How High Availability Works

The Cisco EPN Manager high availability (HA) framework ensures continued system operation in case of failure. HA uses a pair of linked, synchronized Cisco EPN Manager servers to minimize or eliminate the impact of application or hardware failures that may take place on either server. Servers can fail due to issues in one or more of the following areas:

- Application processes—Server, TFTP, FTP, and other process failures. You can view the status of these processes using the CLI `ncs status` command.
- Database server—Database-related process failures (the database server runs as a service on Cisco EPN Manager).
- Network—Problems with network access or reachability.
- System—Problems with the server's physical hardware or operating system.
- Virtual machine (if HA is running in a VM environment)—Problems with the VM environment on which the primary and secondary servers are installed.

The following figure shows the main components and process flows for an HA setup.
An HA deployment consists of a primary and a secondary server with Health Monitor (HM) instances (running as an application process) on both servers. When the primary server fails (either automatically or because it is manually stopped), the secondary server takes over and manages the network while you restore access to the primary server. If the deployment is configured for automatic failover, the secondary server takes over the active role within two to three minutes after the failover. This HA is based on the active/passive or cold standby model of operation. Because it is not a clustered system, when the primary server fails, the sessions are not preserved in the secondary server.

When issues on the primary server are resolved and the server is in a running state, it remains in standby mode during which it begins syncing its data with the active secondary server. When the primary is available again, you can initiate a failback operation. When a failback is triggered, the primary server again takes over the active role. This role switching between the primary and secondary servers happens within two to three minutes.

Whenever the HA configuration determines that the primary server has changed, it synchronizes this change with the secondary server. These changes are of two types:

- **File changes**, which are synchronized using the HTTPS protocol. This includes items such as report configurations, configuration templates, TFTP-root directory, administration settings, licensing files, and the key store. File synchronization is done:
  - In batches, for files that are not updated frequently (such as license files). These files are synchronized once every 500 seconds.
  - Near real-time, for files that are updated frequently. These files are synchronized once every 11 seconds.

- **Database changes**, such as updates related to configuration, performance and monitoring data. Oracle Recovery Manager (RMAN) creates the initial standby database and Oracle Active Data Guard synchronizes the databases when there is any change.

The primary and secondary HA servers exchange the following messages to maintain synchronization between the two servers:

- **Database Sync**—Includes all the information necessary to ensure that the databases on the primary and secondary servers are running and synchronized.
• File Sync—Includes frequently updated configuration files. These are synchronized every 11 seconds, while other infrequently updated configuration files are synchronized every 500 seconds.

**Note**
Configuration files that are updated manually on the primary are not synced to the secondary. When you update a configuration file manually on the primary, you must update the file on the secondary as well.

• Process Sync—Ensures that application- and database-related processes are running. These messages fall under the Heartbeat category.

• Health Monitor Sync—These messages check for the network, system, and health monitor failure conditions.

### Planning HA Deployments

The HA feature supports the following deployment models:

- **Local**: Both of the HA servers are located on the same subnet (giving them Layer 2 proximity), usually in the same data center.

- **Campus**: Both HA servers are located in different subnets connected via LAN. Typically, they will be deployed on a single campus, but at different locations within the campus.

- **Remote**: Each HA server is located in a separate, remote subnet connected via WAN. Each server is in a different facility. The facilities are geographically dispersed across countries or continents.

The following sections explain the advantages and disadvantage of each model, and discusses underlying restrictions that affect all deployment models.

HA will function using any of the supported deployment models. The main restriction is on HA’s performance and reliability, which depends on the bandwidth and latency criteria discussed in “Network Throughput Restrictions on HA”. As long as you are able to successfully manage these parameters, it is a business decision (based on business parameters, such as cost, enterprise size, geography, compliance standards, and so on) as to which of the available deployment models you choose to implement.

### Network Throughput Restrictions on HA

Cisco EPN Manager HA performance is always subject to the following limiting factors:

- The net bandwidth available to Cisco EPN Manager for handling all operations. These operations include (but are not restricted to) HA configuration, database and file synchronization, and triggering failback.

- The net latency of the network across the links between the primary and secondary servers. Irrespective of the physical proximity of these two servers, high latency on these links can affect how Cisco EPN Manager maintains sessions between the primary and secondary servers.

- The net throughput that can be delivered by the network that connects the primary and secondary servers. Net throughput varies with the net bandwidth and latency, and can be considered a function of these two factors.
These limits apply to at least some degree in every possible deployment model, although some models are more prone to problems than others. For example: Because of the high level of geographic dispersal, the Remote deployment model is more likely to have problems with both bandwidth and latency. But both the Local and Campus models, if not properly configured, are also highly susceptible to problems with throughput, as they can be saddled by low bandwidth and high latency on networks with high usage.

You will rarely see throughput problems affecting a failback or failover, as the two HA servers are in more or less constant communication and the database changes are replicated quickly. Most failovers and failbacks take approximately two to three minutes.

The main exception to this rule is the delay for a full database copy operation. This kind of operation is triggered when the primary server has been down for more than the data retention period and you then bring it back up. The data retention period for the express, express-plus and standard configurations server is six hours and for professional and Gen 2 appliance server it is 12 hours.

Cisco EPN Manager will trigger a full database copy operation from the secondary to the primary. No failback is possible during this period, although the Health Monitor page will display any events encountered while the database copy is going on. As soon as the copy is complete, the primary server will go to the “Primary Syncing” state, and you can then trigger failback. Be sure not to restart the primary server or disconnect it from the network while the full database copy is in progress.

Variations in net throughput during a full database copy operation, irrespective of database size or other factors, can mean the difference between a database copy operation that completes successfully in under an hour and one that does not complete at all. Cisco recommends for the following:

- Network throughput – minimum 500 Mbps (Mega bit per second), preferably higher.
- Network latency – maximum 100 ms, preferably under 70 ms.

Running at a lower performance may risk system stability and result in a failure to complete high availability scenarios (mainly registration & failback).

### Using the Local Model

The main advantage of the Local deployment model is that it permits use of a virtual IP address as the single management address for the system. Users can use this virtual IP to connect to Cisco EPN Manager, and devices can use it as the destination for their SNMP trap and other notifications.

The only restriction on assigning a virtual IP address is to have that IP address in the same subnet as the IP address assignment for the primary and secondary servers. For example: If the primary and secondary servers have the following IP address assignments within the given subnet, the virtual IP address for both servers can be assigned as follows:

- Subnet mask: 255.255.255.224 (/27)
- Primary server IP address: 10.10.101.2
- Secondary server IP address: 10.10.101.3
- Virtual IP address: 10.10.101.[4-30] e.g., 10.10.101.4. Note that the virtual IP address can be any of a range of addresses that are valid and unused for the given subnet mask.

In addition to this main advantage, the Local model also has the following advantages:

- Usually provides the highest bandwidth and lowest latency.
- Simplified administration.
Device configuration for forwarding syslogs and SNMP notifications is much easier.

The Local model has the following disadvantages:

• Being co-located in the same data center exposes them to site-wide failures, including power outages and natural disasters.

• Increased exposure to catastrophic site impacts will complicate business continuity planning and may increase disaster-recovery insurance costs.

**Using the Campus Model**

The Campus model assumes that the deploying organization is located at one or more geographical sites within a city, state or province, so that it has more than one location forming a “campus”. This model has the following advantages:

• Usually provides bandwidth and latency comparable to the Local model, and better than the Remote model.

• Is simpler to administer than the Remote model.

The Campus model has the following disadvantages:

• More complicated to administer than the Local model.

• Does not permit use of a virtual IP address as the single management address for the system, so it requires more device configuration (see What If I Cannot Use Virtual IP Addressing?, on page 7).

• May provide lower bandwidth and higher latency than the Local model. This can affect HA reliability and may require administrative intervention to remedy (see Network Throughput Restrictions on HA, on page 3).

• While not located at the same site, it will still be exposed to city, state, or province-wide disasters. This may complicate business continuity planning and increase disaster-recovery costs.

**Using the Remote Model**

The Remote model assumes that the deploying organization has more than one site or campus, and that these locations communicate across geographical boundaries by WAN links. It has the following advantages:

• Least likely to be affected by natural disasters. This is usually the least complex and costly model with respect to business continuity and disaster recovery.

• May reduce business insurance costs.

The Remote model has the following disadvantages:

• More complicated to administer than the Local or Campus models.

• Does not permit use of a virtual IP address as the single management address for the system, so it requires more device configuration (see What If I Cannot Use Virtual IP Addressing?, on page 7).

• Usually provides lower bandwidth and higher latency than the other two models. This can affect HA reliability and may require administrative intervention to remedy (see Network Throughput Restrictions on HA, on page 3).
Automatic Versus Manual Failover

Configuring HA for automatic failover reduces the need for network administrators to manage HA. It also reduces the time taken to respond to the conditions that provoked the failover, since it brings up the secondary server automatically.

However, we recommend that the system be configured for Manual failover under most conditions. Following this recommendation ensures that Cisco EPN Manager does not go into a state where it keeps failing over to the secondary server due to intermittent network outages. This scenario is most likely when deploying HA using the Remote model. This model is often especially susceptible to extreme variations in bandwidth and latency (see Planning HA Deployments, on page 3 and Network Throughput Restrictions on HA, on page 3).

If the failover type is set to Automatic and the network connection goes down or the network link between the primary and secondary servers becomes unreachable, there is also a small possibility that both the primary and secondary servers will become active at the same time. We refer to this as the “split brain scenario”.

To prevent this, the primary server always checks to see if the secondary server is Active. As soon as the network connection or link is restored and the primary is able to reach the secondary again, the primary server checks the secondary server’s state. If the secondary state is Active, then the primary server goes down on its own. Users can then trigger a normal, manual failback to the primary server.

Note that this scenario only occurs when the primary HA server is configured for Automatic failover. Configuring the primary server for Manual failover eliminates the possibility of this scenario. This is another reason why we recommend Manual failover configuration.

Automatic failover is especially ill-advised for larger enterprises. If a particular HA deployment chooses to go with Automatic failover anyway, an administrator may be forced to choose between the data that was newly added to the primary or to the secondary. This means, essentially, that there is a possibility of data loss whenever a split-brain scenario occurs. For help dealing with this issue, see How to Recover From Split-Brain Scenario, on page 30.

To ensure that HA is managed correctly, Cisco recommends that Cisco EPN Manager administrators always confirm the overall health of the HA deployment before initiating failover or failback, including:

- The current state of the primary.
- The current state of the secondary.
- The current state of connectivity between the two servers.

Set Up High Availability

The Cisco Evolved Programmable Network Manager Installation Guide describes how to install the primary and secondary servers in your high availability deployment. As part of the installation, your administrator configures your HA deployment to use manual or automatic failover. You can check the current failover setting using the `ncs ha status` command or by checking the Health Monitor web page (see Use the Health Monitor Web Page, on page 17).

After the primary and secondary servers are installed, you must perform the HA configuration steps described in How to Configure HA Between the Primary and Secondary Servers, on page 7.

The following topics provide additional information about the HA deployment:

- Using Virtual IP Addressing With HA, on page 7
Using Virtual IP Addressing With HA

A virtual IP address represents the management IP address of the active HA server. During failover or failback, the virtual IP address automatically switches between the two HA servers. This provides two benefits:

- You do not need to know which server is active in order to connect to the Cisco EPN Manager web GUI. Using a virtual IP, your requests are automatically forwarded to the HA server that is active.
- You do not need to configure managed devices to forward notifications to both the primary server and the secondary server. Notifications only need to be forwarded to the virtual IP address.

Virtual IP addressing can be enabled when you configure the secondary server with the primary server. You will need to provide the virtual address (IPv4 or IPv6) that you want both servers to share. See How to Configure HA Between the Primary and Secondary Servers, on page 7.

Using virtual IP addresses does not change the fact that active client-server sessions are terminated when a failover or failback occurs. Even though the virtual IP address will remain available, active client-server sessions (web GUI or NBI) are terminated as the new server begins servicing new requests. Web GUI users will have to log out and back in. For information on handling broken NBI sessions, see the Cisco Evolved Programmable Network Manager MTOSI API Guide for OSS Integration.

Note

To use a virtual IP, the IP addresses of the primary and secondary servers must be on the same subnet.

What If I Cannot Use Virtual IP Addressing?

Depending on the deployment model you choose, not configuring a virtual IP address may result in the administrator having to perform additional steps in order to ensure that syslogs and SNMP notifications are forwarded to the secondary server in case of a failover. The usual method is to configure the devices to forward all syslogs and traps to both servers, usually via forwarding them to a given subnet or range of IP addresses that includes both the primary and secondary server.

This configuration work should be done at the same time HA is being set up: that is, after the secondary server is installed but before HA registration is done on the primary server. It must be completed before a failover so that the chance of losing data is eliminated or reduced. Not using a virtual IP address entails no change to the secondary server install procedure. The primary and secondary servers still need to be provisioned with their individual IP addresses, as normal.

How to Configure HA Between the Primary and Secondary Servers

To enable HA, you must configure HA on the primary server. The primary server needs no configuration during installation in order to participate in the HA configuration. The primary needs to have only the following information:
How to Configure HA Between the Primary and Secondary Servers

- The IP address or host name of the secondary HA server you have already installed and configured (Installing the secondary server is described in the Cisco Evolved Programmable Network Manager Installation Guide.)

- The authentication key you set during installation of the secondary server.

- (Optional) One or more email addresses, to which notifications will be sent.

- The Failover Type (see Automatic Versus Manual Failover, on page 6).

If you plan to use virtual IP addressing (see Using Virtual IP Addressing With HA, on page 7), you will also need to:

- Select the Enable Virtual IP checkbox.

- Specify the IPv4 virtual IP address to be shared by the primary and secondary HA servers. You may also specify an IPv6 virtual IP address, although this is not required.

The following steps explain how to configure HA on the primary server. Follow the same steps when re-configuring HA.

**Step 1**
Log in to Cisco EPN Manager with a user ID and password that has administrator privileges.

**Step 2**
From the menu, select Administration > Settings > High Availability. Cisco EPN Manager displays the HA status page.

**Step 3**
Select HA Configuration and then complete the fields as follows:

a. **Secondary Server**: Enter the IP address or the host name of the secondary server.

   **Note**: We always recommend to use DNS server for resolving the host name to IP address. If you are using the "/etc/hosts" file instead of DNS server, you should enter the secondary IP address instead of host name.

b. **Authentication Key**: Enter the authentication key password you set during the secondary server installation.

c. **Email Address** (Optional): Enter the address (or comma-separated list of addresses) to which notification about HA state changes should be mailed. If you have already configured email notifications using the Mail Server Configuration page (see Forward Alarms and Events as Email Notifications (Administrator Procedure)), the email addresses you enter here will be appended to the list of addresses already configured for the mail server.

d. **Failover Type**: Select either Manual or Automatic. We recommend that you select Manual.

**Step 4**
If you are using the virtual IP feature: Select the Enable Virtual IP checkbox, then complete the additional fields as follows:

a. **IPV4 Virtual IP**: Enter the virtual IPv4 address you want both HA servers to use.

b. **IPV6 Virtual IP**: (Optional) Enter the IPv6 address you want both HA servers to use.

Note that virtual IP addressing will not work unless both servers are on the same subnet.

**Step 5**
Click Check Readiness to ensure if the HA related environmental parameters are ready for the configuration.

For more details, see Check Readiness for HA Configuration, on page 9.

**Note**: The readiness check does not block the HA configuration. You can configure HA even if some of the tests do not pass.
Step 6  Click **Save** to save your changes. Cisco EPN Manager initiates the HA configuration process. When configuration completes successfully, **Configuration Mode** will display the value **HA Enabled**.

**Note**  If FTP or TFTP service is running on the primary server, you must restart the secondary server after the configuration is complete to ensure failover does not fail.

---

**Configure an SSO Server in an HA Environment**

Single Sign-On (SSO) authentication is used to authenticate and manage users in a multi-user, multi-repository environment. SSO is responsible for storing and retrieving the credentials that are used for logging into different systems. You can set up a Cisco EPN Manager as the SSO server for other instances of Cisco EPN Manager.

To configure an SSO server in the high-availability environment, choose one of the procedures listed in the Table 1: SSO Configuration in a HA Deployment. See these topics for more information:

- To configure the SSO server, see Add a RADIUS or TACACS+ Server to Cisco EPN Manager.
- To configure the HA servers, see the Cisco Evolved Programmable Network Manager Installation Guide.

**Table 1: SSO Configuration in a HA Deployment**

<table>
<thead>
<tr>
<th>SSO Configuration</th>
<th>Setup SSO Server</th>
<th>Sever Failover Scenario</th>
<th>SSO Server Failure Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO as a standalone server</td>
<td>1. Configure the standalone SSO server.</td>
<td>When the primary server fails, the secondary server is activated. All machines that are connected to the primary server will be redirected to the secondary server.</td>
<td>When the SSO server fails, SSO functionality is disabled. Cisco EPN Manager will use local authentication.</td>
</tr>
<tr>
<td></td>
<td>2. Configure the primary and secondary HA servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSO on the secondary Server</td>
<td>1. Configure one server to be the SSO server and the primary server (in other words, the primary server will also be the SSO server).</td>
<td>When the primary server fails, the secondary server is activated. All machines that are connected to primary server will not be redirected to the secondary server (because SSO is configured on the primary server).</td>
<td>When the SSO (primary) server fails, the secondary server can be set as the failback option for SSO. This enables all instances to connect to the secondary server. If the secondary server is not set as the SSO server failback option, Cisco EPN Manager will use local authentication.</td>
</tr>
<tr>
<td></td>
<td>2. Configure the secondary HA server.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Check Readiness for HA Configuration**

During the HA configuration, other environmental parameters related to HA like system specification, network configuration and bandwidth between the servers determine the HA configuration.
15 checks are run in the system to ensure the HA configuration completion without any error or failure. The checklist name and the corresponding status with recommendations if any, will be displayed when you run the Check Readiness feature.

**Note**

The Check Readiness does not block the HA configuration. You can configure HA even if some of the checks do not pass.

To check readiness for HA configuration, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to Cisco EPN Manager with a user ID and password that has administrator privileges.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the menu, select <strong>Administration &gt; Settings &gt; High Availability</strong>. Cisco EPN Manager displays the HA status page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>HA Configuration</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Provide the secondary server IP address in the <strong>Secondary Server</strong> field and secondary Authentication Key <strong>Authentication Key</strong> field.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Check Readiness</strong>.</td>
</tr>
</tbody>
</table>

A pop up window with the system specifications and other parameters will be displayed. The screen will show the Checklist Item name, Status, Impact and Recommendation details.

Below, is the list of checklist test name and the description displayed for Check Readiness:

**Table 2: Checklist name and description**

<table>
<thead>
<tr>
<th>Checklist Test Name</th>
<th>Test Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM - CHECK CPU COUNT</td>
<td>Checks the CPU count in both the primary and secondary servers. The CPU count in both servers must meet the requirements.</td>
</tr>
<tr>
<td>SYSTEM - CHECK DISK IOPS</td>
<td>Checks the disk speed in both the primary and secondary servers. The minimum expected disk speed is 200 MBps.</td>
</tr>
<tr>
<td>SYSTEM - CHECK RAM SIZE</td>
<td>Checks the RAM size of both the primary and secondary servers. The RAM size of both servers must meet the requirements.</td>
</tr>
<tr>
<td>SYSTEM - CHECK DISK SIZE</td>
<td>Checks the disk size of both the primary and secondary servers. The disk size of both servers must meet the requirements.</td>
</tr>
<tr>
<td>SYSTEM - CHECK SERVER PING REACHABILITY</td>
<td>Checks that the primary server can reach the secondary server through ping.</td>
</tr>
<tr>
<td>SYSTEM - CHECK OS COMPATABILITY</td>
<td>Checks that the primary server and secondary servers have the same OS version.</td>
</tr>
</tbody>
</table>
### System - Health Monitor Status
Checks whether the health monitor process is running in both the primary and secondary servers.

### Network - Check Network Interface Bandwidth
Checks if the speed of interface eth0 matches the recommended 100 Mbps in both primary and secondary servers.
This test will not measure network bandwidth by transmitting data between primary and secondary server.

### Network - Check Firewall for Database Port Accessibility
Checks if the database port 1522 is open in the system firewall.
If the port is disabled, the test will grant permission for 1522 in the iptables list.

### Database - Check Online Status
Checks if the database files status is online and accessible in both primary and secondary servers.

### Database - Check Memory Target
Checks for "/dev/shm" database memory target size for HA setup.

### Database - Listener Status
Checks if the database listeners are up and running in both primary and secondary servers.
If there is a failure the test will attempt to start the listener and report the status.

### Database - Check Listener Config Corruption
Checks if all the database instances exist under database listener configuration file "listener.ora"

### Database - Check TNS Config Corruption
Checks if all the “WCS” instances exist under database TNS listener configuration file "tnsnames.ora"

### Database - TNS Reachability Status
Checks if TNSPING is successful in both primary and secondary server.

#### Step 6
Once the check is completed for all the parameters, check their status and click **Clear** to close the window.

#### Note
Failback and failover events during **Check Readiness** are forwarded to the Alarms and Events page.
Configuration failure events are not present in the Alarms and Events list.

## How to Patch HA Servers
You can download and install UBF patches for your HA servers in one of the following ways:

- Install the patch on HA servers that are not currently paired. Cisco recommends this method if you have not set up HA for Cisco EPN Manager.
- Install the patch on existing paired HA servers using manual failover. This is the method Cisco recommends if you already have HA set up.
• Install the patch on existing paired HA servers using automatic failover.

For information on each method, see:

**How to Patch New HA Servers**

If you are setting up a new Cisco EPN Manager High Availability (HA) implementation and your new servers are not at the same patch level, follow the steps below to install patches on both servers and bring them to the same patch level.

**Step 1** Download the patch and install it on the primary server:

a) Point your browser to the software patches listing for Cisco EPN Manager.(see Software patches listing for Cisco Evolved Programmable Network Manager)

b) Click the **Download** button for the patch file you need to install (the file name ends with a UBF file extension), and save the file locally.

c) Log in to the primary server using an ID with administrator privileges and choose **Administration > Licenses and Software Updates > Software Update**.

d) Click the **Upload** link at the top of the page and browse to the location where you saved the patch file.

e) Select the UBF file and click **OK** to upload the file.

f) When the upload is complete: On the Software Upload page, verify that the Name, Published Date and Description of the patch file are correct.

g) Select the patch file and click **Install**.

h) Click **Yes** in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.

i) After the installation is complete on the primary server, verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

**Step 2** Install the same patch on the secondary server:

a) Access the secondary server’s Health Monitor (HM) web page by pointing your browser to the following URL:

   **https://ServerIP:8082**

   where **ServerIP** is the IP address or host name of the secondary server.

b) You will be prompted for the secondary server authentication key. Enter it and click **Login**.

c) Click the HM web page’s **Software Update** link. You will be prompted for the authentication key a second time. Enter it and click **Login** again.

d) Click **Upload Update File** and browse to the location where you saved the patch file.

e) Select the UBF file and click **OK** to upload the file.

f) When the upload is complete: On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.

g) Select the patch file and click **Install**.

h) Click **Yes** in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.

i) After the installation is complete on the secondary server, verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

**Step 3** Verify that the patch status is the same on both servers, as follows:
How to Patch Paired HA Servers

If your current Cisco EPN Manager implementation has High Availability servers that are not at the same patch level, or you have a new patch you must install on both your HA servers, follow the steps below.

Patching paired HA servers is not supported. You will receive a popup error message indicating that you cannot perform an update on Cisco EPN Manager servers while HA is configured. So, you must first disconnect the primary and secondary servers before attempting to apply the patch.

1. Follow the steps in Remove HA Via the GUI, on page 35 to disconnect the primary and secondary servers.
2. Follow the steps in How to Patch New HA Servers, on page 12 to apply the patch.
3. Follow the steps in Set Up High Availability, on page 6 to restore your HA configuration.

How to Patch Paired HA Servers Set for Manual Failover

If your current Cisco EPN Manager implementation has High Availability servers that are not at the same patch level, or you have a new patch you must install on both your HA servers, follow the steps below.

You must start the patch install with the primary server in “Primary Active” state and the secondary server in “Secondary Syncing” state.

Patching of primary and secondary HA servers set for manual failover takes approximately 30 minutes, and does not require failover or failback. Patching of the primary and secondary HA servers takes approximately 30 minutes. Downtime during the primary patch installation restart takes 15 to 20 minutes.

In some cases, you may receive a popup error message indicating that you cannot perform an update on Cisco EPN Manager servers while HA is configured. If so, you must first disconnect the primary and secondary servers before attempting to apply the patch. In this case, you cannot use the steps in this procedure. Instead, be sure to:

1. Follow the steps in Remove HA Via the GUI, on page 35 to disconnect the primary and secondary servers.
2. Follow the steps in How to Patch New HA Servers, on page 12 to apply the patch.
3. Follow the steps in Set Up High Availability, on page 6 to restore your HA configuration.

Step 1

Ensure that your HA implementation is enabled and ready for update:

a) Log in to the primary server using an ID with Administrator privileges.
b) Select Administration > Settings > High Availability. The primary server state displayed on the HA Status page should be “Primary Active”.  
c) Select HA Configuration. The current Configuration Mode should show “HA Enabled”. We recommend that you set the Failover Type to “manual” during the patch installation.  
d) Access the secondary server’s Health Monitor (HM) web page by pointing your browser to the following URL:  
https://ServerIP:8082  
where ServerIP is the IP address or host name of the secondary server.  
e) Verify that the secondary server state displayed on the HM web page is in the “Secondary Syncing” state.

Step 2  
You will be prompted for the authentication key entered when HA was enabled. Enter it and click Login.

Step 3  
Download the UBF patch and install it on the primary server:  
a) Point your browser to the software patches listing for Cisco EPN Manager (see Software patches listing for Cisco Evolved Programmable Network Manager).  
b) Click the Download button for the patch file you need to install (the file name ends with a UBF file extension), and save the file locally.  
c) Log in to the primary server using an ID with administrator privileges and choose Administration > Licenses and Software Updates > Software Update.  
d) Click the Upload link at the top of the page and browse to the location where you saved the patch file.  
e) Select the UBF file and click OK to upload the file.  
f) When the upload is complete: On the Software Upload page, verify that the Name, Published Date and Description of the patch file are correct.  
g) Select the patch file and click Install.  
h) Click Yes in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.  
i) After the server restart is complete on the primary server, select Administration > Settings > High Availability, The primary server state displayed on the HA Status page should be “Primary Active”.  
j) Verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

Step 4  
Install the same patch on the secondary server once patching is complete on the primary server:  
a) Access the secondary server’s HM web page and login if needed.  
b) Click the HM web page’s Software Update link. You will be prompted for the authentication key a second time. Enter it and click Login again.  
c) Click Upload Update File and browse to the location where you saved the patch file.  
d) Select the UBF file and click OK to upload the file.  
e) When the upload is complete: On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.  
f) Select the patch file and click Install.  
g) Click Yes in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.  
h) After the server restart is complete on the secondary server, log in to the secondary HM page (https://serverIP:8082) and verify that the secondary server state displayed on the HM web page is “Secondary Syncing”.  
i) Verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

Step 5  
Once the server restart is complete, verify the patch installation as follows:  
a) Log in to the primary server and access its Software Update page as you did in step 2, above. The “Status” column on the Status of Updates > Update tab should show “Installed” for the patch.  
b) Access the secondary server’s Software Update page as you did in step 3, above. The “Status” column on the Status of Updates > Updates tab should show “Installed” for the patch.
For more information, see Software patches listing for Cisco Evolved Programmable Network Manager, Stop and Restart Cisco EPN Manager.

How to Patch Paired HA Servers Set for Automatic Failover

If your current Cisco EPN Manager implementation has High Availability servers that are not at the same patch level, or you have a new patch you must install on both your HA servers, follow the steps below.

You must start the patch install with the primary server in “Primary Active” state and the secondary server in “Secondary Syncing” state.

Patching of primary and secondary HA servers set for automatic failover takes approximately one hour, and requires both failover and failback. Downtime during the failover and failback lasts 10 to 15 minutes.

In some cases, you may receive a popup error message indicating that you cannot perform an update on Cisco EPN Manager servers while HA is configured. If so, you must first disconnect the primary and secondary servers before attempting to apply the patch. In this case, you cannot use the steps in this procedure. Instead, be sure to:

1. Follow the steps in Remove HA Via the GUI, on page 35 to disconnect the primary and secondary servers.
2. Follow the steps in How to Patch New HA Servers, on page 12 to apply the patch.
3. Follow the steps in Set Up High Availability, on page 6 to restore your HA configuration.

Step 1

Ensure that your HA implementation is enabled and ready for update:

a) Log in to the primary server using an ID with Administrator privileges.
b) Select Administration > Settings > High Availability. The primary server state displayed on the HA Status page should be “Primary Active”.
c) Select HA Configuration. The current Configuration Mode should show “HA Enabled”.
d) Access the secondary server’s Health Monitor (HM) web page by pointing your browser to the following URL:
   https://ServerIP:8082
   where ServerIP is the IP address or host name of the secondary server.
e) You will be prompted for the authentication key entered when HA was enabled. Enter it and click Login.
f) Verify that the secondary server state displayed on the HM web page is in the “Secondary Syncing” state.

Step 2

Download the UBF patch and install it on the primary server:

a) Point your browser to the software patches listing for Cisco EPN Manager (see Software patches listing for Cisco Evolved Programmable Network Manager).
b) Click the Download button for the patch file you need to install (the file name ends with a UBF file extension), and save the file locally.
c) Log in to the primary server using an ID with administrator privileges and choose Administration > Licenses and Software Updates > Software Update.
d) Click the upload link at the top of the page and browse to the location where you saved the patch file.
e) Select the UBF file and then click OK to upload the file.
f) When the upload is complete: On the Software Upload page, verify that the Name, Published Date and Description of the patch file are correct.
g) Select the patch file and click Install.

h) Click Yes in the warning pop-up. Failover will be triggered and the primary server will restart automatically. Failover will take 2 to 4 minutes to complete. After the failover is complete, the secondary server will be in “Secondary Active” state.

i) After the primary server is restarted, run the ncs status command to verify that the primary’s processes have re-started. Before you continue, access the primary server’s HM web page and verify that the primary server state displayed is “Primary Syncing”.

Step 3 Failback to the primary using the secondary server’s HM web page:

a) Access the secondary server’s HM web page and login if needed.

b) Click Failback to initiate a failback from the secondary to the primary server. It will take 2 to 3 minutes for the operation to complete. As soon as failback completes, the secondary server will be automatically restarted in the standby mode. It will take a maximum of 15 minutes for the restart to complete, and it will be synched with the primary server.

You can verify the restart by logging into the secondary server’s HM web page and looking for the message “Cisco EPN Manager stopped successfully” followed by “Cisco EPN Manager started successfully.”

After failback is complete, the primary server state will change to “Primary Active”

c) Before continuing: Run the ncs ha status command on both the primary and secondary servers. Verify that the primary server state changes to “Primary Active” and the secondary server state is “Secondary Syncing”.

Step 4 Once failback completes, verify the patch installation by logging in to the primary server and accessing its Software Update page (as you did in step 2, above). The “Status” column on the Status of Updates > Update tab should show “Installed” for the patch.

Step 5 Install the same patch on the secondary server once patching is complete on the primary server:

a) Access the secondary server’s HM web page and login if needed.

b) Click the HM web page’s Software Update link. You will be prompted for the authentication key a second time. Enter it and click Login again.

c) Click Upload Update File and browse to the location where you saved the patch file.

d) Select the UBF file and then click OK to upload the file.

e) When the upload is complete: On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.

f) Select the patch file and click Install.

g) Click Yes in the warning pop-up. The server will restart automatically. The restart typically takes 15 to 20 minutes.

h) After the installation is complete on the secondary server, verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

i) After the server restart is complete on the secondary server, log in to the secondary HM page and verify that the secondary server state displayed on the HM web page is “Secondary Syncing”.

Step 6 Once server restart is complete, verify the patch installation as follows:

a) Log in to the primary server and access its Software Update page as you did in step 2, above. The “Status” column on the Status of Updates > Update tab should show “Installed” for the patch.

b) Access the secondary server’s Software Update page as you did in step 5, above. The “Status” column on the Status of Updates > Updates tab should show “Installed” for the patch.

For more information, see Software patches listing for Cisco Evolved Programmable Network Manager, Stop and Restart Cisco EPN Manager.
Monitor HA Status and Events

These topics describe how to monitor the overall health of the HA environment:

- Use the Health Monitor Web Page, on page 17
- HA Configuration Modes, on page 31
- HA States and Transitions, on page 32
- Check HA Status and Overall Health, on page 19
- View and Customize HA Events, on page 19
- Use HA Error Logging, on page 20

Use the Health Monitor Web Page

The Health Monitor is one of the main components that manage the HA operations. Health Monitor instances run on both servers as an application process, with its own web page on each server. It performs the following functions:

- Synchronizes database and configuration data related to HA (this excludes databases that synchronize separately using Oracle Data Guard).

- Exchanges heartbeat messages between the primary and secondary servers every 5 seconds, to ensure communications are maintained between the servers. If the healthy server does not receive 3 consecutive heartbeats from the other redundant server, it waits for 10 seconds. The healthy server then attempts to open a web URL in the redundant server. If this attempt fails, the healthy server becomes the active server.

- Checks the available disk space on both servers at regular intervals and generates events when storage space runs low.

- Manages, controls, and monitors the overall health of the linked HA servers. If there is a failure on the primary server, the Health Monitor activates the secondary server.

After you have completed HA configuration successfully, you can access the Health Monitor web page from the primary or secondary server by entering the following URL on your browser:

https://ServerIP:8082

where ServerIP is the primary or secondary server’s IP address or host name.

The following example shows a Health Monitor web page for a secondary server in the Secondary Syncing state.
The **Check Readiness** does not block failover to the secondary (either automatic or manual).
Check HA Status and Overall Health

You can use the Cisco EPN Manager web GUI or CLI to check HA status. Either of these approaches will list the state of the server. States are described in HA States and Transitions, on page 32.

To check the HA status from the web GUI, do one of the following:

- From the Cisco EPN Manager web GUI—Choose Administration > Settings > High Availability, then choose HA Status. The current HA status and the event states are displayed.
- From the Health Monitor. See Use the Health Monitor Web Page, on page 17.

To check HA status from the CLI, log into either server as a CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server). The `ncs ha status` command provides a HA-specific output similar to the below example:

```
ncs ha status
```

Use the `ncs status` command to check the Health Monitor and other server processes. You will see an output similar to the following example:

```
ncs status
Health Monitor Server is running. ( [Role] Primary [State] Primary Active )
Database server is running
FTP Service is disabled
TFTP Service is disabled
NMS Server is running.
SAM Daemon is running ... 
DA Daemon is running ...
```

View and Customize HA Events

HA-related alarms are listed in the Alarms and Events table. A list of these alarms is provided in Cisco Evolved Programmable Network Manager Supported Alarms. The following procedure explains how to view these alarms in the web GUI.

If desired, you can also:

- Adjust the severity for these alarms
- Configure notifications for these alarms

For more information, see Work With Server Internal SNMP Traps That Indicate System Problems.

To view HA-related alarms:

1. Choose Monitor > Monitoring Tools > Alarms and Events, then click the Alarms tab.
2. Choose Quick Filter from the Show drop-down list at the top right of the table.
3. In the Message field, enter High Availability.
Use HA Error Logging

To save disk space and maximize performance, HA error logging is disabled by default. If you are having trouble with HA, complete the following procedure to enable error logging and examine the log files.

---

**Step 1** Launch the Health Monitor on the server that is having trouble (see Use the Health Monitor Web Page, on page 17).

**Step 2** In the **Logging** area, select the error-logging level from the **Message Level** drop-down list and then click **Save**.

**Step 3** Download the log files you want to examine:

a. Click **Download**.

   A .zip file is copied to your default download location.

b. Extract the log files and use any ASCII text editor to view them.

---

Trigger Failover

Failover activates the secondary server in response to a failure detected on the primary server.

The Health Monitor detects failure conditions using the heartbeat messages exchanged between the two HA servers. The heartbeat messages are sent every 5 seconds, and if the primary server is not responsive to three consecutive heartbeat messages from the secondary server, the Health Monitor deems the primary server to have failed. During the health check, the Health Monitor also checks the application process status and database health. If there is no proper response to these checks, these are also treated as having failed.

The HA system in the secondary server takes about 15 seconds to detect a process failure on the primary server. If the secondary server is unable to reach the primary server due to a network issue, it might take more time to discover the failure and initiate a failover. In addition, it may take additional time for the application processes on the secondary server to be fully operational.

As soon as the Health Monitor detects a failure, it sends an e-mail notification. The e-mail includes the failure status along with a link to the secondary server's Health Monitor web page. If HA is configured for automatic failover, the secondary server will activate automatically.

To perform a manual failover:

**Before you begin**

- Check the state of the primary and secondary servers.
- Validate the connectivity between the two servers.
- If you are not using virtual IP addresses, make sure all devices are configured to forward traps and syslogs to both servers.

**Step 1** Access the secondary server's Health Monitor web page using the web link given in the email notification, or by entering the following URL on your browser:

https://ServerIP:8082
Step 2   Click Failover.

---

**Trigger Failback**

Failback is the process of re-activating the primary server once it is back online. It also transfers Active status from the secondary server to the primary server, and stops active network monitoring processes on the secondary server.

When a failback is triggered, the secondary server replicates its current database information and updated files to the primary server. The time it takes to complete the failback from the secondary server to the primary server will depend on the amount of data that needs to be replicated and the available network bandwidth.

After the data is replicated successfully, HA changes the state of the primary server to **Primary Active** and the state of the secondary server to **Secondary Syncing**.

During failback, the availability of the secondary server depends on whether the Cisco EPN Manager was reinstalled on the primary server after the failover, as follows:

- If Cisco EPN Manager was reinstalled on the primary server after the failover, a full database copy will be required and the secondary server will not be available during the failback process.
- If Cisco EPN Manager was not reinstalled with primary server, the secondary server is available, except during the period when processes are started on the primary server and stopped on the secondary server. Both servers' Health Monitor web pages are accessible for monitoring the progress of the failback. Additionally, users can also connect to the secondary server to access all normal functionalities.

You must always trigger failback manually, as described in the procedure below. Note:

- Do not initiate configuration or provisioning activity while the failback is in progress.
- After a successful failback, the secondary server will go down and control will switch over to the primary server. During this process, Cisco EPN Manager will be inaccessible to the users for a few moments.

**Before you begin**

- Check the state of the primary and secondary servers.
- Validate the connectivity between the two servers.
- If you are not using virtual IP addresses, make sure all devices are configured to forward traps and syslogs to both servers.
- If you have reinstalled Cisco EPN Manager on the primary server and you are using offline geo maps, you must reinstall the geo maps resources on the primary server before triggering failback. See the **Cisco Evolved Programmable Network Manager Installation Guide**.

---

**Step 1**   Access the secondary server's Health Monitor web page using the link given in the e-mail notification, or by entering the following URL on your browser:

https://ServerIP:8082

**Step 2**   Click Failback.
Respond to Other HA Events

All the HA related events are displayed on the HA Status page, the Health Monitor web pages, and under the Cisco EPN Manager Alarms and Events page. Most events require no response from you other than triggering failover and failback. A few events are more complex, as explained in the following topics:

- HA Registration Fails, on page 22
- Network is Down (Automatic Failover), on page 23
- Network is Down (Manual Failover), on page 23
- Process Restart Fails (Automatic Failover), on page 25
- Process Restart Fails (Manual Failover), on page 26
- Primary Server Restarts During Synchronization (Manual Failover), on page 27
- Secondary Server Restarts During Synchronization, on page 27
- Both HA Servers Are Down, on page 27
- Both HA Servers Are Powered Down, on page 28
- Both HA Servers Are Down and Secondary Server Will Not Restart, on page 28
- How to Replace the Primary Server, on page 29
- How to Recover From Split-Brain Scenario, on page 30
- Secondary Server Goes Down, on page 30
- How to Resolve Database Synchronization Issues, on page 31

HA Registration Fails

If HA registration fails, you will see the following HA state-change transitions for each server:

<table>
<thead>
<tr>
<th>Primary HA State Transitions</th>
<th>Secondary HA State Transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: HA Initializing</td>
<td>From: HA Initializing</td>
</tr>
<tr>
<td>To: HA Not Configured</td>
<td>To: HA Not Configured</td>
</tr>
</tbody>
</table>

To recover from failed HA registration, follow the steps below.

**Step 1**
Use ping and other tools to check the network connection between the two Cisco EPN Manager servers. Confirm that the secondary server is reachable from the primary, and vice versa.

**Step 2**
Check that the gateway, subnet mask, virtual IP address (if configured), server hostname, DNS, NTP settings are all correct.

**Step 3**
Check that the configured DNS and NTP servers are reachable from the primary and secondary servers, and that both are responding without latency or other network-specific issues.

**Step 4**
Check that all Cisco EPN Manager licenses are correctly configured.

**Step 5**
Once you have remedied any connectivity or setting issues, retry the steps in How to Configure HA Between the Primary and Secondary Servers, on page 7.
Network is Down (Automatic Failover)

If there is a loss of network connectivity between the two Cisco EPN Manager servers, you will see the following HA state-change transitions for each server, assuming that the Failover Type is set to “Automatic”:

<table>
<thead>
<tr>
<th>Primary HA State Transitions</th>
<th>Secondary HA State Transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Active</td>
<td>From: Secondary Syncing</td>
</tr>
<tr>
<td>To: Primary Lost Secondary</td>
<td>To: Secondary Lost Primary</td>
</tr>
<tr>
<td>To: Primary Lost Secondary</td>
<td>To: Secondary Failover</td>
</tr>
<tr>
<td>To: Primary Lost Secondary</td>
<td>To: Secondary Active</td>
</tr>
</tbody>
</table>

You will get an email notification that the secondary is active.

Step 1

Check on and restore network connectivity between the two servers. Once network connectivity is restored and the primary server can detect that the secondary is active, all services on the primary will be restarted and made passive automatically. You will see the following state changes:

<table>
<thead>
<tr>
<th>Primary HA State Transitions</th>
<th>Secondary HA State Transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Lost Secondary</td>
<td>From: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Failover</td>
<td>To: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Syncing</td>
<td>To: Secondary Active</td>
</tr>
</tbody>
</table>

Step 2

Trigger a failback from the secondary to the primary. You will then see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions</th>
<th>Secondary HA State Transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Syncing</td>
<td>From: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Failback</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Post Failback</td>
</tr>
<tr>
<td>To: Primary Active</td>
<td>To: Secondary Syncing</td>
</tr>
</tbody>
</table>

Network is Down (Manual Failover)

If there is a loss of network connectivity between the two Cisco EPN Manager servers, you will see the following HA state-change transitions for each server, assuming that the Failover Type is set to “Manual”:

<table>
<thead>
<tr>
<th>Primary HA State Transitions</th>
<th>Secondary HA State Transitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Active</td>
<td>From: Secondary Syncing</td>
</tr>
</tbody>
</table>
You will get email notifications that each server has lost the other.

**Step 1**
Check on and, if needed, restore the network connectivity between the two servers.

You will see the following state changes once network connectivity is restored:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Lost Secondary</td>
<td>From: Secondary Lost Primary</td>
</tr>
<tr>
<td>To: Primary Active</td>
<td>To: Secondary Syncing</td>
</tr>
</tbody>
</table>

No administrator response is required.

**Step 2**
If network connection cannot be restored for any reason, use the HM web page for the secondary server to trigger a failover from the primary to the secondary server. You will see the following state changes:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Lost Secondary</td>
<td>From: Secondary Lost Primary</td>
</tr>
<tr>
<td>To: Primary Lost Secondary</td>
<td>To: Secondary Failover</td>
</tr>
<tr>
<td>To: Primary Failover</td>
<td>To: Secondary Active</td>
</tr>
</tbody>
</table>

You will get an email notification that the secondary server is now active.

**Step 3**
Check and restore network connectivity between the two servers. Once network connectivity is restored and the primary server detects that the secondary server is active, all services on the primary server will be restarted and made passive. You will see the following state changes:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Lost Secondary</td>
<td>From: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Failover</td>
<td>To: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Syncing</td>
<td>To: Secondary Active</td>
</tr>
</tbody>
</table>

**Step 4**
Trigger a failback from the secondary to the primary.

You will then see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Syncing</td>
<td>From: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Failback</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Post Failback</td>
</tr>
</tbody>
</table>
Process Restart Fails (Automatic Failover)

The Cisco EPN Manager Health Monitor process is responsible for attempting to restart any Cisco EPN Manager server processes that have failed. Generally speaking, the current state of the primary and secondary servers should be “Primary Active” and “Secondary Syncing” at the time any such failures occur.

If HM cannot restart a critical process on the primary server, then the primary server is considered to have failed. If your currently configured Failover Type is “automatic”, you will see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Active</td>
<td>From: Secondary Syncing</td>
</tr>
<tr>
<td>To: Primary Uncertain</td>
<td>To: Secondary Lost Primary</td>
</tr>
<tr>
<td>To: Primary Failover</td>
<td>To: Secondary Failover</td>
</tr>
<tr>
<td>To: Primary Failover</td>
<td>To: Secondary Active</td>
</tr>
</tbody>
</table>

When this process is complete, you will get an email notification that the secondary server is now active.

Step 1

Restart the primary server and ensure that it is running. Once the primary is restarted, it will be in the state “Primary Syncing”. You will see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Failover</td>
<td>From: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Preparing for Failback</td>
<td>To: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Syncing</td>
<td>To: Secondary Active</td>
</tr>
</tbody>
</table>

Step 2

Trigger a failback from the secondary to the primary. You will then see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Syncing</td>
<td>From: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Failback</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Post Failback</td>
</tr>
<tr>
<td>To: Primary Active</td>
<td>To: Secondary Syncing</td>
</tr>
</tbody>
</table>
Process Restart Fails (Manual Failover)

The Cisco EPN Manager Health Monitor process is responsible for attempting to restart any Cisco EPN Manager server processes that have failed. Generally speaking, the current state of the primary and secondary servers should be “Primary Active” and “Secondary Syncing” at the time any such failures occur. If HM cannot restart a critical process on the primary server, then the primary server is considered to have failed. You will receive an email notification of this failure. If your currently configured Failover Type is “Manual”, you will see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Active</td>
<td>From: Secondary Syncing</td>
</tr>
<tr>
<td>To: Primary Uncertain</td>
<td>To: Secondary Lost Primary</td>
</tr>
</tbody>
</table>

**Step 1**
Trigger on the secondary server a failover from the primary to the secondary. You will then see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Uncertain</td>
<td>From: Secondary Syncing</td>
</tr>
<tr>
<td>To: Primary Failover</td>
<td>To: Secondary Failover</td>
</tr>
<tr>
<td>To: Primary Failover</td>
<td>To: Secondary Active</td>
</tr>
</tbody>
</table>

**Step 2**
Restart the primary server and ensure that it is running. Once the primary server is restarted, the primary’s HA state will be “Primary Syncing”. You will see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Failover</td>
<td>From: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Preparing for Failback</td>
<td>To: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Syncing</td>
<td>To: Secondary Active</td>
</tr>
</tbody>
</table>

**Step 3**
Trigger a failback from the secondary to the primary. You will then see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Syncing</td>
<td>From: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Failback</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Post Failback</td>
</tr>
<tr>
<td>To: Primary Active</td>
<td>To: Secondary Syncing</td>
</tr>
</tbody>
</table>
Primary Server Restarts During Synchronization (Manual Failover)

If the primary Cisco EPN Manager server is restarted while the secondary server is syncing, you will see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Active</td>
<td>From: Secondary Syncing</td>
</tr>
<tr>
<td>To: Primary Alone</td>
<td>To: Secondary Lost Primary</td>
</tr>
<tr>
<td>To: Primary Active</td>
<td>To: Secondary Syncing</td>
</tr>
</tbody>
</table>

The “Primary Alone” and “Primary Active” states occur immediately after the primary comes back online. No administrator response should be required.

Secondary Server Restarts During Synchronization

If the secondary Cisco EPN Manager server is restarted while syncing with the primary server, you will see the following state transitions:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: Primary Active</td>
<td>From: Secondary Syncing</td>
</tr>
<tr>
<td>To: Primary Lost Secondary</td>
<td>From: Secondary Lost Primary</td>
</tr>
<tr>
<td>To: Primary Active</td>
<td>To: Secondary Syncing</td>
</tr>
</tbody>
</table>

No administrator response should be required.

Both HA Servers Are Down

If both the primary and secondary servers are down at the same time, you can recover by bringing them back up in the correct order, as explained in the steps below.

**Step 1**
Restart the secondary server and the instance of Cisco EPN Manager running on it. If for some reason you cannot restart the secondary server, see Both HA Servers Are Down and Secondary Server Will Not Restart, on page 28.

**Step 2**
When Cisco EPN Manager is running on the secondary, access the secondary server’s Health Monitor web page. You will see the secondary server transition to the state “Secondary Lost Primary”.

**Step 3**
Restart the primary server and the instance of Cisco EPN Manager running on it. When Cisco EPN Manager is running on the primary, the primary will automatically sync with the secondary. To verify this, access the primary server’s Health Monitor web page. You will see the two servers transition through the following series of HA states:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>To: Primary Lost Secondary</td>
<td>To: Secondary Lost Primary</td>
</tr>
</tbody>
</table>
Both HA Servers Are Powered Down

If both the primary and secondary servers are powered down at the same time, you can recover by bringing them back up in the correct order, as explained in the steps below.

### Step 1
Power on the secondary server and the Cisco EPN Manager instance running on it. The secondary HA restart will fail at this state because the primary server is not reachable. However, the secondary server's HM process will be running (with an error).

### Step 2
When Cisco EPN Manager is running on the secondary server, access the secondary server's HM web page (see Use the Health Monitor Web Page, on page 17). You will see the secondary server transition to the **Secondary Lost Primary** state.

### Step 3
Power on the primary server and the Cisco EPN Manager instance running on it.

### Step 4
When Cisco EPN Manager is running on the primary server, the primary server will automatically begin syncing with the secondary server. To verify this, access the primary server's HM web page. You will see the two servers transition through the following series of HA states:

<table>
<thead>
<tr>
<th>Primary HA State Transitions...</th>
<th>Secondary HA State Transitions...</th>
</tr>
</thead>
<tbody>
<tr>
<td>To: Primary Lost Secondary</td>
<td>To: Secondary Lost Primary</td>
</tr>
<tr>
<td>To: Primary Active</td>
<td>To: Secondary Syncing</td>
</tr>
</tbody>
</table>

### Step 5
Restart the secondary server and the Cisco EPN Manager instance running on it. This is required because not all processes will be running on the secondary server at this point.

If for some reason you cannot restart the secondary server, see Both HA Servers Are Down and Secondary Server Will Not Restart, on page 28.

### Step 6
When Cisco EPN Manager finishes restarting on the secondary server, all processes should be running. Verify this by running the `ncs ha status` command.

---

Both HA Servers Are Down and Secondary Server Will Not Restart

If both HA servers are down at the same time and the secondary server will not restart, you will need to remove the HA configuration from the primary server in order to use it as a standalone server until you can replace or restore the secondary server.

The following steps assume that you have already tried and failed to restart the secondary server.

### Step 1
Attempt to restart the primary instance of Cisco EPN Manager. If the primary server is able to restart at all, the restart will abort with an error message indicating that you must remove the HA configuration.
Step 2  Open a CLI session with the primary server (see Establish an SSH Session With the Cisco EPN Manager Server).
Step 3  Enter the following command to remove the HA configuration on the primary server:
ncs ha remove
Step 4  Confirm that you want to remove the HA configuration.

You should now be able to restart the primary instance of Cisco EPN Manager without receiving an error message, and use it as a standalone server. When you are able to restore or replace the secondary server, proceed as explained in How to Configure HA Between the Primary and Secondary Servers, on page 7.

How to Replace the Primary Server

Under normal circumstances, the state of your primary server will be **Primary Active** and your secondary server will be **Secondary Syncing**. If the primary server fails for any reason, a failover to the secondary will take place (automatically or manually).

You may find that restoring full HA access requires you to reinstall the primary server using new hardware. If this happens, you can follow the steps below to bring up the new primary server without losing any data.

**Before you begin**

Make sure you have the password (authentication key) that was set when HA was configured on the secondary server. You will need it for this procedure.

---

**Step 1**  Ensure that the secondary server is in the **Secondary Active** state. If the primary server is configured for manual failover, you will need to trigger failover to the secondary server (see Trigger Failover, on page 20).

**Step 2**  Ensure that the old primary server you are replacing has been disconnected from the network.

**Step 3**  Ensure that the new primary server is ready for use. This will include connecting it to the network and configuring it similar to the old primary server (IP address, subnet mask, and so forth). You will need to enter the same authentication key that you entered when installing HA on the secondary server.

**Step 4**  Ensure that both the primary and secondary servers are at the same patch level.

**Step 5**  Trigger a failback from the secondary server to the newly-installed primary server. During failback to the new primary HA server, a full database copy will be performed, so this operation will take time to complete depending on the available bandwidth and network latency. You will see the two servers transition through the following series of HA states:

<table>
<thead>
<tr>
<th><strong>Primary HA State Transitions</strong></th>
<th><strong>Secondary HA State Transitions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>From: HA not configured</td>
<td>From: Secondary Active</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Failback</td>
</tr>
<tr>
<td>To: Primary Failback</td>
<td>To: Secondary Post Failback</td>
</tr>
<tr>
<td>To: Primary Active</td>
<td>To: Secondary Syncing</td>
</tr>
</tbody>
</table>
How to Recover From Split-Brain Scenario

In a split-brain scenario, both the primary and secondary servers become active at the same time, perhaps due to a network outage or a link that temporarily goes down. However, because the primary server constantly checks the secondary server, when the connection is reestablished, the primary server will go down due to the secondary server being active.

The possibility of data loss always exists on the rare occasions when a “split-brain scenario” occurs. In this case, you can choose to save the newly added data on the secondary and forget the data that was added on the primary, as explained in the following steps.

---

### Step 1
Once the network is up, and the secondary server is up, the primary will restart itself automatically, using its standby database. The HA status of the primary server will be, first, “Primary Failover” transitioning to “Primary Syncing”. You can verify this by logging on to the primary server’s Health Monitor web page.

### Step 2
Once the primary server’s status is “Primary Syncing, confirm that a user can log into the secondary server’s Cisco EPN Manager page using the web browser (for example, https://server-ip-address:443). Do not proceed until you have verified this.

### Step 3
Once access to the secondary is verified, initiate a failback from the secondary server's Health Monitor web page (see Trigger Failback, on page 21 ). You can continue to perform monitoring activities on the secondary server until the switchover to the primary is completed.

---

Secondary Server Goes Down

In this scenario, the secondary server is acting as a standby server and it goes down.

To get the secondary server up and running again:

---

### Step 1
Power on the secondary server.

### Step 2
Start Cisco EPN Manager on the secondary server.

### Step 3
On the primary server, verify that the primary server's HA status changes from "Primary Lost Secondary" to "Primary Active." Go to Administration > Settings > High Availability > HA Configuration.

### Step 4
Log into the secondary server's Health Monitor page by entering the following URL in your browser: https://serverIP:8082.

### Step 5
Verify that the secondary server's HA status changes from "Secondary Lost Primary" to "Secondary Syncing."
No further action is required once the above statuses are displayed. However, if the HA status does not change, the secondary server cannot be recovered automatically. In this case, continue with the following steps.

### Step 6
Remove the HA configuration on the primary server. Go to Administration > Settings > High Availability > HA Configuration and click Remove.

### Step 7
Register the secondary server with the primary server. See How to Configure HA Between the Primary and Secondary Servers, on page 7.
If HA registration is successful, no further action is required. However, if HA registration is unsuccessful, it indicates that the secondary server might have suffered hardware/software loss. In this case, continue with the following steps.

### Step 8
Remove the HA configuration on the primary server.

### Step 9
Reinstall the secondary server with the same release and patches (if any) as the primary server.
Step 10 Register the secondary server with the primary server. See How to Configure HA Between the Primary and Secondary Servers, on page 7.

How to Resolve Database Synchronization Issues

To resolve the database synchronization issue, when the primary server is in "Primary Active" state and the secondary server is in "Secondary Syncing" state, do the following:

Step 1 Remove HA, see Remove HA Via the CLI, on page 35 and Remove HA Via the GUI, on page 35.
Step 2 After both the primary and secondary servers reaches "HA not configured" state, perform the HA configuration. See Set Up High Availability, on page 6.

High Availability Reference Information

The following topics provide reference information on HA:

- HA Configuration Modes, on page 31
- HA States and Transitions, on page 32
- High Availability CLI Command Reference, on page 34
- Reset the HA Authentication Key, on page 34
- Remove HA Via the CLI, on page 35
- Remove HA Via the GUI, on page 35
- Remove HA During Upgrade, on page 35
- Remove HA During Restore, on page 36
- Use HA Error Logging, on page 20
- Reset the Server IP Address or Host Name, on page 36

HA Configuration Modes

HA configuration modes represent the overall status of the complete HA configuration (as opposed to HA states, which are specific to a server).

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Not Configured</td>
<td>HA is not configured on this server.</td>
</tr>
<tr>
<td>HA Initializing</td>
<td>HA configuration process between the primary and secondary servers has started.</td>
</tr>
<tr>
<td>HA Enabled</td>
<td>HA is enabled between the primary and secondary servers.</td>
</tr>
</tbody>
</table>
HA States and Transitions

The following table lists the HA states, including those that require no response from you. You can view these states from the HA Status page (Administration > Settings > High Availability > HA Status) or from the Health Monitor. For a list of HA events and instructions for enabling, disabling, and adjusting them, see Customize Server Internal SNMP Traps and Forward the Traps.

<table>
<thead>
<tr>
<th>State</th>
<th>Server</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Alone</td>
<td>Both</td>
<td>Server is running alone because one of the servers is down, out of sync, or unreachable.</td>
</tr>
<tr>
<td>Stand Alone</td>
<td>Both</td>
<td>HA is not configured on this server.</td>
</tr>
<tr>
<td>Primary Alone</td>
<td>Primary</td>
<td>Primary server has restarted after it lost the secondary server (only Health Monitor is running in this state).</td>
</tr>
<tr>
<td>HA Initializing</td>
<td>Both</td>
<td>HA configuration process between the primary and secondary server has started.</td>
</tr>
<tr>
<td>Primary Active</td>
<td>Primary</td>
<td>Primary server is now active and is synchronizing with the secondary server.</td>
</tr>
<tr>
<td>Primary Database Copy Failed</td>
<td>Primary</td>
<td>Restarted primary server detected a data gap, triggered a data copy from the active secondary server, and the database copy failed. When a primary server is restarted, it always checks to see if a data gap has occurred due to the primary server being down for 24 hours or more. This copy rarely fails but if it occurs, all attempts to failback to the primary are blocked until the database copy completes successfully. As soon as it does, the primary state is set to Primary Syncing.</td>
</tr>
<tr>
<td>Primary Failover</td>
<td>Primary</td>
<td>Primary server detected a failure.</td>
</tr>
<tr>
<td>Primary Failback</td>
<td>Primary</td>
<td>User-triggered failback is currently in progress.</td>
</tr>
<tr>
<td>Primary Lost Secondary</td>
<td>Primary</td>
<td>Primary server is unable to communicate with the secondary server.</td>
</tr>
<tr>
<td>Primary Preparing for Failback</td>
<td>Primary</td>
<td>Primary server has started up in standby mode after a failover (because the secondary server is still active). When the primary server is ready for failback, its state will be set to Primary Syncing.</td>
</tr>
<tr>
<td>Primary Syncing</td>
<td>Primary</td>
<td>Primary server is synchronizing the database and configuration files from the active secondary server. This occurs after a failover, when primary processes are brought up (and the secondary server is playing the active role).</td>
</tr>
<tr>
<td>Primary Uncertain</td>
<td>Primary</td>
<td>Primary server's application processes are not able to connect to its database.</td>
</tr>
<tr>
<td>Secondary Alone</td>
<td>Secondary</td>
<td>Primary server is not reachable from secondary server after a primary server restart.</td>
</tr>
</tbody>
</table>
Secondary server is synchronizing the database and configuration files from the primary server.

Failover from the primary server to the secondary server has completed successfully.

Secondary server is not able to connect to the primary server (occurs when the primary fails or network connectivity is lost).

For automatic failover, the secondary server will automatically move to the Secondary Active state. For Manual failover, you must trigger the failover to make the secondary server active (see Trigger Failover, on page 20).

Secondary triggered and is in progress.

Secondary Failback triggered and database and file replication is in progress.

Secondary triggered; associated process stops and restarts are in progress. Database and configuration files have been replicated from the secondary server to the primary server. The primary server status will change to Primary Active, and the secondary server HA status will change to Secondary Syncing.

Secondary server's application processes cannot connect to the server's database.

The following figure illustrates the primary server HA state changes.

This figure illustrates the secondary server HA state changes.
The following table lists the CLI commands available for HA management. You must be logged in as the admin CLI user to use these commands. The output reflects the status of the server you are using. In other words, if you run `ncs ha status` from the primary server, Cisco EPN Manager reports the status of the primary server.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ncs ha ?</td>
<td>Displays the command usage message.</td>
</tr>
<tr>
<td>ncs ha authkey newAuthkey</td>
<td>Updates the authentication key to newAuthKey.</td>
</tr>
<tr>
<td>ncs ha remove</td>
<td>Removes the HA configuration.</td>
</tr>
<tr>
<td>ncs ha status</td>
<td>Displays the current status for HA.</td>
</tr>
</tbody>
</table>

**High Availability CLI Command Reference**

Users with administrator privileges can change the HA authentication key using the `ha authkey` command. You will need to ensure that the new authorization key meets the password standards.

**Step 1** Log in to the primary server as a Cisco EPN Manager CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server).

**Step 2** Enter the following at the command line:

```
ha authkey newAuthKey
```
Where newAuthKey is the new authorization key.

---

### Remove HA Via the GUI

The simplest method for removing an existing HA implementation is via the GUI, as shown in the following steps. You can also remove the HA setup via the command line.

Note that, to use this method, you must ensure that the primary Cisco EPN Manager server is currently in the “Primary Active” state. If for any reason the secondary server is currently active, perform a failback and then try to remove the HA configuration after the failback is complete and the secondary’s automatic restart has finished.

**Step 1**
Log in to the primary Cisco EPN Manager server with a user ID that has administrator privileges.

**Step 2**
Select Administration > Settings > High Availability > HA Configuration.

**Step 3**
Select Remove. Removing the HA configuration takes from 3 to 4 minutes.

Once the removal is complete, ensure that the HA configuration mode displayed on the page now reads “HA Not Configured”.

### Remove HA Via the CLI

If for any reason you cannot access the Cisco EPN Manager GUI on the primary server, administrators can remove the HA setup via the command line, using the steps below.

Note that, to use this method, you must ensure that the primary Cisco EPN Manager server is currently in the “Primary Active” state. If for any reason the secondary server is currently active, perform a failback and then try to remove the HA configuration after the failback is complete and the secondary’s automatic restart has finished.

**Step 1**
Connect to the primary server via CLI. Do not enter “configure terminal” mode.

**Step 2**
Enter the following at the command line:

```
admin# ncs ha remove.
```

### Remove HA During Upgrade

To upgrade a Cisco EPN Manager implementation that uses HA, follow the steps below.

**Step 1**
Use the GUI to remove the HA settings from the primary server. See Remove HA Via the GUI, on page 35.

**Step 2**
Upgrade the primary server as needed.

**Step 3**
Re-install the secondary server using the current image.
Note that upgrading the secondary server from the previous version or a beta version is not supported. The secondary server must always be a fresh installation.

**Step 4** Once the upgrade is complete, perform the HA configuration process again.

---

**Remove HA During Restore**

Cisco EPN Manager does not back up configuration settings related to high availability. If you are restoring an implementation that is using HA, you should only restore data to the primary server. The restored primary server will automatically replicate its data to the secondary server. If you try to run a restore on a secondary server, Cisco EPN Manager will generate an error message.

Follow these steps when restoring an implementation that uses HA:

1. Use the GUI to remove the HA settings from the primary server. See Remove HA Via the GUI, on page 35.
2. Restore data on the primary server. See Restore Cisco EPN Manager Data.
3. When the restore process is complete, perform the HA configuration process again. See How to Configure HA Between the Primary and Secondary Servers, on page 7.

---

**Reset the Server IP Address or Host Name**

Avoid changing the IP address or hostname of the primary or secondary server, if possible. If you must change the IP address or hostname, remove the HA configuration from the primary server before making the change. When finished, re-register HA.