Post Upgrade Tasks

Confirm That Upgrade Is Complete

Step 1 Log into Cisco UCS Manager to ensure that the HX nodes have no pending server activities.

From **Servers tab** > **Servers** > **Pending Activities** tab check for all server activities.

Step 2 Confirm that the HX nodes match the expected firmware version.

In Cisco UCS Manager, from **Equipment** > **Firmware Management** > **Installed Firmware** tab, verify for the correct firmware version.

Step 3 Log into any controller VM through SSH.

```
# ssh admin@controller_vm_ip
```

Step 4 Confirm the HyperFlex Data Platform version.

```
# hxcli cluster version
```

```
Cluster version: 4.5(1a)
Node hx220-m5-node1 version: 4.5(1a)
Node hx220-m5-node3 version: 4.5(1a)
Node hx220-m5-node3 version: 4.5(1a)
Node hx220-m5-node4 version: 4.5(1a)
```

Step 5 Verify that the HX storage cluster is online and healthy.

```
# hxcli cluster info|grep -i health
```

```
Sample output:
healthstate : healthy
state: healthy
storage cluster is healthy
```

Step 6 Verify that the upgrade is complete and is successful.

```
stcli cluster upgrade-status
```

```
Nodes up to date:
[HX-Cluster, HX-Node-1(1.1.1.1), HX-Node-2(1.1.1.2), HX-Node-3(1.1.1.3)]
Cluster upgrade succeeded.
```

Step 7 For each browser interface you use, empty the cache and reload the browser page to refresh the HX Connect content.

Enable Snapshot Scheduler (Optional)

If you had disabled snapshot scheduler before starting the upgrade, enable the schedule now. SSH to HyperFlex cluster IP and run the command *stcli snapshot-schedule –enable* snapshot schedule.

Enable HyperFlex Software Encryption

HyperFlex Software Encryption provides file-level end-to-end AES 256-bit encryption of data at-rest. You can leverage the capability of HyperFlex Software Encryption to protect the confidentiality of your data against device theft, such as drives, servers, or entire clusters. Encryption keys are securely and remotely stored by the Intersight Key Manager, available in both the Intersight SaaS and the Intersight virtual appliance.

To enable HyperFlex Software Encryption on your cluster, check that you meet the HX Data Platform and Intersight license requirements, see Cisco HyperFlex Systems Ordering and Licensing Guide. After confirming license requirements are met, to enable HyperFlex Software Encryption, you need to download the encryption package from My Cisco Entitlement, install the package, and then enable encryption from Intersight. For more information, see HyperFlex Software Encryption.