VNF Upgrade/Redeployment Automation

Upgrading/Redeploying VNFs for Hyper-Converged Ultra M Model

USP-based VNF software upgrade and redeployment procedures are performed by executing a single remote procedure call from AutoDeploy. From an upgrade/redeployment perspective, the VNF comprises the UEM, CF, and SF. As such, performing the upgrade/redeployment operation affects each of these components.

While it is recommended to create backups of important information prior to performing the upgrade/redeployment, volumes containing call detail records (CDRs) generated by the VNF can be preserved. If this functionality is enabled, the preserved volumes are reattached to the VNF once the upgrade is completed.

Information and instructions for performing the upgrade/redeployment procedures are located in Upgrade/Redeploy Your VNF, on page 1.

Though the UEM can be upgraded with other VNF components, patch updates may be made available for the UEM under certain circumstances. Information and instructions for performing the UEM patch upgrade procedures are located in Manually Applying Patch Upgrades to the UEM, on page 6.

Upgrade/Redeploy Your VNF

This section provides instructions for upgrading VNFs deployed within Hyper-Converged Ultra M solution models.

Caution Upgrade/redeployment operations are disruptive as they involve terminating VMs for the UEM, CF, and SF components that comprise the VNF. It is strongly recommended that you backup all files related to the deployment including configuration files, logs, and images before performing the upgrade or redeployment. Refer to Backing Up Deployment Information for more information.

Important The process described in this section is supported only with Ultra M deployments based on OSP 10 and that leverage the Hyper-Converged architecture.

To upgrade or redeploy your VNF:

1. Verify that the deployment is ready for an upgrade by performing the checks identified in Pre-Deactivation/Post-Activation Health Check Summary.
2. Log on to the active AutoDeploy VM as *ubuntu*. Use the password that was created earlier for this user.
3. Become the *root* user.

   ```
   sudo -i
   ```
4. Modify the VNF package descriptor within your VNF rack and VNF descriptor configuration file to refer to the desired USP ISO.

   ```
   <--- SNIP --->
   vnf-packaged <vnf-pkg-name>
    location          <URL/package-name>
    validate-signature true
    configuration <day0_dayN_cfg_identifier>
     external-url <URL/day0_dayN_cfg_name>
    !
   !
   <--- SNIP --->
   ```

Important The VNF package name and version must be different than the previously deployed VNF package version. If the versions are identical, no actions will be taken.

For example, if you previously deployed a configuration with the following parameters:

```
<--- SNIP --->
vnf-packaged vnf-pkg1
 location home/ubuntu/6_0-1234/isos/usp-6_0-1234.iso
 validate-signature true
 configuration staros
  external-url /root/system.cfg
 !
!
<--- SNIP --->
```

Your upgrade configuration would have to specify a different name for “vnf-package” and a different ISO name in “package-location”. For example:

```
<--- SNIP --->
vnf-packaged vnf-pkg2
 location home/ubuntu/6_0-1342/isos/usp-6_0-1342.iso
 validate-signature true
 configuration staros
  external-url /root/system.cfg
 !
```

```
!
<--- SNIP --->
```

5. Modify the VNF package descriptor identifier at the NSD-level of your VNF rack and VNF descriptor configuration to reference the new VNF package.

```
nsd <nsd_name>
...
 vnf-package <vnf-pkg-name>
<--- SNIP --->
```

6. *Optional.* Modify the VNF package descriptor identifier at the VDU-levels (e.g. VNFM, UEM, CF, SF, AutoVNF) of your VNF rack and VNF descriptor configuration to reference the new VNF package.

```
<--- SNIP --->
vdu <vdu_name>
...
  image vnf-package <vnf-pkg-name>
<--- SNIP --->
```

7. Modify your cf-cdr volume catalog within theAutoDeploy configuration file to ensure that the volume containing charging detail records (CDRs) is preserved through the VNF upgrade/redeployment.

```
<--- SNIP --->
volume-catalog cf-cdr
  volume type         LUKS
  volume size         200
  volume bus          ide
  volume bootable     false
volume preserve-on-upgrade true
 !
<--- SNIP --->
```

8. *Optional.* If you're upgrading from a pre-6.0 release (e.g. 5.8) to a 6.x release (e.g. 6.0), perform this stepprefer to . If not, proceed to step 9, on page 3.

   a. Deactivate your current deployment at the Service level using the information and instructions in UAS Upgrade and Redeployment Operations.

   b. Deploy the new VNF release using the information and instructions in Deploying Hyper-Converged Ultra M Models Using UAS.

   c. Proceed to step 11, on page 4.

9. Load the modified configuration.

   a. Login to the ConfD CLI as the admin user.

   ```
   confd_cli -u admin -C
   ```

   b. Enter the ConfD configuration mode.

   ```
   config
   ```

   c. Load the VNF rack and VNF descriptor configuration file to provide the deployment artifacts to the VIM.

   ```
   load replace <your_ad_file_name>.cfg
   commit
   end
   ```

Important The **load replace** command replaces the config file with the new config file.

10. Activate the VNF rack and VNF descriptor configuration.

    activate nsd *<nsd_name>*

11. Verify that all the deployed resources have been added to the VIM once the activation process is complete.
12. Confirm that the software functions are running the desired version. Refer to the following sections for more information:
    - Determining the Running AutoDeploy Version
    - Monitoring VNF Operations -execute the **show version verbose** command through the VNF's Control Function

Upgrading/Redeploying VNFs Deployed Through a Stand-alone AutoVNF Instance

USP-based VNF software upgrade and redeployment procedures are performed by deactivating the existing deployment and then reactivating it with the new images and any related configuration changes. From an upgrade/redeployment perspective, the VNF comprises the UEM, CF, and SF. As such, performing the upgrade/redeployment operation affects each of these components.

Information and instructions for performing the upgrade/redeployment procedures are located in Upgrade/Redeploy Your VNF, on page 4.

Though the UEM can be upgraded with other VNF components, patch updates may be made available for the UEM under certain circumstances. Information and instructions for performing the UEM patch upgrade procedures are located in Manually Applying Patch Upgrades to the UEM, on page 6.

Upgrade/Redeploy Your VNF

This section provides instructions for upgrading VNFs deployed through a stand-alone AutoVNF instance.

Caution Upgrade/redeployment operations are disruptive as they involve terminating VMs for the UEM, CF, and SF components that comprise the VNF. It is strongly recommended that you backup all files related to the deployment including configuration files, logs, and images before performing the upgrade or redeployment. Refer to Backing Up Deployment Information for more information.

Important This procedure assumes that you have access to the USP ISO containing the desired VNF component (VNFC) images.

To upgrade or redeploy a VNF deployed through a stand-alone AutoVNF instance:

1. Verify that the deployment is ready for an upgrade by performing the applicable checks identified in Pre-Deactivation/Post-Activation Health Check Summary.
2. *Optional.* Onboard the ISO as described in Onboard the USP ISO if you haven't already done so.
3. *Optional.* Extract the UEM image as described in Extract the UEM VM Image if you haven't already done so.
4. *Optional.* Extract the UGP images as described in Extract the UGP VM Image if you haven't already done so.
5. *Optional.* Upload the USP images to Glance as described in Upload the USP VM Images to Glance if you haven't already done so.
6. Log on to the active AutoVNF VM as *ubuntu*. Use the password that was created earlier for this user.
7. Become the *root* user.

   ```
   sudo -i
   ```
8. *Optional.* If you're upgrading from a pre-6.0 release (e.g. 5.8) to a 6.x release (e.g. 6.0), perform this step. If not, proceed to step 9, on page 5.
   a. Delete the AutoVNF installation.

      ```
      ./boot_uas.py --autofvnf --delete
      ```
   b. Deploy the new VNF release using the information and instructions in Deploying VNFs Using AutoVNF.
   c. Proceed to step 14, on page 6.
9. Modify the VNF package descriptor within your VNF rack and VNF descriptor configuration file to refer to the desired USP ISO.

   ```
   <--- SNIP --->
   vnf-packaged <vnf-pkg-name>
    location          <URL/package-name>
    validate-signature true
    configuration <day0_dayN_cfg_identifier>
     external-url <URL/day0_dayN_cfg_name>
    !
   !
   <--- SNIP --->
   ```

Important The VNF package name and version must be different than the previously deployed VNF package version. If the versions are identical, no actions will be taken.

For example, if you previously deployed a configuration with the following parameters:

```
<--- SNIP --->
vnf-packaged vnf-pkg1
 location home/ubuntu/5_5_1-1234/isos/usp-5_5_1-1234.iso
 validate-signature true
 configuration staros
  external-url /root/system.cfg
```

```
 !
!
<--- SNIP --->
```

Your upgrade configuration would have to specify a different name for “vnf-package” and a different ISO name in “package-location”. For example:

```
<--- SNIP --->
vnf-packaged vnf-pkg2
 location home/ubuntu/6_0-1342/isos/usp-6_0-1342.iso
 validate-signature true
 configuration staros
  external-url /root/system.cfg
 !
!
<--- SNIP --->
```

10. Modify the VNF package descriptor identifier at the NSD-level of your VNF rack and VNF descriptor configuration to reference the new VNF package.

```
nsd <nsd_name>
...
 vnf-package <vnf-pkg-name>
<--- SNIP --->
```

11. *Optional.* Modify the VNF package descriptor identifier at the VDU-levels (e.g. VNFM, UEM, CF, SF, AutoVNF) of your VNF rack and VNF descriptor configuration to reference the new VNF package.

```
<--- SNIP --->
vdu <vdu_name>
...
  image vnf-package <vnf-pkg-name>
<--- SNIP --->
```

12. Load the AutoVNF VNF configuration file to load the deployment name and its attributes in the AutoVNF database.

```
load replace <your_vnfm_file_name>.cfg
commit
end
```

13. Activate the AutoVNF VNF configuration file.

```
activate nsd <nsd_name>
```

14. Verify that all the deployed resources have been added to the VIM once the activation process is complete.

Manually Applying Patch Upgrades to the UEM

Under normal circumstances, available software updates are perfomed on the UEM through the standard USP upgrade process as described above. However, under certain circumstances patch updates may be made available for the UEM to minimize system downtime. The patched software files are applied manually as per the instructions that follow.

As described in Ultra Element Manager (UEM), the UEM is comprised of the following software modules:

- Service Configuration Manager (SCM)

- Life Cycle Manager (LCM; note that this is also sometimes referred to as the VNFM-Proxy)
- Service Level Agreement Manager (SLA-M)

The UEM patch process allows for each of these modules to be updated individually.

UEM software patches are distributed as a single .tar.gz file (e.g *em_patch.tar.gz*). This file containing a number of binary files for each of the three software modules identified above. The files are organized into separate directories based on the module:

- SCM patch upgrade files are contained in *scm/*:
  - cisco-asa
  - cisco-staros-cli
  - cisco-staros-nc
  - em-sdk
  - juniper-junos
  - manual-ha
  - usc-manager
  - vnf-auto-mount
  - vnfm-proxy
- LCM patch upgrade files are contained in *vnfm-proxy/*:
  - vnfmadpt-api.jar
  - vnfmadpt-esc.jar
  - vnfmadpt-static.jar
  - vnfmproxy-core.jar
  - vnfmproxy-persistence.jar
- SLAM-M patch upgrade files are contained in *sla-m/*:
  - sla-m-<*version*>-SNAPSHOT-all.jar

Important UEM VMs are deployed in an HA cluster. (Refer to UEM Redundancy.) The patch update process must be performed on each of these VMs as described in the procedure that follows.

Caution The patch upgrade procedure is a manual process that requires copying and replacing files. Extreme caution must be exercised to ensure that the correct files are copied or removed.

To apply patch updates to the UEM software:

1. Login to the master (active) UEM VM using its VIP address. The default username is *ubuntu*.
2. Copy the UEM patch upgrade file to /tmp directory on the master (active) UEM VM.
3. Unzip and extract the new binaries.

   ```
   cd /tmp
   tar xvfz em_patch.tar.gz
   ```

   This extracts the new binaries/patch files to the */tmp/em_patch* directory.
4. Open an SSH connection to the follower (slave/standby) UEM VM using its VIP address. The default username is *ubuntu*.
5. Replace the files identified in the distribution.

   Updating SCM files:

   a. Make a backup copy of the existing SCM package.

      ```
      sudo cp -R /opt/cisco/em/git/em-scm/packages
      /opt/cisco/em/git/em-scm/packages_backup
      ```

      This creates a directory named *packages_backup* and copies the existing SCM package files to it.

   b. Delete the existing SCM files.

      ```
      sudo rm -rf /opt/cisco/em/git/em-scm/packages/*
      ```

   c. Copy updated SCM files to the load path.

      ```
      cp -r scm /opt/cisco/em/git/em-scm/packages/
      ```

   d. Verify that the files have been correctly transferred and replaced by checking the date stamps and files sizes of each file.

   e. Delete the cached files that are currently in use.

      ```
      sudo rm -rf /opt/cisco/em/git/em-scm/state/packages-in-use*
      ```

   Updating SLA-M files:

   a. Make a backup copy of the existing SLA-M package.

      ```
      sudo cp -R /opt/cisco/em/bin/sla /opt/cisco/em/bin/sla_backup
      ```

      This creates a directory named *sla_backup* and copies the existing SLA-M file(s) to it.

   b. Delete the existing SLA-M file.

      ```
      sudo rm /opt/cisco/em/bin/sla/sla-m-5.0.0-SNAPSHOT-all.jar
      ```

   c. Copy updated SLA-M file to the load path.

      ```
      sudo cp sla-m/sla-m-5.0.0-SNAPSHOT-all.jar /opt/cisco/em/bin/sla
      ```

   d. Verify that the files have correctly transferred and have been replaced by checking the date stamps and files sizes of each file.

   Updating LCM files:

   a. Make a backup copy of the existing LCM package.

```
sudo cp -R /opt/cisco/em/bin/vnfm-proxy/bundles/
/opt/cisco/em/bin/vnfm-proxy/bundles_backup
```

This creates a directory called bundles_backup and copies the existing LCM package files to it.

b. Delete the existing SCM files.

```
sudo rm /opt/cisco/em/bin/vnfm-proxy/bundles/*
```

c. Copy updated SCM files to the load path.

```
sudo cp vnfm-proxy/*.jar /opt/cisco/em/bin/vnfm-proxy/bundles/
```

d. Verify that the files have been correctly transferred and replaced by checking the date stamps and files sizes of each file.

e. Delete the cached files that are currently in use.

```
sudo rm -rf /opt/cisco/usp/apps/karaf/apache-karaf-4.0.7/data
```

Important Deleting the data folder causes Karaf to reboot. This in turn triggers the UEM VM to reboot.

6. Reboot the UEM VM.

Important If you upgraded the LCM files as part of step 5, on page 8, you can skip this step since the UEM VM would have already rebooted.

```
sudo reboot
```

7. Upon reboot, log back into the VM and verify that the modules have been properly updated.

a. Verify that the modules have started and are being monitored.

```
sudo -i
ncs_cli -u admin -C
show ems
```

```
EM VNFM
ID SLA SCM PROXY

2 UP UP UP
3 UP UP UP
```

b. Verify that the files have been loaded are in use.

```
ls /opt/cisco/em/git/em-scm/state/packages-in-use
```

```
1 2
```

c. Login to the SCM and check the HA state.

```
sudo -i
ncs_cli -u admin -C
show ncs-state ha
```

```
ncs-state ha mode connected-slave
ncs-state ha node-id 3-1500421436
ncs-state ha master [ 2-1500421473 ]
```

d. Verify that Karaf created a new cache.

```
ls /opt/cisco/usp/apps/karaf/apache-karaf-4.0.7/data
```

```
cache generated-bundles kar log port security tmp
```

Important If there are any issues, replace the updated files with the backup copies you have made, reboot the VM, and contact your local service representative. Do not proceed to the next step.

8. Log off the follower (standby) UEM VM and login to the follower UEM VM (the third UEM VM in the HA cluster) using its VIP address. The default username is *ubuntu*.
9. Repeat steps 5, on page 8 through 7, on page 9 on the follower UEM VM.

Important If there are any issues, replace the updated files with the backup copies you have made, reboot the VM, and contact your local service representative. You will also need to replace the files on the follower (slave/standby) UEM VM that was initially patched and then reboot it. Do not proceed to the next step.

10. Log off the follower UEM VM.
11. Repeat steps 5, on page 8 through 7, on page 9 on the master (active) VM. When reloading the VM, the follower (standby) UEM VM will become active with the newly patched software files.

Important If there are any issues, replace the updated files with the backup copies you have made, reboot the VM, and contact your local service representative. You will also need to replace the files on the follower (slave/standby) and follower (standby) UEM VMs that were patched earlier in this process and then reboot them.