt1-pod2-rtr-1
  neighbor 15.15.15.15
   remote-as 65017        >>>>>> configs got pushed to device after sync to followed by correcting
 the template in 2.6.3.
  exit
!
!
<< 15-Oct-2019::23:03:35.123 SET_TIMEOUT
<< 15-Oct-2019::23:03:35.661 PREPARE OK
```

Performing a Rollback

The following sections describe the procedure to roll back to the Cisco VTS version from which you upgraded.

- Performing a Rollback on vCenter
- Performing a Rollback on OpenStack

Performing a Rollback on OpenStack

Do the following to rollback to the Cisco VTS version from which you upgraded. This should be done for all the VTC VMs (Master and Slave).

Step 1 On the controller, run **virsh list**.

```
root@vts-controller-110 ]# virsh list
 Id          Name             State
```

```
------------------------------------
236          VTC1             running
237          VTC2             running
```

Step 2 Virsh destroy already existing VTC VMs (Master and Slave).

```
virsh destroy <id>
```

Step 3 Copy *vtc1.qcow2.tar* and *vtc2.qcow2.tar* from external drive to the controller.

Step 4 Untar *vtc1.qcow2.tar* and *vtc2.qcow2.tar*

```
untar –xvf vtc1.qcow2.tar
untar –xvf vtc2.qcow2.tar
```

Step 5 Create Master and Slave VTC (virsh create utility) using *vtc.xml* file which points to the location of *qcow* images that is untarred in the above step.

Note Create the Master VTC first, wait for two to three minutes, and then create the Slave VTC.

Step 6 Verify if Master and Slave are up and running in HA mode. Verify GUI log in using VIP IP.

Note Make sure that the *service nso status* of both VTCs is in *active* state.

In case nso status is in *inactive* state then kill and recreate that VTC. Then reverify if Master and Slave are up and running in HA mode. Verify GUI log in using VIP IP. Also, make sure that service nso status of both VTC is currently in *active* state.

Step 7 Manually reregister the VMM and Host Agent from VTS GUI.

Performing a Rollback on vCenter

Do the following to rollback to the Cisco VTS version from which you upgraded. This should be done for all the VTC VMs (Master and Slave).

Step 1 Power Off the VTC VM (recommended).

Step 2 Right click on VTC VM and select **Snapshot**, and then **Snapshot Manager...**.

Step 3 Select **Snapshot** and click **Go to**. Click **Close** to close the screen.

Step 4 Power On the VTC VM.

Step 5 Verify if HA is up and running. Verify GUI log in using VIP IP.

Step 6 Manually reregister VMM from VTS GUI.