Upgrading Cisco Elastic Services Controller

Cisco Elastic Service Controller supports two type of upgrades:

- **Backup and Restore Upgrade**: This upgrade process involves stopping the ESC keepalive daemon (for ESC HA), backing up the database, stopping and renaming (or deleting) the ESC instances, re-installing the ESC instances, and restore database. For information on the supported ESC versions for ESC 4.2 upgrade, see the table below.
- **In-service upgrade**: ESC supports in-service upgrade for high-availability nodes with a minimum downtime.

You can upgrade the ESC instance as a standalone instance or as a high availability pair. The upgrade procedure is different for standalone and high availability pair.

This chapter lists separate procedures on how to upgrade ESC standalone and ESC High Availability instance. You must review these instructions before you decide to upgrade the ESC instance. See the Installation Scenarios for more information on the installation scenarios.

- ESC only support direct upgrade from previous two minor releases. For example, ESC 2.3 will support direct upgrade from ESC 2.1 and ESC 2.2. For any release older than the supported versions for direct upgrade, you need to perform the staged upgrade.
- Upgrading ESC using RPM Package (referred to as RPM Upgrade in this chapter) applies only to the ESC upgrade between ESC patch releases with the same release number. For Example, the upgrade from ESC 3.1.0.116 to ESC 3.1.0.150. If you want to upgrade ESC between minor releases (for example, upgrade from ESC 2.3.1 to ESC 2.3.2) or major releases (for example, upgrade from ESC 3.0 to ESC 4.0), you can upgrade through Backup and Restore upgrade process using qcow2 image.
- For ESC upgrade, you should be familiar with ESC installation process.
    - For OpenStack, refer to the OpenStack installation procedures, see Chapter 4: Installing Cisco Elastic Services Controller in OpenStack.
    - For VMware, refer to the VMware Installation installation procedures, see Chapter 7: Installing Cisco Elastic Services Controller in VMware vCenter.

- For ESC HA, please refer to the ESC HA installation procedures, see Chapter 5 : Configuring High Availability for OpenStack and Chapter 8: Configuring High Availability for VMware.

Table 1: Supported ESC Versions for Upgrading to ESC 4.2

Virtual Infrastructure Manager	Supported Versions for Backup and Restore Upgrade	Supported Versions for In-Service Upgrade
OpenStack	4.0, 3.1	4.0, 3.1
VMware	4.0, 3.1	4.0, 3.1

IMPORTANT NOTES

- ESC portal now displays the notification data that was present in the database, even after the upgrade. This feature is supported only from ESC 2.1. If you are upgrading from 1.1 to 2.1 or later, you will not be able to see the notifications from the 1.1 release on the ESC portal as this data was not present in the database.
- After upgrading to the new ESC version, ESC service will manage the life cycle of all VNFs deployed in the previous release. To apply any new features (with new data models) to the existing VNFs, you must undeploy and redeploy these VNFs.

- Upgrading Standalone ESC Instance, on page 2
- Upgrading ESC HA Instances, on page 4
- In-Service Upgrade of the ESC HA Nodes in OpenStack, on page 6
- In-Service Upgrade of the ESC HA Nodes in Kernel-Based Virtual Machine (KVM), on page 9
- In-Service Upgrade of the ESC HA Nodes in VMware, on page 13

Upgrading Standalone ESC Instance

To upgrade standalone ESC instance, perform the following tasks:

1. Back up the ESC database. For more information, see Backup the Database for ESC Standalone Instance.
2. Redeploy the ESC instance. For more information, see the below section, **Deploy the ESC for Upgrade**.
3. Restore the ESC database on the new ESC instance. For more information, see the below section, **Restoring the ESC Database**.

Deploy the ESC for Upgrade

After backing up and shutting down of the old ESC VM, a new/upgraded (based on new ESC package) ESC VM should be installed. All parameters for ESC installation should be the same as the old ESC VM deployment.

- For OpenStack, you need to register the new ESC qcow2 image using the Glance command with a new image name and then use new bootvm.py script and new image name to install ESC VM.

Note In OpenStack, if an old ESC VM was assigned with floating IP, the new ESC VM should be associated with the same floating IP after the installation.

- For VMWare, you need to use the new ESC OVA file to install ESC VM. All other configurations and property values should be the same as the old VM.

Restoring the ESC Database

Restore the ESC database on the new ESC instance , using the following procedure:

Step 1 Connect to the new ESC instance using SSH.

```
$ ssh USERNAME@NEW_ESC_IP
```

Step 2 Switch to the root user.

```
$ sudo bash
```

Step 3 Stop the ESC service.

```
$ sudo escadm stop
```

Step 4 Check ESC service status to make sure all the services are stopped.

```
$ sudo escadm status
```

Step 5 Restore the database files.

```
$ scp://<username>:<password>@<backup_ip>:<filename>
$ sudo escadm restore --file /path/where/file/scp-ed/to/db.tar.bz2
```

Note If a dynamic mapping file (dynamic_mapping.xml) is used by ESC service, the dynamic mapping file should be restored into the ESC VM. Before starting ESC service, you need to copy the backup dynamic mapping file (dynamic_mapping.xml) to the path */opt/cisco/esc/esc-dynamic-mapping/*

Step 6 Restart the ESC service:

```
$ sudo escadm restart
```

After ESC service is started, the standalone ESC upgrade is complete. You can check the health of the new ESC service by running `$ sudo escadm status` in the new ESC VM.

Step 7 In Openstack, after restoring the database successfully, delete the old ESC instance:

```
$ nova delete OLD_ESC_ID
```

Important Notes:

After upgrading to the new ESC version, ESC service will keep doing life cycle management of all VNFs deployed by the old version. However, to apply any new features (with new data models) to the VNFs deployed

by the ESC with old version is not guaranteed. If you want to apply any new feature of the new ESC version to existing VNFs, you have to undeploy and redeploy those VNFs.

Upgrading ESC HA Instances

To upgrade ESC HA nodes, perform the following tasks:

1. Back up the database from an old ESC HA primary instance. For more information, see Backup the Database from the ESC HA Instances.
2. Deploy new ESC HA nodes based on new ESC version. For more information, see the below section, **Deploy the ESC HA nodes for Upgrade**.
3. Restore the Database on Primary ESC instance (Standby ESC instance will sync with the Primary ESC instance). For more information, see the below section, **Restoring the ESC Database on New Master and Standby Instances**.

Deploying the ESC HA nodes for Upgrade

After backing up and shutting down the two old ESC VMs, based on new ESC package install the new ESC VMs.

- For OpenStack, you need to register the new ESC qcow2 image using the Glance command with a new image name and then to use new bootvm.py script and new image name to install ESC VM. All other bootvm.py arguments should be the same as used to setup an old VMs.
- For VMWare, there are two steps to bring up HA pair in VMware: 1) setup two standalone instances 2) reconfigure each instance with HA info. All other configurations and property values should be the same as the old VMs.
- If VIP is used for Northbound access, keep VIP the same for the new deployment as used to reconfigure the old HA pair.

Restoring the ESC Database on New Master and Standby ESC Instances

Shut down the Standby ESC instance.

Step 1 Connect to the standby ESC instance using SSH.

```
$ ssh USERNAME@ESC_STANDBY_IP
```

Step 2 Verify that the ESC instance is standby and note the name of the standby ESC HA instance :

```
$ sudo escadm status
```

If the output value shows "BACKUP", the node is the standby ESC node.

Note If a dynamic mapping file (dynamic_mapping.xml) is used by ESC service, the dynamic mapping file should be restored into the backup ESC VM. Before power off the standby ESC node, you need to copy the backup dynamic mapping file (dynamic_mapping.xml) to the path */opt/cisco/esc/esc-dynamic-mapping/* .

Step 3 Shutdown the standby ESC instance through OpenStack Kilo/Horizon using Nova command. For ESC VM instances based in VMware vSphere, shutdown the primary instance through VMware client dashboard. An example of shutting down the standby ESC instance in OpenStack is shown below:

```
$ nova stop NEW_ESC_STANDBY_ID
```

Restore the database on the new Master ESC instance.

Step 4 Connect to the primary ESC instance using SSH.

```
$ ssh USERNAME@ESC_MASTER_IP
```

Step 5 Switch to the root user.

```
$ sudo bash
```

Step 6 Verify that the ESC instance is primary.

```
$ sudo escadm status
```

If the output value shows 'MASTER' , the node is the master ESC node.

Step 7 Stop the ESC services on the master node and verify the status to ensure the services are stopped.

```
$ sudo escadm stop
$ sudo escadm status
```

Step 8 Restore the database files.

```
$ sudo escadm restore --file /tmp/db.tar.bz2
$ scp://<username>:<password>@<backup_ip>:<filename>
```

Note If a dynamic mapping file (dynamic_mapping.xml) is used by ESC service, the dynamic mapping file should be restored into the ESC VM. Before starting the ESC node, you need to copy the backup dynamic mapping file (dynamic_mapping.xml) to the path */opt/cisco/esc-dynamic-mapping/*.

Step 9 Reboot the VM to restart the full ESC service:

```
$ sudo escadm restart
```

Step 10 Use the `$ sudo escadm status` to check the status of the ESC service.

Step 11 Start the standby ESC node.

Power on the standby ESC node through OpenStack Nova/Horizon or VMware client. After starting the standby node, ESC HA upgrade process should be complete.

Step 12 Delete the old HA instance through OpenStack Nova/Horizon or VMware client. An example of deleting the VM on OpenStack is shown below:

```
$ nova delete OLD_ESC_MASTER_RENAMED OLD_ESC_STANDBY_RENAMED
```

Upgrading VNF Monitoring Rules

In ESC 2.1 and earlier, mapping the actions and metrics defined in the datamodel to the valid actions and metrics available in the monitoring agent is enabled using the *dynamic_mappings.xml* file. The file is stored in the ESC VM and can be modified using a text editor. ESC 2.2 and later do not have an *esc-dynamic-mapping* directory and *dynamic_mappings.xml* file. The CRUD operations for mapping the actions and the metrics is available through REST API.

To upgrade the VNF monitoring rules, you must back up the *dynamic_mappings.xml* file and then restore the file in the upgraded ESC VM. For more information, see the backup and restore procedures. For upgrade of

HA instance, see Upgrading ESC HA Instances. For upgrade of the standalone instance, see Upgrading Standalone ESC Instance.

In-Service Upgrade of the ESC HA Nodes in OpenStack

In-Service upgrade in OpenStack using ESC RPM packages

Procedure

	Command or Action	Purpose
Step 1	Backup ESC database and log files.	
Step 2	Log into the ESC HA secondary VM and stop the escadm service.	`$ sudo escadm stop`

Step 3	Ensure the ESC VM is in STOP state. ESC may take some time to switch to the STOP state. If ESC status turns into STOP state, please note that it won't be the part of HA cluster and you will lose HA function temporarily.	`$ sudo escadm status`
		
		`Expected output:`
		`ESC status=0 ESC HA is stopped`

Step 4	Copy the RPM file for upgrade to the ESC VM and execute the rpm command for upgrade.	`$ sudo rpm -Uvh /home/admin/cisco-esc-3.1.0-145.x86_64.rpm`
Step 5	Start the escadm service.	`$ sudo escadm start`
Step 6	Log into the ESC HA Primary VM and repeat step 3 to step 6 in Primary VM. Please note that after stop escadm service in Primary ESC VM, a failover will be triggered and the upgraded secondary VM will take over the Primary role.	
Step 7	Check the ESC version on each instance to verify the version is upgraded correctly and make sure ESC service is running properly in new Primary VM.	`# esc_version` `# health.sh (in Primary VM)`

In-Service upgrade in OpenStack using ESC qcow2 Image

Step 1 Backup ESC database and log files.

a) Perform ESC database backup from primary node. For more information on backing up the database, see Backup the Database from the ESC HA instances.

b) Collect and backup all logs from both primary and secondary VMs. To backup the log, use the following command:

```
# sudo escadm log collect
```

Note A timestamped file will be generated in: /var/tmp/esc_log-<timestamp>.tar.bz2

c) Copy the database backup file and logs files (generated in /tmp/esc_log-.tar.bz2)* out of ESC VMs.

d) Copy the preupgrade.sh script to both Primary ESC VM and Secondary ESC VMs. Make sure the file has execution mode set. Execute the following command in both ESC VMs:

```
chmod +x preupgrade.sh
$ sudo bash preupgrade.sh

Expect output:
Success
```

Step 2 Redeploy secondary ESC instance. Register new ESC image on the secondary instance, and wait for the data to be synchronized.

a) Delete the secondary instance through Horizon/Kilo using OpenStack Nova client. In OpenStack controller, running following command through nova client.

```
nova delete <secondary_vm_name>
```

b) Register new ESC image into OpenStack Glance for redeployment usage.

```
glance image-create --name <image_name> --disk-format qcow2 --container-format bare --file
<esc_qcow2_file>
```

c) Redeploy the secondary ESC VM instance based on newer image version. Re-install new the secondary instance by using the new ESC package (bootvm.py and new registered image). All other installation parameters should be the same as the former ESC VM deployment. For example, hostname, ip address, gateway_ip, ha_node_list, kad_vip, kad_vif have to use the same values. Once the new ESC instance with upgraded version is up, it will be in secondary state.

d) Log into the new instance and run the following command to check the synchronization state of the new ESC node.

```
# drbd-overview
```

Wait until the output of drbd-overview show both nodes are "UpToDate" like the output below. It means the new ESC instance has completed the data synchronization from the primary instance.

```
esc/0 Connected Secondary/Primary UpToDate/UpToDate
```

Step 3 Stop keepalived service on Secondary instance, Power off primary instance, and then start Secondary keepalived service.

a) Log into the primary instance, set ESC primary node into maintenance mode.

```
$ sudo escadm op_mode set --mode=maintenance
```

Make sure there is no in-flight transaction ongoing before moving to the next step. To verify there are no in-flight transactions, use the following command:

```
For ESC 2.3:
$ sudo escadm ip_trans
```

For versions older than ESC 2.3, check escmanager log at (/var/log/esc/escmanager.log) and make sure there are no new transaction in escmanager log.

b) Log in to the upgraded secondary instance and shut down the ESC service.

```
$ sudo escadm stop
```

c) Power off the primary instance through OpenStack Nova client/Horizon and make sure it is off. In OpenStack Controller, run:

```
$ nova stop <primary_vm_name>
$ nova list | grep <primary_vm_name>
```

d) Log into the previously upgraded secondary instance which is in stopped state and restart the ESC service. The secondary ESC instance will take the primary role (switchover will be triggered) and start providing services with new version.

```
$ sudo escadm restart
```

Step 4 Check the ESC version on the new primary instance to verify the version is upgraded correctly.

```
$ sudo escadm status (check ha status)

Expected output:
0 ESC status=0 ESC Master Healthy

$ esc_version (check esc version)
version : 3.x.x
release : xxx
```

Step 5 Re-deploy the old primary instance with the new ESC image.

Delete the old primary instance and redeploy it by using the new ESC package (bootvm.py and new registered image).

a) Log in to the new deployed instance and check ha status. The new instance should be in secondary state:

```
$ sudo escadm status --v
```

b) Run the following command to check the synchronization state of the new ESC secondary node:

```
# drbd-overview
```

Wait until the output of drbd-overview shown as UpToDate.

c) For the new ESC secondary node, make sure the health check is passed and the ESC version are upgraded correctly.

```
$ sudo escadm status (check ha status)
Expected output:
0 ESC status=0 ESC Master Healthy
$ esc_version (check esc version)version : 2.x.x
release : xxx
$ health.sh
Expected output:
ESC HEALTH PASSED
```

Step 6 Go back in to the first upgraded primary instance and check the health and keepalived state.

```
$ drbd-overview
Expected output:
1:esc/0  Connected Primary/Secondary UpToDate/UpToDate /opt/cisco/esc/esc_database ext4 2.9G 52M 2.7G
 2%

$ sudo escadm status (check ha status)
Expected output:
0 ESC status=0 ESC Master Healthy
```

```
$ esc_version (check esc version) Expected output:
version : 2.x.x
release : xxx

$ health.sh (check esc health)
Expected output:
ESC HEALTH PASSED
```

Note Quick rollback: In case of an upgrade failure, shutdown the upgraded instance and start the old primary instance to have a quick rollback. Run the following command in the old primary instance.

```
sudo bash preupgrade.sh --revoke
```

Then redeploy the upgraded instance with old esc version to have a full rollback.

Rollback Procedure for In-service Upgrade

1. Copy the database and log backup files to a location out of ESC VMs.
2. Delete any remaining ESC instance and redeploy ESC HA VMs using qcow2 image with old version.
3. Restore the database. Follow the procedures in the section, Upgrading ESC HA Instance with Backup and Restore for HA database restore.
4. After database restore, you should have ESC service back with the old version.

In-Service Upgrade of the ESC HA Nodes in Kernel-Based Virtual Machine (KVM)

In-Service Upgrade in KVM using ESC RPM packages

Use this procedure to upgrade ESC high-availability nodes with a minimum service interruption on a Kernel-based virtual machine.

Step 1 Backup ESC database and log files.

a) Perform ESC database backup from primary node. For more information on backing up the database, see Backup the Database from the ESC HA instances.

b) Collect and backup all logs from both primary and secondary VMs. To backup the log, use the following command:

```
$ sudo escadm log collect
```

Note A timestamped log file will be generated in: /var/tmp/esc_log-<timestamp>.tar.bz2

c) Copy the database backup file and logs files (generated in /tmp/esc_log-.tar.bz2)* out of ESC VMs.

Step 2 Log into the ESC HA secondary VM and stop the ESC service.

```
$ sudo escadm stop
```

Step 3 Make sure the secondary ESC VM is in STOP state.

```
$ sudo escadm status --v
```

If ESC status=0 esc ha is stopped.

Step 4 In secondary VM, execute the rpm command for upgrade:

```
$ sudo rpm -Uvh /home/admin/cisco-esc-<latest rpm filename>.rpm
```

Step 5 Log into the primary instance, set ESC primary node into maintenance mode.

```
$ sudo escadm op_mode set --mode=maintenance
```

Make sure there are no in-flight transactions and no new transactions during the upgrade. From ESC 2.3, you may use following commands to check in-flight transactions.

```
$ sudo escadm ip_trans
```

For any build older than ESC 2.3, you may need to check escmanager log for transactions at (/var/log/esc/escmanager.log).

Step 6 Power off ESC primary node and make sure it is completely shut down. In KVM ESC controller, execute the following commands:

```
$ virsh destroy <primary_vm_name>

$ virsh list --all
```

Step 7 Log in the upgraded ESC instance (previous secondary one), start the ESC service. The upgraded VM will take over primary role and provide ESC service.

```
$ sudo escadm restart
$ start esc_monitor
```

Step 8 Check the ESC version on the new primary instance to verify the upgraded version is correct. Once it is in the Primary state, make sure ESC service is running properly in the new Primary VM.

```
$ sudo escadm status
Expected output:
0 ESC status=0 ESC Master Healthy

$ esc_version

$ health.sh
Expected output:
ESC HEALTH PASSED
```

Step 9 Power on the old primary instance. In KVM ESC controller, execute the following commands:

```
$ virsh start <primary_vm_name>
```

Step 10 Log into the VM which is still with old ESC version and repeat step 2, 3, 4, and 7 in the VM.

In-Service Upgrade in KVM using ESC OVA Image

Step 1 Backup ESC database and log files.

a) Perform ESC database backup from primary node. For more information on backing up the database, see Backup the Database from the ESC HA instances.

b) Collect and backup all logs from both primary and secondary VMs. To backup the log, use the following command:

```
$ sudo escadm log collect
```

Note A timestamped log file will be generated in: /var/tmp/esc_log-<timestamp>.tar.bz2

c) Copy the database backup file and logs files (generated in /tmp/esc_log-.tar.bz2)* out of ESC VMs.

Step 2 Redeploy secondary ESC instance. Register new ESC image on the secondary instance.

a) Delete the secondary instance through lib vert Virsh commands. On KVM host, run the following command:

```
$ Virsh destroy the <secondary_vm_name>
$ Virsh undefine --remove-all-storage <secondary_vm_name>
```

b) Copy the new ESC image into Kvm Host for redeployment usage:

```
sshpass -p "host Password' scp  /scratch/BUILD-2_x_x_x/BUILD-2_x_x_x/ESC-2_x_x_x.qcow2 root@HOSTIP:
```

c) Redeploy the secondary ESC VM instance based on newer image version. Re-install new the secondary instance by using the new ESC package (bootvm.py and new registered image). All other installation parameters should be the same as the former ESC VM deployment. For example, hostname, ip address, gateway_ip, ha_node_list, kad_vip, kad_vif have to use the same values. Once the new ESC instance with upgraded version is up, it will be in secondary state.

d) Log into the new instance and run the following command to check the synchronization state of the new ESC node.

```
$ drbd-overview
```

wait until the output of drbd-overview show both nodes are "UpToDate" like the output below. It means the new ESC instance has completed the data synchronization from the primary instance.

```
esc/0 Connected Secondary/Primary UpToDate/UpToDate
```

Step 3 Stop keepalived service on Secondary instance, Power off primary instance, and then start Secondary keepalived service.

a) Log into the primary instance, set ESC primary node into maintenance mode.

```
$ sudo escadm op_mode set --mode=maintenance
```

Make sure there is no in-flight transaction ongoing before moving to the next step. To verify there are no in-flight transactions, use the following command:

```
For ESC 2.3:
$ sudo escadm ip_trans
```

For versions older than ESC 2.3, check escmanager log at (/var/log/esc/escmanager.log) and make sure there are no new transaction in escmanager log.

b) Log in to the upgraded secondary instance and shut down the keepalived service.

```
$ sudo escadm stop
```

c) Power off the primary instance and make sure it has been completely turned off. In KVM ESC Controller, run:

```
$ virsh destroy <primary_vm_name>
$ virsh list --all
```

d) Log into the previously upgraded secondary instance which is in stopped state and start the ESC service. The secondary ESC instance will take the primary role (switchover will be triggered) and start providing services with new version.

```
$ sudo escadm restart
```

Step 4 Check the ESC version on the new primary instance to verify the version is upgraded correctly.

```
$ sudo escadm status (check ha status)
```

```
Expected output:
0 ESC status=0 ESC Master Healthy

$ esc_version (check esc version)
version : 4.1.x
release : xxx

$ health.sh (check esc health)

Expected output:
ESC HEALTH PASSED
```

Step 5 Re-deploy the old primary instance with the new ESC image.

Delete the old primary instance and redeploy it by using the new ESC package (bootvm.py and new registered image). All other installation parameters should be the same as the old ESC VM deployment. For example, hostname, ip address, gateway_ip, ha_node_list, kad_vip, kad_vif have to be the same values.

a) Log in to the new deployed instance and check ha status. The new instance should be in secondary state:

```
$ sudo escadm status
```

b) Run the following command to check the synchronization state of the new ESC secondary node:

```
$ drbd-overview
```

Wait until the output of drbd-overview shown as UpToDate.

c) For the new ESC secondary node, make sure the health check is passed and the ESC version are upgraded correctly.

```
$ sudo escadm status (check ha status)
Expected output:
0 ESC status=0 ESC Master Healthy
$ esc_version (check esc version)version : 4.1.x
release : xxx
$ health.sh
Expected output:
ESC HEALTH PASSED
```

Step 6 Go back in to the first upgraded primary instance and check the health and keepalived state.

```
$ drbd-overview
Expected output:
1:esc/0  Connected Primary/Secondary UpToDate/UpToDate /opt/cisco/esc/esc_database ext4 2.9G 52M 2.7G
 2%

$ sudo escadm status (check ha status)
Expected output:
0 ESC status=0 ESC Master Healthy

$ esc_version (check esc version) Expected output:
version : 2.x.x
release : xxx

$ health.sh (check esc health)
Expected output:
ESC HEALTH PASSED
```

Note Quick rollback: In case of an upgrade failure, shutdown the upgraded instance and start the old primary instance to have a quick rollback. Run the following command in the old primary instance.

```
sudo bash preupgrade.sh --revoke
```

Then redeploy the upgraded instance with old esc version to have a full rollback.

Rollback Procedure for In-service Upgrade

1. Copy the database and log backup files to a location out of ESC VMs.
2. Delete any remaining ESC instance and redeploy ESC HA VMs using qcow2 image with old version.
3. Restore the database. Follow the procedures in the section, Upgrading ESC HA Instance with Backup and Restore for HA database restore.
4. After database restore, you should have ESC service back with the old version.

In-Service Upgrade of the ESC HA Nodes in VMware

In-Service upgrade in VMware using ESC RPM packages

Use this procedure to upgrade the ESC high-availability nodes one node at a time with a minimum service interruption. This process leverages the ESC HA replication and failover capability to smoothly move ESC service to the new upgraded node without the manual database restore.

Step 1 Backup ESC database and log files.

a) Perform ESC database backup from primary node. For more information on backing up the database, see Backup the Database from the ESC HA instances.

b) Collect and backup all logs from both primary and secondary VMs. To backup the log, use the following command:

```
# sudo escadm log collect
```

c) Copy the database backup file and logs files (generated in /tmp/esc_log-.tar.bz2)* out of ESC VMs.

d) Copy the preupgrade.sh script and RPM files to both Primary ESC VM and Secondary ESC VMs. Execute the following command in both ESC VMs:

```
$ sudo bash preupgrade.sh

Expect output:
Success
```

Step 2 Log into the ESC HA secondary VM and stop the keepalived service.

```
$ sudo escadm stop
```

Step 3 Make sure the secondary ESC VM is in STOP state.

```
$ sudo escadm status --v
```

If ESC status=0 esc ha is stopped.

Step 4 In secondary VM, execute the rpm command for upgrade:

```
$ sudo rpm -Uvh /home/admin/cisco-esc-2.2.9-50.rpm
```

Step 5 Log into the primary instance, set ESC primary node into maintenance mode.

```
$ sudo escadm op_mode set --mode=maintenance
```

Make sure there are no in-flight transactions and no new transactions during the upgrade. From ESC 2.3, you may use following commands to check in-flight transactions.

```
$ sudo escadm ip_trans
```

For build older than ESC 2.3, you may need to check escmanager log and make sure no new transactions are recorded in this log file. The log file can be located at (/var/log/esc/escmanager.log).

Step 6 Power off ESC primary node. In VMware vSphare Client, select **Home > Inventory > VMs and Templates**, right click the primary instance name from the left panel, and select **Power > Power Off**.

Step 7 Log in to the upgraded ESC instance (previous secondary one), and start the keepalived service. The upgraded VM will take over primary role and provide ESC service.

```
$ sudo escamd restart
```

Step 8 Check the ESC version on the new primary instance to verify the upgraded version is correct. Once it is in the Primary state, make sure ESC service is running properly in the new Primary VM.

```
$ sudo escadm status
Expected output:
0 ESC status=0 ESC Master Healthy

$ esc_version

$ health.sh
Expected output:
ESC HEALTH PASSED
```

Step 9 Power on the old primary instance. In VMware vSphare Client, select **Home > Inventory > VMs and Templates**, right click the primary instance name from the left panel, then select **Power > Power On**.

Step 10 Log into the VM which is still with old ESC version and repeat step 2, 3, 4, and 7 in the VM.

Note **For a Quick rollback:**For a quick rollback to the previous version, you can just power off the upgraded primary instance. You can get the old ESC service back immediately. Run the following command in the old primary instance.

```
sudo bash preupgrade.sh --revoke
```

You can then redeploy the secondary instance to fully rollback the HA.

In-Service upgrade in VMware using ESC qcow2 Image

Step 1 Backup ESC database and log files.

a) Perform ESC database backup from primary node. For more information on backing up the database, see Backup the Database from the ESC HA instances.

b) Collect and backup all logs from both primary and secondary VMs. To backup the log, use the following command:

```
# sudo escadm log collect
```

Note A timestamped log file will be generated in: /var/tmp/esc_log-<timestamp>.tar.bz2

c) Copy the database backup file and logs files (generated in /tmp/esc_log-.tar.bz2)* out of ESC VMs.

d) Copy the preupgrade.sh script to both Primary ESC VM and Secondary ESC VMs. Execute the following command in both ESC VMs:

```
$ sudo bash preupgrade.sh

Expect output:
Success
```

Step 2 Redeploy secondary ESC instance. Register new ESC image on the secondary instance, and wait for the data to be synchronized.

a) Delete the secondary instance. To delete the secondary ESC instance, you need to first "Power Off" the instance through vSphere Client and then use the **Delete from Disk** option. In VMware vSphare Client, select **Home > Inventory > VMs and Templates**, right click the instance name from the left panel, then select **Power > Power Off**. Now to delete the secondary instance, select **Home > Inventory > VMs and Templates**, right click the instance name from the left panel, then select **Delete from Disk**.

b) Redeploy the secondary ESC VM instance based on newer image version. Re-install new the secondary instance by using the new ESC package (bootvm.py and new registered image). Once the new ESC instance with upgraded version is up, it will be in secondary state.

c) Log into the new instance and run the following command to check the synchronization state of the new ESC node.

```
$ drbd-overview
```

Wait until the output of drbd-overview show both nodes are "UpToDate" like the output below. It means the new ESC instance has completed the data synchronization from the primary instance.

```
esc/0 Connected Secondary/Primary UpToDate/UpToDate
```

Step 3 Stop keepalived service on Secondary instance, Power off primary instance, and then start Secondary keepalived service.

a) Log into the primary instance, set ESC primary node into maintenance mode.

```
$ sudo escadm op_mode set --mode=maintenance
```

Make sure there is no in-flight transaction ongoing before moving to the next step. To verify there are no in-flight transactions, use the following command:

```
For ESC 2.3:
$ sudo escadm ip_trans
```

For versions older than ESC 2.3, check escmanager log at (/var/log/esc/escmanager.log) and make sure there are no new transaction in escmanager log.

b) Log in to the upgraded secondary instance and shut down the keepalived service.

```
$ sudo escadm stop
```

c) Power off the primary instance and make sure the primary instance has been powered off. In VMware vSphare Client, select **Home > Inventory > VMs and Templates**, right click the instance name from the left panel, then select **Power > Power Off**.

d) Log into the previously upgraded secondary instance which is in stopped state and start the keepalived service. The secondary ESC instance will take the primary role (switchover will be triggered) and start providing services with new version.

```
$ sudo escadm start
```

Step 4 Check the ESC version on the new primary instance to verify the version is upgraded correctly.

```
$ sudo escadm status --v(check ha status)

Expected output:
0 ESC status=0 ESC Master Healthy

$ esc_version (check esc version)
version : 3.x.x
release : xxx

$ health.sh (check esc health)

Expected output:
ESC HEALTH PASSED
```

Step 5 Re-deploy the old primary instance with the new ESC image.

Delete the old primary instance and redeploy it by using the new ESC package (bootvm.py and new registered image). All other installation parameters should be the same as the old ESC VM deployment. For example, hostname, ip address, gateway_ip, ha_node_list, kad_vip, kad_vif have to be the same values. To delete, in the VMware vSphare Client, access, **Home > Inventory > VMs and Templates**, right click the instance name from the left panel, then select **Delete from Disk**.

a) Log in to the new deployed instance and check ha status. The new instance should be in secondary state:

```
$ sudo escadm status
```

b) Run the following command to check the synchronization state of the new ESC secondary node:

```
$ drbd-overview
```

Wait until the output of drbd-overview shown as UpToDate.

c) For the new ESC secondary node, make sure the health check is passed and the ESC version are upgraded correctly.

```
$ sudo escadm status (check ha status)
Expected output:
0 ESC status=0 ESC Master Healthy
$ esc_version (check esc version)version : 3.x.x
release : xxx
$ health.sh
Expected output:
ESC HEALTH PASSED
```

Step 6 Go back in to the first upgraded primary instance and check the health and keepalived state.

```
$ drbd-overview
Expected output:
1:esc/0  Connected Primary/Secondary UpToDate/UpToDate /opt/cisco/esc/esc_database ext4 2.9G 52M 2.7G
 2%
```

```
$ sudo escadm status (check ha status)
Expected output:
0 ESC status=0 ESC Master Healthy

$ esc_version (check esc version) Expected output:
version : 3.x.x
release : xxx

$ health.sh (check esc health)
Expected output:
ESC HEALTH PASSED
```

Note Quick rollback: In case of an upgrade failure, shutdown the upgraded instance and start the old primary instance to have a quick rollback. Run the following command in the old primary instance.

```
sudo bash preupgrade.sh --revoke
```

Then redeploy the upgraded instance with old esc version to have a full rollback.

Rollback Procedure for In-service Upgrade

1. Copy the database and log backup files to a location out of ESC VMs.
2. Delete any remaining ESC instance and redeploy ESC HA VMs using qcow2 image with old version.
3. Restore the database. Follow the procedures in the section, Upgrading ESC HA Instance with Backup and Restore for HA database restore.
4. After database restore, you should have ESC service back with the old version.