



Configure High Availability

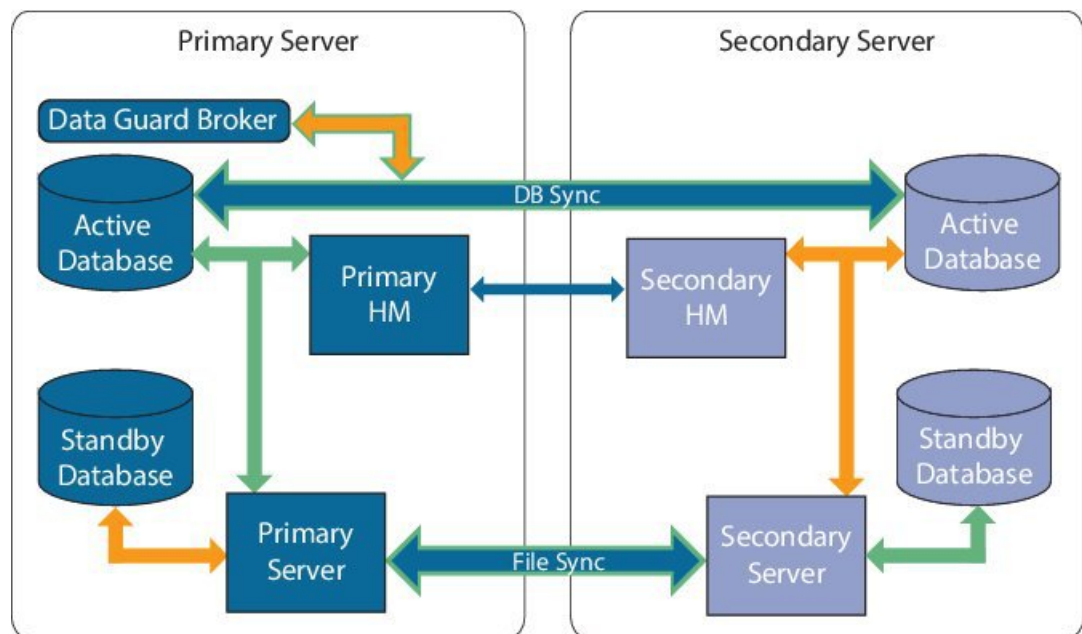
- [How High Availability Works, page 1](#)
- [Set Up High Availability, page 5](#)
- [Monitor HA Status and Events, page 11](#)
- [Trigger Failover, page 14](#)
- [Trigger Failback, page 15](#)
- [Common Failover/Failback Scenarios, page 16](#)
- [High Availability CLI Command Reference, page 21](#)

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 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.
- **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.

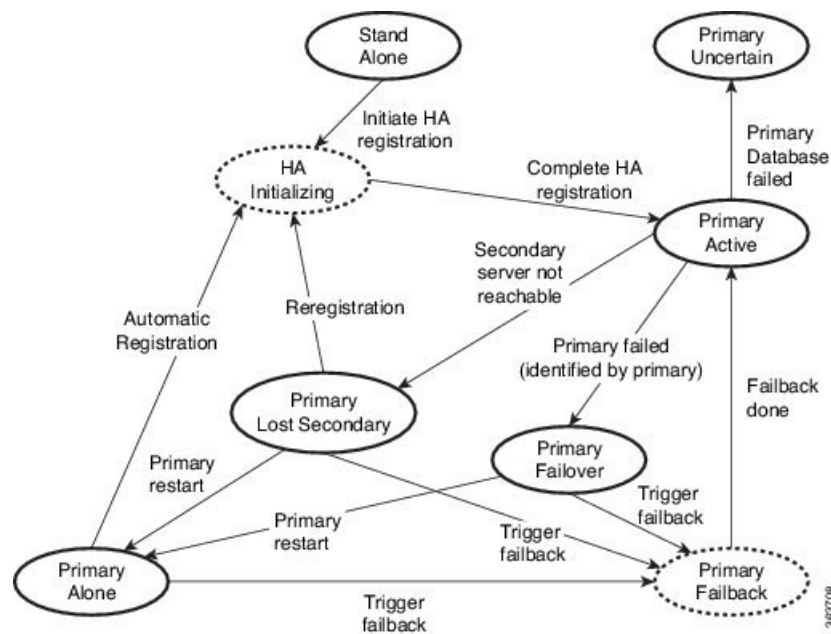
HA States and Transitions

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](#).

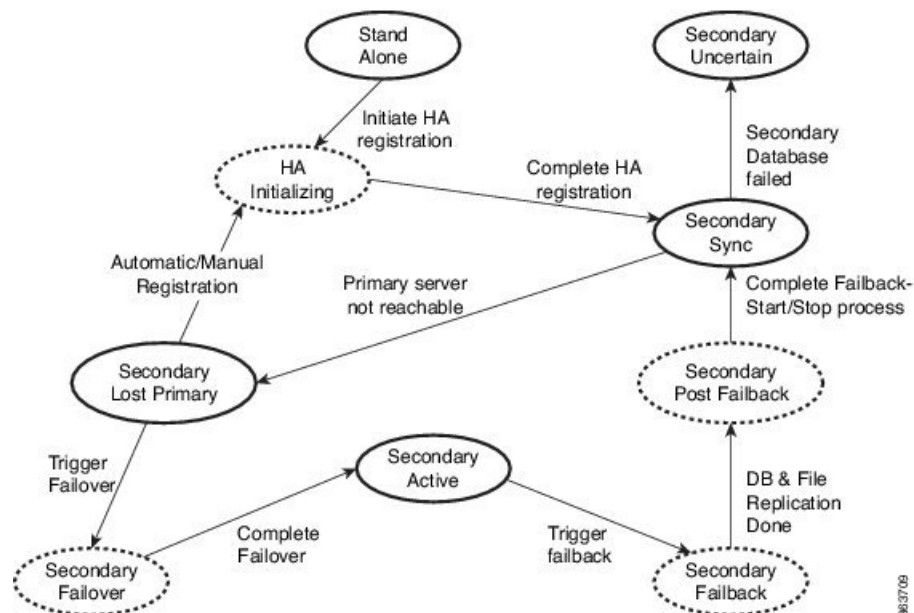
State	Server	Description
Stand Alone	Both	HA is not configured on this server
Primary Alone	Primary	Primary restarted after it lost secondary (only Health Monitor is running in this state).
HA Initializing	Both	HA Registration process between the primary and secondary server has started.
Primary Active	Primary	Primary server is now active and is synchronizing with secondary server.
Primary Database Copy Failed	Primary	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 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 .
Primary Failover	Primary	Primary server detected a failure.
Primary Failback	Primary	User-triggered failback is currently in progress.
Primary Lost Secondary	Primary	Primary server is unable to communicate with the secondary server.
Primary Preparing for Failback	Primary	Primary 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 .

Primary Syncing	Primary	Primary server is synchronizing the database and configuration files from the active secondary. This occurs after a failover, when primary processes are brought up (and the secondary is playing the active role).
Primary Uncertain	Primary	Primary server's application processes are not able to connect to its database.
Secondary Alone	Secondary	Primary server is not reachable from secondary server after a primary server restart.
Secondary Syncing	Secondary	Secondary server is synchronizing the database and configuration files from the primary.
Secondary Active	Secondary	Failover from the primary server to the secondary server has completed successfully.
Secondary Lost Primary	Secondary	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 will automatically move to the Secondary Active state. For Manual failover, you must trigger the failover to make the secondary active (see Trigger Failover, on page 14).
Secondary Failover	Secondary	Failover triggered and is in progress.
Secondary Failback	Secondary	Failback triggered and database and file replication is in progress.
Secondary Post Failback	Secondary	Failback 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 Uncertain	Secondary	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.



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 11).

After the primary and secondary servers are installed, you must perform the HA registration steps described in [Register the Secondary Server for HA](#), on page 7.

The following topics describe additional setup tasks you may need to perform when managing your HA deployment.

- [Configure an SSO Server in a High Availability Environment](#), on page 9
- [Reset the HA Authentication Key](#), on page 10
- [Reset the Server IP Address or Host Name](#), on page 10

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 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 register 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 [Register the Secondary Server for HA](#), 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 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.

Register the Secondary Server for HA

These topics describe the HA registration process:

- [What Happens During Secondary Server Registration, on page 7](#)
- [Register the Secondary Server on the Primary Server, on page 7](#)
- [Troubleshoot an HA Registration Failure, on page 9](#)

What Happens During Secondary Server Registration

After the secondary server is registered on the primary server, Cisco EPN Manager copies all database and configuration data from the primary to the secondary server. The length of this process depends on the amount of database and configuration data, and the available bandwidth on the network link between the two servers. The bigger the data and the slower the link, the longer the replication will take.

Cisco EPN Manager initiates synchronization between the primary and the secondary HA servers. The synchronization should not have any impact on user activity, although users may observe slow system response until the synchronization is complete. There is no impact on the execution of user- or system-related activity during the sync.

When Cisco EPN Manager is replicating the database, the secondary server itself will be in passive mode (and in the **Secondary Syncing** state), but all processes on the secondary server will be running. For example, if you execute the CLI command **ncs status** on the secondary server, the command output will show all processes as running.

Register the Secondary Server on the Primary Server

After installing the secondary server, you must register it on the primary server. The registration steps must be performed from the primary server. (Installing the secondary server is described in the [Cisco Evolved Programmable Network Manager Installation Guide](#).)

Before You Begin

- Log in as the Linux CLI admin user and stop and restart the primary and secondary servers by running the "ncs stop" and "ncs start" commands. Check that the services are up and running on both servers by running the "ncs status" command.
- If you are not using virtual IP addresses, make sure devices are configured to forward traps and syslogs to both the primary and secondary server. (For information on using virtual IP addresses with HA, see the [Cisco Evolved Programmable Network Manager Installation Guide](#). That guide explains any restrictions—for example, both servers must be on the same subnet to use virtual IP addresses.)

**Note**

If you choose to deploy the primary and secondary servers on the same IP subnet, you can configure your devices to send notifications to Cisco EPN Manager at a single virtual IP address. If you choose to disperse the two servers geographically, such as to facilitate disaster recovery, you will need to configure your devices to send notifications to both servers.

- Make sure you have the following information:
 - IP address or host name of the secondary server
 - Password (authentication key) that was specified when installing the secondary server
 - An e-mail address for HA state change notifications
 - The preferred failover type (manual is recommended to avoid failovers that result from intermittent network outages)
- A web GUI user ID that has administrator privileges and access to ROOT-DOMAIN.

-
- Step 1** On the primary server, log into the Cisco EPN Manager web GUI with a user ID that has administrator privileges.
- Step 2** Choose **Administration > Settings > High Availability**, then choose **HA Configuration**.
- Step 3** In the **General** area, complete the **Authentication Key**, **Email Address**, **Failover Type**, and **Secondary Server** fields. For the **Email Address** field, you can enter a comma-separated list of addresses to which notifications should be mailed. If you already configured email notifications, the email addresses you enter here will be appended to the list of addresses already configured (see [Forward Alarms and Events as Email Notifications \(Administrator Procedure\)](#)).
- Step 4** (If you are using the virtual IP feature) Check the **Virtual IP** check box, and then enter the virtual IPv4 or IPv6 address you want both servers to use.
- Step 5** Click **Save** to save your changes and initiate the HA registration process.
- Step 6** On the HA Configuration page, ensure that the **Configuration Mode** field displays the value **HA Enabled** to verify that the registration is successful. You can now log in to the Health Monitor.
-

What to Do Next

Monitor the server state changes that are listed in the following table. On the primary server's HA Status page, click **Refresh** to view the progress. (You can also view the status from either server using the Health Monitor web page.)

Server	Expected State Transitions
Primary	Stand Alone to HA Initializing to Primary Active
Secondary	Stand Alone to HA Initializing to Secondary Syncing

Troubleshoot an HA Registration Failure

You can tell that registration has failed if the state of both the servers changes from **HA Initializing** to **Stand Alone**.

To recover from failed HA registration:

-
- Step 1** Use ping and other tools to check the network connectivity between the two 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, and NTP settings are all correct.
 - Step 3** Check that configured DNS, NTP, and SSO 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 the required device and feature licenses are installed on the primary server.
-

What to Do Next

Once you have remedied any connectivity or setting issues, retry the steps in [Register the Secondary Server on the Primary Server](#), on page 7.

Configure an SSO Server in a High Availability 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 High Availability 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 high availability servers, see the [Cisco Evolved Programmable Network Manager Installation Guide](#).

Table 1: SSO Configuration in a High Availability Deployment

SSO Configuration	Setup SSO Server	Sever Failover Scenario	SSO Server Failure Scenario
SSO as a standalone server	<ol style="list-style-type: none"> 1 Configure the standalone SSO server. 2 Configure the primary and secondary high availability servers. 	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.	When the SSO server fails, SSO functionality is disabled. Cisco EPN Manager will use local authentication.

SSO Configuration	Setup SSO Server	Sever Failover Scenario	SSO Server Failure Scenario
SSO on the secondary Server	<ol style="list-style-type: none"> 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). 2 Configure the secondary high availability server. 	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).	<p>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.</p> <p>If the secondary is not set to be the SSO server failback option, Cisco EPN Manager will use local authentication.</p>

Reset the HA Authentication Key

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 into 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.

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.

Restore Data In an HA Deployment

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 On the primary server, remove HA using the **ncs ha remove** command.
- 2 Restore data on the primary server as described in [Restore Cisco EPN Manager Data](#).
- 3 When the restore process is complete, perform the HA registration process again.

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 11
- [HA Configuration Modes](#), on page 13
- [HA States and Transitions](#), on page 3
- [Check HA Status and Overall Health](#), on page 13
- [View and Customize HA Events](#), on page 14
- [Use HA Error Logging](#), on page 14

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 do not receive 3 consecutive heartbeats from the other redundant server, it waits for 10 seconds. Subsequently the healthy server attempts to open a webURL in the redundant server, when 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.

Once you have completed HA registration 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 Active** state.

The screenshot displays the Cisco EPN Manager Health Monitor web interface. At the top, the title bar includes the Cisco logo, 'EPN Manager Health Monitor', and navigation links for 'Secondary', 'Software Update', 'Refresh', and 'Logout'. Below the title bar, the 'Health Monitor Details' section shows the version as '3.0 (3.0.0.0.66)'. The main content area is divided into several sections: 'Settings' (1), 'Status' (2) which shows a green checkmark indicating HA is enabled, 'Primary IP Address' (4) showing '192.0.2.122', 'State' (5) showing 'Secondary Active', 'Failover Type' (9) showing 'Manual', and 'Action' (10) showing a 'Failback' button. A 'Logging' section includes a 'Message Level' dropdown set to 'Information' and a 'Save' button (7), along with a 'Download Health Monitor Log Files' button (5). The 'Events' section at the bottom provides a chronological list of HA-related events, including failover completion, primary server loss, and health monitor availability.

Time	State	Description
Aug 20, 2015 01:39:13 PM	Secondary Active	Completed failover from sjd-v-ha1 [192.0.2.123] to sjd-v-ha2 [192.0.2.122]
Aug 20, 2015 01:38:54 PM	Secondary Active	Primary Evolved Programmable Network Manager sjd-v-ha1 [192.0.2.123] lost service and is going to failover to Secondary Evolved Programmable Network Manager sjd-v-ha2 [192.0.2.122]
Aug 20, 2015 01:38:54 PM	Secondary Lost Primary	Started failover from sjd-v-ha1 [192.0.2.123] to sjd-v-ha2 [192.0.2.122]
Aug 20, 2015 01:35:20 PM	Secondary Lost Primary	Secondary lost the connection with the primary due to Administrative shutdown from
Aug 20, 2015 10:18:25 AM	Secondary Syncing	New Primary Evolved Programmable Network Manager server
Aug 20, 2015 10:10:04 AM	HA Initializing	Primary Evolved Programmable Network Manager
Aug 17, 2015 12:13:42 PM	HA not Configured	Secondary EPN Manager Server started successfully as standby
Aug 17, 2015 11:53:59 AM	Health Monitor Available	Health Monitor Started

1	Settings—Displays Health Monitor state and configuration detail in five separate sections.	2	Status—Indicates the current functional status of the HA setup (a green check mark indicates HA is enabled and working).
3	Events—Displays the current HA-related events, in chronological order, with the most recent events at the top.	4	IP address—Displays the IP address of paired server. Because this HM instance is running on the secondary server, it shows the IP address of the primary server.
5	Download—Lets you download Health Monitor log files.	6	State—Shows the current state of the server on which this HM instance is running (in this case, the secondary server).
7	Message Level—Indicates the current logging level, which you can change (Error, Informational, or Trace). You must click Save to change the logging level.	8	Title bar—Identifies the HA server whose HM web page you are viewing, along with the Refresh and Logout buttons. Software Update is only displayed for secondary servers.
9	Failover Type—Shows whether you have Manual or Automatic failover configured.	10	Action—Actions you can perform, such as failover or failback. Only the appropriate actions are displayed.

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).

Mode	Description
HA Not Configured	HA is not configured on this server
HA Initializing	HA registration process between the primary and secondary servers has started
HA Enabled	HA is enabled between the primary and secondary servers
HA Alone	Server is running alone because one of the servers is down, out of sync, or unreachable.

Check HA Status and Overall Health

You can use the web GUI or CLI to check HA status. All of these approaches will list the state of the server. States are described in [HA States and Transitions](#), on page 3.

To use the web GUI:

- From the Cisco EPN Manager web GUI. Choose **Administration > Settings > High Availability**, then choose **HA Status**. The current HA status and the HA states for the events are displayed.
- From the Health Monitor. See [Use the Health Monitor Web Page](#), on page 11.

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 the following HA-specific output:

```
ncs ha status
[Role] Secondary [Primary Server] cisco-ha1(192.0.2.133) [State] Secondary Active [Failover
Type] Manual
```

Use the `ncs status` to check the Health Monitor and other server processes:

```
ncs status
Health Monitor Server is running. ( [Role] Secondary [State] Secondary Active )
Database server is running
Ftp Server is running
Tftp Server is running
Matlab Server is running
Matlab Server Instance 1 is running
Matlab Server Instance 2 is running
Matlab Server Instance 3 is running
NMS Server is running.
Plug and Play Gateway 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:

-
- | | |
|---------------|--|
| Step 1 | Choose Monitor > Monitoring Tools > Alarms and Events , then click the Alarms tab. |
| Step 2 | Choose Quick Filter from the Show drop-down list at the top right of the table. |
| Step 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 11). |
| 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: <ol style="list-style-type: none"> 1 Click Download.
A .zip file is copied to your default download location. 2 Extract the log files and use any ASCII text editor to view them. |
-

Trigger Failover

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

The Health Monitor detects failure conditions using the heartbeat messages exchanged between the two servers. The heartbeat messages are sent every 5 seconds. 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, 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. In case of a network issue, HA system takes a longer time to discover the failure and initiate a failover. If the secondary server is unable to reach the primary server due to a network issue, it might take more time to 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 the failure, it sends an email notification. The email 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:
<code>https://ServerIP:8082</code> |
| 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, and stops active network monitoring processes on the secondary.

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.

Once the data has begun replicating 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 or not the primary server has been reinstalled with Cisco EPN Manager after the failover, as follows:

- If the primary server has not been reinstalled with Cisco EPN Manager, the secondary server is available except during the period when processes are started on the primary and stopped on the secondary. 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 functionality
- 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.

- Do not initiate configuration or provisioning activity while the failback is in progress.
- Be aware that, 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.

You must always trigger failback manually, as 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 syslog 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 email notification, or by entering the following URL on your browser:
`https://ServerIP:8082`
- Step 2** Click **Failback**.
-

Common Failover/Failback Scenarios

The following topics describe common HA scenarios that may require failover and failback.

- [Network is Down](#), on page 17
- [Process Restart Fails](#), on page 17
- [Primary Server Restarts During Synchronization](#), on page 18
- [Secondary Server Restarts During Synchronization](#), on page 18
- [Split Brain Scenario \(Servers Come Up at Same Time\)](#), on page 18
- [Both HA Servers Are Powered Down](#), on page 19
- [Both HA Servers Are Down and Secondary Will Not Restart](#), on page 19
- [Replace the Primary HA Server](#), on page 20
- [Secondary Server Goes Down](#), on page 20

Network is Down

If there is a loss of network connectivity between the primary and secondary servers, you will get email notifications that each server has lost connectivity to the other server.

If Automatic Failover is Configured:

After the failover is complete, you will receive an email notification that the secondary server is now active.

- 1 Check on and restore network connectivity between the two servers.
- 2 Restart the primary server.
- 3 Trigger a failback from the secondary to the primary server (see [Trigger Failback, on page 15](#)).

If Manual Failover is Configured:

- 1 Check on and restore network connectivity between the two servers.
- 2 Use the Health Monitor web page for the secondary server to trigger a failover from the primary to the secondary server (see [Use the Health Monitor Web Page, on page 11](#)).
- 3 Once you have received email notification that the secondary is now active, trigger a failback from the secondary to the primary server (see [Trigger Failback, on page 15](#)).

Process Restart Fails

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

If Health Monitor 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 Automatic Failover is Configured:

After the failover is complete, you will receive an email notification that the secondary server is now active.

- 1 Restart the primary server and ensure that it is running. When the primary server is up, its HA state will be **Standalone**.
- 2 Trigger a failback from the secondary to the primary server (see [Trigger Failback, on page 15](#)).

If Manual Failover is Configured:

- 1 Trigger a failover from the primary to the secondary (see [Trigger Failover, on page 14](#)).
- 2 Restart the primary server and ensure that it is running. When the primary server is up, its HA state will be **Standalone**.
- 3 Trigger a failback from the secondary to the primary (see [Trigger Failback, on page 15](#)).

Primary Server Restarts During Synchronization

If Manual Failover is Configured:

If the primary server is restarted while the secondary server is synchronizing, the **Standalone** and the **HA Initializing** states occur immediately after the primary comes back online. No administrator response should be required.

If Automatic Failover is Configured:

If the primary server is restarted while the secondary server is synchronizing, you must trigger a failback from the secondary to the primary (see [Trigger Failback](#), on page 15).

Secondary Server Restarts During Synchronization

If the secondary server is restarted while syncing with the primary server, you will see the same state transitions regardless of the Failover Type settings. No administrator response should be required.

Split Brain Scenario (Servers Come Up at Same Time)

In a split-brain scenario, both the primary and secondary servers become active at the same time, perhaps due to a network outage or 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.

Use the primary server and its newly-added data. When the network comes up, the primary server will go down and its HA status will be **Primary Failover**. Do the following:

- 1 Restart the primary server. Its status changes to **Primary Alone**.
- 2 Remove the HA configuration, then re-register the secondary server with the primary server.

Use the secondary server and its newly-added data. When the network comes up, the primary server will go down and its HA status will be **Primary Failover**. Do the following:

- 1 Confirm that a user can log into the Cisco EPN Manager GUI on the secondary server (for example, `https://ip-address:443`). Do not proceed until this access has been verified.
- 2 Initiate a failback from the secondary server's Health Monitor web page. Users can continue to perform monitoring activities on the secondary server until the switchover to the primary is completed.

Both HA Servers Are Powered 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** Power on the secondary server and the instance of Cisco EPN Manager 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 11](#)). You will see the secondary server transition to the **Secondary Lost Primary** state.
- Step 3** Power on the primary server and the instance of Cisco EPN Manager 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:
- Primary server will change from **Primary Lost Secondary** to **Primary Active**.
 - Secondary server will change from **Secondary Lost Primary** to **Secondary Syncing**.
- Step 5** Restart the secondary server and the instance of Cisco EPN Manager 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 Will Not Restart, on page 19](#).
- 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 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 until you can replace or restore 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.
- Step 5** Enter N (no) when you are prompted to confirm that you want to remove all of the HA database information from both the primary and secondary servers.

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. When you are able to restore or replace the secondary server, proceed as explained in [Register the Secondary Server on the Primary Server, on page 7](#).

---

## Replace the Primary HA 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 14](#)).
  - 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** Trigger a failback from the secondary server to the newly-installed primary server. You will see the two servers transition through the following series of HA states:
    - Primary server will transition from **HA Not Configured** to **Primary Failback** to **Primary Active**.
    - Secondary server will transition from **Secondary Active** to **Secondary Failback** to **Secondary Post Failback** to **Secondary Syncing**.
- 

## 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 [Register the Secondary Server for HA, 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 [Register the Secondary Server for HA, on page 7](#).
- 

## High Availability CLI Command Reference

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 2: High Availability Commands**

| Command                                 | Description                                        |
|-----------------------------------------|----------------------------------------------------|
| <b>ncs ha ?</b>                         | Display the command usage message                  |
| <b>ncs ha authkey <i>newAuthkey</i></b> | Update the authentication key to <i>newAuthKey</i> |
| <b>ncs ha remove</b>                    | Remove the HA configuration                        |
| <b>ncs ha status</b>                    | Get the current status for HA                      |

