Upgrade to Cisco EPN Manager 2.2

If you are already working with Cisco EPN Manager, you can upgrade to Cisco EPN Manager 2.2 by following one of the Valid Upgrade Paths, on page 1.

There are two upgrade methods:

- Backup-restore upgrade (recommended)—Involves backing up all data from the currently installed version of Cisco EPN Manager, then installing Cisco EPN Manager 2.2 on a new server, then restoring the backed up data to the new Cisco EPN Manager 2.2 server.
- In-place upgrade—Involves upgrading the application to the latest version on the server on which you are currently running Cisco EPN Manager.

This chapter provides instructions for upgrading to Cisco EPN Manager 2.2 using both of these methods.

The following topics provide prerequisites and procedures for upgrading in standard and high availability deployments:

Valid Upgrade Paths

Direct upgrade to Cisco EPN Manager 2.2 is possible from the following versions:

- Cisco EPN Manager 2.1.2 installed with the latest available point patch.
- Cisco EPN Manager 2.1.3
- Cisco EPN Manager 2.1.3 installed with the latest available point patch

The following table lists the valid paths for installing/upgrading to Cisco EPN Manager 2.2 from previous versions.

Current Cisco EPN Manager Version	Upgrade Path to Cisco EPN Manager 2.2:
Cisco EPN Manager 1.2.x, 2.0.x	**Cisco EPN Manager 2.1 > 2.1.3 > 2.2**

Current Cisco EPN Manager Version	Upgrade Path to Cisco EPN Manager 2.2:
Cisco EPN Manager 2.1	**Cisco EPN Manager 2.1.3 > 2.2**
Cisco EPN Manager 2.1.0.x	**Cisco EPN Manager 2.1.0.x (latest point patch) > 2.1.3 > 2.2**
Cisco EPN Manager 2.1.1	**Cisco EPN Manager 2.1.3 > 2.2**
Cisco EPN Manager 2.1.1.x	**Cisco EPN Manager 2.1.1.x (latest point patch) > 2.1.3 > 2.2**
Cisco EPN Manager 2.1.2 or 2.1.2.x	**Cisco EPN Manager 2.1.2.x (latest point patch) > 2.2**
Cisco EPN Manager 2.1.3	**Cisco EPN Manager 2.2**
Cisco EPN Manager 2.1.3.x	**Cisco EPN Manager 2.1.3.x (latest point patch) > 2.2**

See the relevant installation guide for installation prerequisites and procedures for Cisco EPN Manager versions.

For point patch installation instructions, see the readme file supplied with the patch file on the on the Software Download site on Cisco.com.

Prerequisites for Upgrading to Cisco EPN Manager 2.2

Before starting the upgrade:

1. Ensure that you have followed the relevant upgrade path based on your current version of Cisco EPN Manager. See Valid Upgrade Paths, on page 1.
2. Ensure that your deployment meets the requirements in the relevant prerequisites topic:
   - Prerequisites for OVA/VM Installations. For OVA/VM deployments, the upgrade is run from the vmWare vSphere client.
   - Prerequisites for ISO/Bare Metal Installations. For ISO/bare metal deployments, the upgrade is run from the Cisco IMC server.
3. Remove any devices running uncertified software versions from Cisco EPN Manager. This step is not mandatory but highly recommended.
4. Back up your data. See Create a Copy of Your Data.
5. Ensure that no backups are running.
6. Ensure that SCP is enabled on your client machine and the required ports are open (see Ports Used by Cisco EPN Manager). You will need to use SCP to copy files from your client machine to the Cisco EPN Manager server.
7. Copy any gpg files located in /localdisk/defaultRepo to an external repository and then delete them from this folder.

Create a Copy of Your Data

Use one or both of the following options to create a copy of your current data:

1. Back up your data to a remote repository. Refer to the backup topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide . If necessary, you can revert to the previous version by restoring the data. See Revert to the Previous Version using Data Restore.
2. If you are using a virtual machine (VM), take a base snapshot of the VM. Depending on whether you have a high availability (HA) environment or not, follow one of the procedures below. If necessary, you can revert to the previous version using the VM snapshot to restore the data. See Revert to the Previous Version Using the VM Snapshot.

Take a Base Snapshot of the VM (no HA)

Step 1 Stop Cisco EPN Manager.

```
ncs stop
```

Step 2 Suspend the VM and take a VM snapshot. Consult your system administrator for assistance, if necessary.

Step 3 Start Cisco EPN Manager.

```
ncs start
```

Take a Base Snapshot of the VM (HA)

Step 1 Remove the HA configuration:

1. Log into the Cisco EPN Manager web GUI as a user with Administrator privileges.
2. From the left sidebar, choose **Administration** > **Settings** > **High Availability**.
3. Click **HA Configuration** on the left.
4. Click **Remove**.
5. When the remove operation completes, confirm that the Configuration Mode field displays **HA Not Configured**.

Step 2 Stop Cisco EPN Manager on the primary and the secondary servers (while logged in as the Cisco EPN Manager CLI admin user.)

```
ncs stop
```

Step 3 Pause the VM and take a VM snapshot on both the primary and secondary servers. Consult your system administrator for assistance, if necessary.

Step 4 Start Cisco EPN Manager on the primary and secondary servers.

```
ncs start
```

Upgrade to Cisco EPN Manager 2.2 (No HA)

These topics explain how to upgrade to Cisco EPN Manager 2.2 from an earlier version of Cisco EPN Manager in a standard deployment (no high availability).

- In-Place Upgrade
- Backup-Restore Upgrade
- Post-Upgrade Tasks

If you are performing an upgrade in a high availability deployment, see Upgrade to Cisco EPN Manager 2.2 (High Availability), on page 6.

In-Place Upgrade

In-place upgrade involves upgrading the application to the latest version on the server on which you are currently running Cisco EPN Manager.

In-place upgrade involves the following basic steps which are explained in detail in the procedure below:

1. Download the upgrade image from Cisco.com to your client machine.
2. Copy the files from your client machine to the Cisco EPN Manager server.
3. Perform the upgrade.
4. Perform the post-upgrade licensing, authentication, and web GUI tasks described in Post-Upgrade Tasks.

Before You Begin

1. Complete the tasks in Prerequisites for Upgrading to Cisco EPN Manager 2.2, on page 2.
2. Ensure that there will be enough space for the upgrade files by doing the following:
    1. Log in as the as Linux CLI root user as described in Log In and Out as the Linux CLI Users.
    2. Check that there is at least 13G of total space by running the following command:

       ```
       df -HP /storeddata/ | awk '{ print $2 }' | tail -1
       ```

    3. If the output shows that there is total space of 13G or less, run the following command (one line):

       ```
       $ rm -rf /storeddata/Installing; mkdir /opt/Installing; ln -s /opt/Installing
       /storeddata/Installing;
       ```

    4. Log out as the Linux CLI root user.

       ```
       su - admin
       ```

To upgrade:

Step 1 From the Software Download site on Cisco.com , locate and download the upgrade image to your client machine. The file will have the prefix **CEPNM-upgrade** and the suffix **.tar.gz**. The numbers in the filename may not align to the current Cisco EPN Manager version, so be sure to check the file description.

Step 2 After the download completes, compare the upgrade image’s size on the Software Download site with its size on your client machine to make sure that the full file was downloaded. On the Software Download site, hover your mouse cursor over the upgrade image to view its MD5 Checksum size in a popup window, then compare it against the size on your client machine.

Step 3 Make sure the /localdisk/defaultRepo directory has enough space to copy the files.

1. Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
2. Log in as the as Linux CLI root user as described in Log In and Out as the Linux CLI Users.
3. Verify that /localdisk/defaultRepo has enough space using the following command. If it does not, delete all files and directories to free up some space.

   ```
   df -h /localdisk/defaultRepo
   ```

Step 4 Use SCP to retrieve the files from your client machine and copy them to the Cisco EPN Manager server's default local repository (/localdisk/defaultRepo). Run this command as the Linux CLI root user.

```
scp clientUsername@clientIP:/fullpath-to-file /localdisk/defaultRepo
```

Where:

- *clientUsername* is your username on the client machine
- *clientIP* is the IP address of the client machine to which you downloaded the files in Step 1
- *fullpath-to-file* is the full pathname of the upgrade file on the client machine

For example (the following command is one line):

```
scp jsmith@123.456.789.101:/temp/CEPNM-Upgrade-2.1.X_to_2.2.tar.gz /localdisk/defaultRepo
```

Step 5 After the file is transferred to the Cisco EPN Manager server, compare the MD5 Checksum size of the Cisco EPN Manager upgrade image against the value in Step 2 to ensure it has not been damaged.

Step 6 Log out as the Linux CLI root user.

```
su admin
```

Step 7 Stop the server.

```
ncs stop
```

Step 8 From the vmWare vSphere client (OVA) or the Cisco IMC server (Bare Metal): Upgrade the Cisco EPN Manager software using the upgrade file that is located in /localdisk/defaultRepo.

```
application upgrade filename defaultRepo
```

Where *filename* is the upgrade file located in /localdisk/defaultRepo. For example:

```
application upgrade CEPNM-Upgrade-2.1.X_to_2.2.tar.gz defaultRepo
```

Step 9 The script will ask you if you want to save the running ADE-OS configuration, and if you want to proceed with the upgrade. Answer **yes** to both questions.

```
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Please ensure you have a backup of the system before proceeding.Proceed with the application install
 ? (yes/no) [yes] ? yes
```

Step 10 Wait for the upgrade to complete and for Cisco EPN Manager to restart. This could take a few hours.

What to do next

Perform the tasks in Post-Upgrade Tasks.

Backup-Restore Upgrade

Backup-restore upgrade involves backing up all data from the currently installed version of Cisco EPN Manager, then installing Cisco EPN Manager 2.2 on a new server, then restoring the backed up data to the new Cisco EPN Manager 2.2 server. This is the recommended upgrade method.

Before You Begin

- Make sure you have completed the tasks in Prerequisites for Upgrading to Cisco EPN Manager 2.2, on page 2.
- Make sure the new server has at least the same hardware specifications as the server from which the backup was taken.
- Note the location of the remote backup repository used by the old server. You will need it to configure the same backup location on the new server.

Step 1 On the new server, install Cisco EPN Manager 2.2 by following the steps in Install Cisco EPN Manager 2.2 (No HA).

Step 2 Configure the new server to use the same remote backup repository as the old server, as explained in the remote backup repository topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Step 3 Restore the backup in the remote repository to the new server, as explained in the restore backup topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

What to do next

Perform the tasks in Post-Upgrade Tasks.

Upgrade to Cisco EPN Manager 2.2 (High Availability)

The following topics provide procedures for upgrading to Cisco EPN Manager 2.2 in a high availability deployment:

- In-Place Upgrade (High Availability)
- Backup-Restore Upgrade (High Availability)

Note High availability will not be functional until the upgrade is complete.

In-Place Upgrade (High Availability)

In-place upgrade in an HA environment involves the following basic steps which are explained in detail in the procedure below:

1. Remove the HA configuration.
2. Download the upgrade image from Cisco.com to your client machine.
3. Copy the file from your client machine to the Cisco EPN Manager primary server.
4. Perform the upgrade on the primary server.

5. Install Cisco EPN Manager 2.2 on the secondary server.
6. Perform the post-upgrade licensing, authentication, and web GUI tasks described in Post-Upgrade Tasks.
7. Reconfigure HA by pairing the primary and secondary servers.

Before You Begin

Ensure that:

- Your deployment meets the general HA requirements listed in Prerequisites for High Availability Installations.
- Your deployment meets the upgrade-specific requirements listed in Prerequisites for Upgrading to Cisco EPN Manager 2.2.
- You have the password (authentication key) that was created when HA was enabled. You will need it to perform the Cisco EPN Manager 2.2 installation on the secondary server.

Step 1 On the primary server, note the HA configuration, then remove it.

1. Log into Cisco EPN Manager as a user with Administrator privileges.
2. Choose **Administration > Settings > High Availability**.
3. Make note of the HA configuration. You will need this information to reconfigure HA after the upgrade.
4. Choose **HA Configuration** in the left navigation area, then click **Remove**.
5. Wait for the remove operation to complete.
6. Click **HA Configuration** in the left navigation area and confirm that the Configuration Mode field displays **HA Not Configured**.

Step 2 From the Software Download site on Cisco.com , locate and download the upgrade image to your client machine. The file will have the prefix **CEPNM-upgrade** and the suffix **.tar.gz**. The numbers in the filename may not align to the current Cisco EPN Manager version, so be sure to check the file description.

Step 3 Compare the MD5 Checksum size of the CEPNM upgrade image from the Software Download site against the size on your client machine. On the Software Download site, hover your mouse cursor over the upgrade image to view its size in a popup window, then compare it against the size on your client machine.

Step 4 On the primary server, make sure the /localdisk/defaultRepo directory has enough space to copy the files.

1. Start an SSH session with the primary Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
2. Log in as the as Linux CLI root user as described in Log In and Out as the Linux CLI Users.
3. Verify that /localdisk/defaultRepo has enough space using the following command. If it does not, delete all files and directories to free up some space.

```
df -h /localdisk/defaultRepo
```

Step 5 Use SCP to retrieve the files from your client machine and copy them to the Cisco EPN Manager primary server's default local repository (/localdisk/defaultRepo). You should run this command as the Linux CLI root user.

```
scpclientUsername@clientIP:/fullpath-to-file/localdisk/defaultRepo
```

Where:

- *clientUsername* is your username on the client machine
- *clientIP* is the IP address of the client machine to which you downloaded the files in *Step 2*
- *fullpath-to-file* is the full pathname of the upgrade file on the client machine

For example (the following command is one line):

```
scp jsmith@123.456.789.101:/temp/CEPNM-Upgrade-2.1.X_to_2.2.tar.gz /localdisk/defaultRepo
```

Step 6 After the file is transferred to the primary server, compare the MD5 Checksum size of the Cisco EPN Manager upgrade image against the value in *Step 3* to ensure it has not been damaged.

Step 7 On the primary server, log out as the Linux CLI root user.

```
su admin
```

Step 8 Stop the primary server by running the following command:

```
ncs stop
```

Step 9 From the vmWare vSphere client (OVA) or the Cisco IMC server (Bare Metal):Upgrade the primary server using the upgrade file that is located in /localdisk/defaultRepo.

```
application upgrade filename defaultRepo
```

Where *filename* is the upgrade file located in /localdisk/defaultRepo. For example:

```
application upgrade CEPNM-Upgrade-2.1.X_to_2.2.tar.gz defaultRepo
```

Step 10 The script will ask you if you want to save the running ADE-OS configuration, and if you want to proceed with the upgrade. Answer **yes** to both questions.

Save the current ADE-OS running configuration? (yes/no) [yes] ? **yes**

Please ensure you have a backup of the system before proceeding.Proceed with the application install ? (yes/no) [yes] ? **yes**

This step can take 30 minutes or more to complete, depending on the size of the application database. However you can continue with the next step while the upgrade is in progress for the primary server. Once the upgrade is complete, the primary server will be automatically restarted as part of the upgrade.

Step 11 Install Cisco EPN Manager 2.2 on the secondary server (you will perform a fresh installation on this server):

- **OVA/VM installation**—Perform these steps:
  1. Delete the existing VM:
     1. Launch the VMware vSphere client.
     2. Select the VM to be deleted and choose **Shut Down Guest**.
     3. Select the VM again and choose **Delete From Disk**.
     4. Click **Yes** in the displayed confirmation message.
  2. Deploy the OVA from the VMware vSphere Client
  3. Install Cisco EPN Manager on the secondary server. See Install Cisco EPN Manager on the Server

  Note (OVA/VM) If you want to retain the same IP address on the secondary server, you must first remove it from the vmWare vSphere client, then use the original address when you deploy the OVA.

- **ISO/bare metal installation**—Perform the steps in these sections:

  Note The installation procedure provided in these sections is specific to the UCS server type and hardware requirements described in Bare Metal Requirements.

1. Configure the Bare Metal Cisco UCS Server
2. Install Cisco EPN Manager on the Server

Step 12 Log into the secondary server as a Cisco EPN Manager CLI admin user and stop and restart the secondary server by running the following commands:

```
ncs stop
ncs start
```

Step 13 Update the time zone for the Compliance engine.

1. Log into the primary server as the Linux CLI root user (see Log In and Out as the Linux CLI Users).
2. Update the time zone using a soft link (the following command is one line):

```
ln -sf /usr/share/zoneinfo/$(grep ^clock /storedconfig/active/startup-config | cut -d " " -f 3)
 /etc/localtime
```

Step 14 On the primary server:

1. Start the server and then verify that the server is restarted.
2. Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted. Ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 15 On the secondary server:

1. Verify that the server is restarted.
2. Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted. Ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 16 Perform the post-upgrade tasks on the primary server. See Post-Upgrade Tasks.

Step 17 Once the post upgrade tasks are completed, re-configure HA by registering the secondary server on the primary server. Use the information you saved in *Step 1*. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server, in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Backup-Restore Upgrade (High Availability)

Backup-restore upgrade in an HA environment involves the following basic steps which are explained in detail in the procedure below:

1. Remove HA.
2. Back up your data to a remote repository.
3. Perform a fresh installation of Cisco EPN Manager on both the primary and secondary servers.
4. Restore the backup data on the primary server.
5. Reconfigure HA.

Before You Begin

- Make sure your deployment meets the general HA requirements listed in Prerequisites for High Availability Installations.
- Make sure your deployment meets the upgrade-specific requirements listed in Prerequisites for Upgrading to Cisco EPN Manager 2.2, on page 2.
- Make sure the new server has at least the same hardware specifications as the server from which the backup was taken.
- Note the location of the remote backup repository used by the old server (if applicable). You will need it to configure the same backup location on the new server.
- Make sure that you have the password (authentication key) that was created when HA was enabled. You will need it to perform the Cisco EPN Manager 2.2 installation on the secondary server.

Step 1 On the primary server, remove the High Availability configuration:

1. Log into Cisco EPN Manager as a user with Administrator privileges.
2. Choose **Administration > Settings > High Availability**.
3. Make a note of the HA configuration. You will need this information to reconfigure HA after the upgrade.
4. Choose **HA Configuration** in the left navigation area, then click **Remove**.
5. Wait for the remove operation to complete.
6. Click **HA Configuration** in the left navigation area and confirm that the Configuration Mode field displays **HA Not Configured**.

Step 2 Back up your data to the remote repository. For details, see the topics on backups in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Note If you do not have a remote repository, configure one. See the topics on remote backup repositories in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Step 3 Install Cisco EPN Manager 2.2 on the two new servers as described in Install Cisco EPN Manager 2.2 in a High Availability Deployment.

Step 4 Once the installation is completed, configure the new primary server to use the same remote backup repository as the old primary server (which you used in *Step 2*). See the topics on remote backup repositories in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Step 5 On the primary server (only), restore the backup from the remote repository. See the topics on restoring data in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Note You only need to perform the restore operation on the primary server. The secondary server will be synchronized with the primary server when HA is re-enabled.

Step 6 On the primary server:

1. Verify that the server is restarted.
2. Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted. Ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 7 If the **ncs status** output on the primary server lists **Compliance engine is stopped**, do the following:

1. Stop Cisco EPN Manager.

```
ncs stop
```

2. Log in as the Linux CLI root user (see Log In and Out as the Linux CLI Users).
3. Update the time zone using a soft link (the following command is one line):

```
ln -sf /usr/share/zoneinfo/$(grep ^clock /storedconfig/active/startup-config | cut -d " "  -f 3)
 /etc/localtime
```

Step 8 Once the restore is completed, perform the post-upgrade tasks on the primary server. See Post-Upgrade Tasks.

Step 9 Re-configure HA by registering the secondary server on the primary server. Use the information you saved in *Step 1*. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server, in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Post-Upgrade Tasks

- If you are using Cisco Smart Licensing, re-register Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. Refer to the topics that describe managing licenses in the Cisco Evolved Programmable Network Manager User and Administrator Guide .
- Synchronize the inventory of all devices with the database, as follows:
  1. In the Cisco EPN Manager GUI, choose **Monitor > Network Devices**.
  2. Select all devices, then click **Sync**.
- Instruct users to clear the browser cache on all client machines that accessed an older version of Cisco EPN Manager before they try to connect to the upgraded Cisco EPN Manager server.
- If you were using external AAA before the upgrade, configure external authentication again. Refer to the user management topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide.
- During the upgrade, the Cisco EPN Manager home page will be reset to the default home page (Getting Started page). Users can select their own default home page from the Getting Started page or from the Settings menu at the top right of the page.
- Reset all dashboards, as follows:
  1. Open any dashboard.
  2. Click on **Settings** in the top right of the dashboard.
  3. Choose **Manage Dashboards** > **Reset All Dashboards**.

Note The reset dashboard operation removes existing user-defined dashboard tabs and they must be recreated. The reset dashboard operation must be performed after backup/restore or upgrade tasks.

Note The reset dashboard operation must be performed after backup/restore or upgrade tasks.

Revert to the Previous Version of Cisco EPN Manager

This section describes how to go back to the previous version of Cisco EPN Manager after you have installed Cisco EPN Manager, for both high availability and standard environments. This is a manual process—automatic rollback is not supported.

Note You can only revert to a previous version if you created a copy of your data before installing Cisco EPN Manager, as described in Create a Copy of Your Data.

The procedure for reverting to the previous version of Cisco EPN Manager differs depending on which method you used to create a copy of your data.

- If you used the backup facility, see Revert to the Previous Version using Data Restore.
- If you took a VM snapshot, see Revert to the Previous Version Using the VM Snapshot.

Revert to the Previous Version using Data Restore

If you used the backup facility to create a copy of your data, follow one of these procedures to revert to the previous version of Cisco EPN Manager (non-HA or HA).

For non-HA environments, do the following:

1. Reinstall the previous release of Cisco EPN Manager—the release from which you did the backup.
2. Restore the data from the backup. See the topics related to restoring data in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

For HA environments, do the following:

1. Reinstall the previous release of Cisco EPN Manager on the primary and secondary servers—the release from which you did the backup.
2. On the primary server, restore the data from the backup. See the topics related to restoring data in the Cisco Evolved Programmable Network Manager User and Administrator Guide.
3. Configure HA and register the secondary server on the primary server. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Revert to the Previous Version Using the VM Snapshot

If you are using a VM for your installation and you took a VM snapshot prior to the installation, follow one of these procedures to revert to the previous version of Cisco EPN Manager (non-HA or HA).

For non-HA environments, do the following:

1. Shut down the VM.
2. Revert the VM snapshot.
3. Start the VM.

4. Start Cisco EPN Manager.

   ```
   ncs start
   ```

For HA environments, do the following:

1. Shut down the primary and secondary VM servers.
2. Revert the VM snapshot on both servers.
3. Start the primary and secondary VM servers.
4. Start Cisco EPN Manager on the primary server and on the secondary server.

   ```
   ncs start
   ```

5. Configure HA and register the secondary server on the primary server. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server in the Cisco Evolved Programmable Network Manager User and Administrator Guide.