CHAPTER 18

Using the Cisco NAC Profiler Server Command Line

Topics in this chapter include:

- Overview, page 18-1
- The Service Profiler Command Set, page 18-2
- Cisco NAC Profiler Server Database Operations, page 18-6
- Adding HA to an Operational Standalone System, page 18-13
- Repairing the Configuration of an HA Pair, page 18-14
- Forcing a Cisco NAC Profiler Server HA-Pair to Failover, page 18-16
- Temporarily Disabling HA, page 18-17
- Permanently Removing the HA Configuration, page 18-19
- Returning a Cisco NAC Profiler Server to Factory Defaults, page 18-20
- Changing the beacon and root System User Account Passwords, page 18-21

Overview

The vast majority of the configuration and management tasks for the Cisco NAC Profiler system are performed using the web-based user interface. There are however some functions that are performed via the command line on the Cisco NAC Profiler Server appliances. This chapter outlines several command line operations that may need to be performed on the NAC Profiler Server as part of NAC Profiler system administration.

Note The commands outlined in this chapter are specific to the NAC Profiler Server **only**, and are not functional for the Collector service running on Cisco NAC Servers. The CLI commands for the Collector service running on the NAC Server are documented in Chapter 4, "Issuing CLI Commands to the Cisco NAC Profiler Collector" section on page 4-61

The command line is accessed on a NAC Profiler Server appliance by initiating a console session or establishing an SSH session to the management interface (eth0) of the appliance.

Tip Cisco NAC Profiler Server appliances will allow SSH connections to only the beacon system user account; attempts to access the root system user are blocked by the system as a security measure. When root access is required, initiate the SSH session as system user beacon (**ssh beacon@**...) and then use the **su** command to elevate to root.

Tip For NAC Profiler Server HA-pairs, the command line of the Primary node can be accessed by establishing an SSH session to the VIP as the beacon system user

The Service Profiler Command Set

The NAC Profiler Server command line provides a 'service profiler' command set that enables several system-level functions to be executed from the command line of Cisco NAC Profiler Server appliances. These commands provide control of the Cisco NAC Profiler software on the appliance as well as running selected configuration scripts.

A description, guidelines for usage and example output (if applicable) are provided for each of the available commands.

service profiler status

(Can be run as root or beacon system user)

This command will provide the current NAC Profiler Server software version, and enumerate the current status of the module(s) installed on the system. For each of the modules running on a Cisco NAC Profiler Server appliance, the current status can be:

- running
- not running
- not installed

service profiler start

(Can be run as root or beacon system user)

Starts all the installed Profiler modules on the NAC Profiler Server system.

service profiler stop

(Can be run as root or beacon system user)

Stops all the installed Profiler modules on the NAC Profiler Server system. Reports the following:

```
profiler stopping
```

service profiler restart

(Can be run as root or beacon system user)

Stops all the installed Profiler modules and then immediately restarts them.

service profiler debug

(Can be run as root or NAC Profiler Server system user)

This subcommand places the Server module in debug mode and enables verbose logging to the Server.out log file for the purposes of advanced debugging. While operating in debug mode, the log files can grow very large in a short amount of time and the use of this mode should be restricted to that directed by a Great Bay technical support representative.

Tip Systems should only be placed in the debug mode under the direction of the Cisco TAC and the system should be operated in debug mode for limited amounts of time to prevent excessive growth of the log files.

Tip Note that the proper usage of this command is to stop the service first via **`service profiler stop`**, then start the service in debug mode with **`service profiler debug`**. Typically the service is run in debug mode for a specified period of time, and the service is returned to normal operation by restarting it (service profiler restart). The Server.out (located in usr/beacon/logging) containing the debug information is then collected for offline analysis.

`service profiler config`

(Requires root access). If the command as run as user beacon, the system prompts the user:

```
You must be root to use the 'config' subcommand
```

Re-runs the start-up scripts for the system. This subcommand will cycle through the 5 sub-scripts performed at system start up in the following order:

Tip Most of these scripts can be called individually. See the later subcommands in the list.

- Network Configuration (eth0 IP address, mask, default gateway and name server)

Warning **The network configuration script should NOT be run on an operational HA-pair as it will disrupt the HA protocol. If the network configuration of a NAC Profiler Server in an HA-pair requires re-configuration, HA needs to removed first and then re-configured in accordance with the procedures found later in this chapter. When HA is enabled on a system, running service profiler setupnetwork is prevented by the system.**

- NTP Configuration (remove or add NTP Servers)
- Endpoint Profiler
- HA setup scripts
- Certificate Action (view, create download, or backup SSL Certificates)

If an existing configuration is found, the system will prompt if re-configuration is desired. If re-configuration is not selected, the script will move onto the next configuration task without making changes to the existing configuration. At the completion of the scripts, the system will be restarted.

Tip If re-configuration is selected, the scripts will prompt for new information without displaying the current settings.

service profiler setupccakey

This subcommand is specific to integration of NAC Profiler Server with Cisco NAC appliance.

Refer to Chapter 13, "Integrating with the Cisco NAC Appliance"for instructions on the use of this subcommand.

service profiler setupcert

(Requires root access). If the command as run as user beacon, the system prompts the user:

```
You must be root to use the 'setupcert' subcommand
```

This subcommand re-runs the Digital Certificate Management script that is normally run for the first time when NAC Profiler Server is initially configured.

It can be used to view current Digital Certificate parameters, generate a CSR or new self-signed certificate on the system.

service profiler setupha

(Requires root access). If the command as run as user beacon, the system prompts the user:

```
You must be root to use the 'setupha' subcommand
```

This subcommand will run the scripts necessary to add HA to a running All-in-one or Server Only appliance. It is utilized for two procedures outlined later in this chapter: "Adding HA to an Operational Standalone System" section on page 18-13 and "Repairing the Configuration of an HA Pair" section on page 18-14.

service profiler setupldaps

This command allows the NAC Profiler Server's LDAP subsystem to use Secure LDAP or LDAPS and is specific to the configuration of the NAC Profiler Server system for LDAP integration. See Chapter 17, "Enabling LDAP Integration" for further details about using this subcommand to enable an optional feature of the LDAP integration.

service profiler setupntp

(Requires root access). If the command as run as user beacon, the system prompts the user:

```
You must be root to use the 'setupntp' subcommand
```

This subcommand allows the user to add or reconfigure NTP on the NAC Profiler Server System. It is recommended that NTP be configured on all NAC Profiler Server appliances. Using NTP on NAC Profiler Server will provide accurate timestamps for logs and statuses of various UI display screens. See Chapter 4, "Installing and Performing an Initial Configuration," for further instructions on configuring NTP. Note that if the system has been previously configured for NTP the following message will be displayed:

"This system appears to have a previous NTP configuration. Would you like to skip reconfiguration?"

Select "No" in order to reconfigure the NTP Configuration.

service profiler setupnetwork

(Requires root access). If the command as run as user beacon, the system prompts the user:

```
You must be root to use the 'setupnetwork' subcommand
```

This subcommand allows the user to reconfigure the NAC Profiler Server eth0 interface configuration settings by running the Network Configuration script, which was used during the initial setup of the NAC Profiler Server. On systems that have a valid interface configuration, the first message displayed asks the user:

"This system appears to have a previous network configuration. Would you like to skip reconfiguration?"

Select "No" in order to reconfigure the eth0 interface configuration.

Warning **Do not attempt to make changes to the interface configuration of a member of an operational HA-pair. If changes to the IP configuration of an appliance in an HA-pair are required, the HA configuration should be removed first, changes made to the configuration as required, and the HA configuration re-added. The correct procedure for removing and re-adding HA configuration is provided in the"Repairing the Configuration of an HA Pair" section on page 18-14.**

Tip Running this script after completion of the initial startup will not allow the changing of the host name of the appliance.

`service profiler HApushCert`

(Specific to HA systems, requires root access)

This subcommand allows the user to copy the exiting SSL Certification on the Primary node of an HA pair and push it to the Secondary node so that both appliances in the pair are using the same digital certificate for the SSL subsystem of the UI server. This is performed automatically when setting up an HA-pair during the appliance startup.

This command is used only when a new digital certificate is installed on a HA-pair, when a CA-signed certificate is installed for example. Complete instructions for this operation are provided in Chapter 5 in the "Importing a Digitally Signed SSL Certificate into the Cisco NAC Profiler System" section on page 5-17.

HA System Considerations for Service Profiler Commands

NAC Profiler Server systems implemented as HA-pairs have additional considerations for use of the service profiler commands. The Secondary node in a NAC Profiler Server HA-pair will always show the status of all installed modules as 'Not Running.' This is the normal state for the Secondary node in an HA pair—the HA protocol is maintaining database synchronization and in the event of failure of the Primary node, the NAC Profiler modules will be started in conjunction with the failover.

```
[beacon@BeaconHA2 /usr/beacon]$ service profiler status

Profiler Status
       Version: Profiler-3.0.0r_6
      o Server         Not Running
      o Forwarder      Not Running
      o NetMap         Not Running
      o NetTrap        Not Running
      o NetWatch       Not Running
      o NetInquiry     Not Running
      o NetRelay       Not Running
```

Warning **The command service profiler start should not be executed on the Secondary node of an HA-pair. If this command is entered at the command line of an appliance in a HA-pair while it is the Secondary node, the following message will be displayed:**

```
''This service is being managed by HA subsystem -- no action taken.''
```

On a running NAC Profiler Server HA-pair, the NAC Profiler services on the Secondary node of the pair should be left to the control of the HA protocol and not manipulated via the command line.

Cisco NAC Profiler Server Database Operations

The NAC Profiler Server system utilizes a PostgreSQL database to store all system configuration and endpoint data. PostgreSQL is a powerful, enterprise-class relational database system that strongly conforms to ANSI-SQL 92/99 standards.

Because the system configuration and endpoint data is stored in a single database, system backup and restore consists of creating a backup copy of the Profiler database and moving it to an off-system repository for safe keeping should the NAC Profiler Server system need to be rebuilt. In case of catastrophic failure of the NAC Profiler Server, the recovery model is to restore the NAC Profiler Server system from media, then restore the Profiler database to the most recent successful backup to restore the entire system to the state it was in previous to the failure.

Note System-level configuration of the appliance including network configuration of the interfaces (for example, IP address, mask, default gateway, etc.), system user account passwords (root and beacon), and Cisco NAC Profiler licenses are **not** stored in the database. In a disaster recovery scenario, after the NAC Profiler Server image is re-installed using the ISO process the appliance will require the completion of the startup scripts as described in Chapter 4, “Installing and Performing an Initial Configuration” to provide this configuration of the system and licensing. The database restore can then be performed to return the system to service in the state it was in prior to the catastrophic failure.

The Server module will perform an automatic copy of the Profiler database each day at approximately 3:00AM system time. These daily backups can be found in the /backup directory in compressed (.gz) format.

Tip A symbolic link is created in the /backup directory that points to the most recent database backup file. The symbolic link is filename dailyDB-latest.gz and can be seen in an ls -la of the /backup directory on the NAC Profiler Server.

Tip As outlined later in this chapter, the .gz compressed format used in creating database backups from the UI and the automated backups is the format that the database restore scripts expect when restoring a backed-up database to a system.The database backup files can be stored as-is and used to restore a NAC Profiler system from backup as described in “Database Restore” section on page 18-8.

The Server module will maintain the backup directory so that database backups older than 30 days are automatically deleted from the backup directory. This prevents the automatic backups from taking up too much disk space.

```
[root@BeaconHA1 /backup]# ls -la
total 4540
drwxrwx---   2 beacon  beacon    1024 Mar  2 03:15 .
drwxr-xr-x  21 root    wheel      512 Feb 20 14:37 ..
-rw-r--r--   1 beacon  beacon  392055 Feb 21 03:00 dailyDB-1235203200.gz
-rw-r--r--   1 beacon  beacon  400557 Feb 22 03:00 dailyDB-1235289600.gz
```

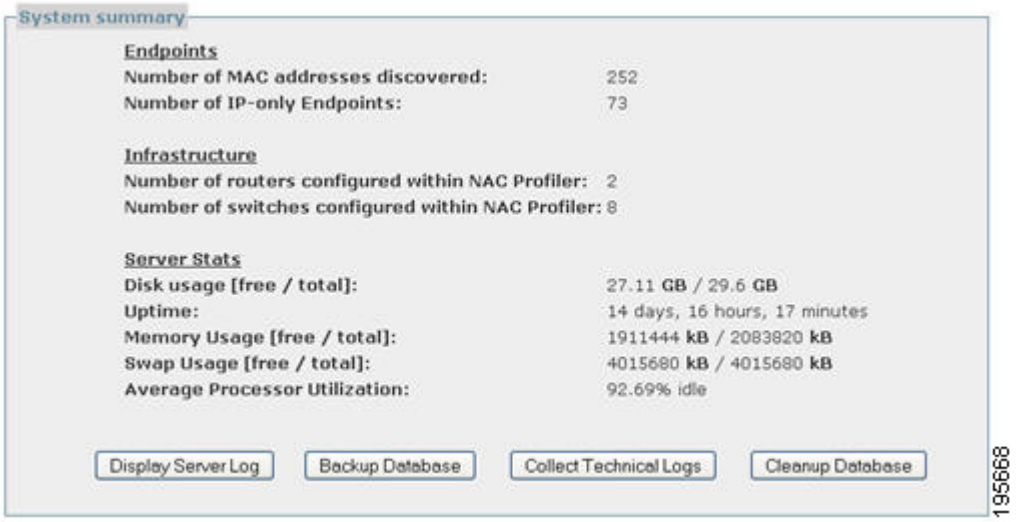
```
-rw-r--r--   1 beacon  beacon  382173 Feb 23 03:00 dailyDB-1235376001.gz
-rw-r--r--   1 beacon  beacon  401301 Feb 24 03:00 dailyDB-1235462400.gz
-rw-r--r--   1 beacon  beacon  390508 Feb 25 03:00 dailyDB-1235548801.gz
-rw-r--r--   1 beacon  beacon  384097 Feb 26 03:00 dailyDB-1235635201.gz
-rw-r--r--   1 beacon  beacon  393513 Feb 27 03:00 dailyDB-1235721601.gz
-rw-r--r--   1 beacon  beacon  373798 Feb 28 03:00 dailyDB-1235808000.gz
-rw-r--r--   1 beacon  beacon  386236 Mar  1 03:00 dailyDB-1235894401.gz
-rw-r--r--   1 beacon  beacon  376795 Mar  2 03:00 dailyDB-1235980800.gz
lrwxr-xr-x   1 beacon  beacon      29 Mar  2 03:00 dailyDB-latest.gz -> /backup/
```

Tip It is highly recommended that the NAC Profiler Server database backups are moved off the appliance regularly and stored with other system backups in accordance with system backup best practices.

Manual Database Backup

In addition to the automated backups performed by the system, it is also possible to make a backup copy of the Profiler database at any time. In Versions 2.1.8 and greater, a backup copy can be made and transferred off the system in a single operation through the NAC Profiler Server UI. Navigate to the Utilities tab, and select System Summary. At the bottom of the System Summary, four buttons are displayed: Display Server Log, Backup Database, Collect Technical Logs, and Cleanup Database as illustrated in Figure 18-1.

Figure 18-1 System Summary Page



To initiate the backup of the NAC Profiler system database in Version 3.1 and greater, select the "Backup Database" button which results in the browser displaying the download file dialog which will allow the designation of an off-appliance location to save the database backup copy to. Specifying a path for the file will result in the database being saved to a compressed file and copied to the specified location. By default, the filename for the backup copy created by this action is named 'beacondb.gz'.

Database Restore

A backup copy of the NAC Profiler database can be restored to a NAC Profiler system at any time.

Tip Because the database contains both the system configuration and the endpoint data, any changes made to the system configuration since the backup was created will be lost after a database restore on a Cisco NAC Profiler system.

Profiler database restore is performed differently for standalone NAC Profiler Server and HA-pairs. Before restoring a database to a Profiler system, it is important to determine first if it is a Standalone or HA system, then use the appropriate procedure below to restore the Profiler database.

Database Restore on Standalone (non-HA) Systems

Restoring the Profiler database to a Standalone system can be performed through the execution of a single script. Follow these steps to restore the database to a NAC Profiler system.

Step 1 Copy the backup file to be restored to the /backup directory on the NAC Profiler Server via SCP if the desired backup to restore from is not already in the directory.

Tip The database restore script expects the database to be in the Gzip format (.gz file extension). The script will error out and not restore the database(s) that are not in the Gzip format in this release (3.1.1).

Step 2 Initiate a SSH session to the NAC Profiler server as the beacon system user, and change directory to /usr/beacon/scripts/maint

```
cd /usr/beacon/scripts/maint
```

Step 3 Run the following script to restore the selected database backup on the standalone system:

```
./restoreDB.pl /backup/beacondb.gz
```

where beacondb.gz is the filename of the backup the system is to be restored to.

Tip To utilize the most recent backup file in the directory, the symbolic link dailyDB-latest.gz can be passed as the argument to the database restoration script.

Step 4 Once the script has finished running execute an Apply Changes -> Update Modules via the UI to restart the system using the restored database.

Database Restore on HA Systems

The NAC Profiler Server HA protocol includes a database synchronization function that ensures that the system configuration and endpoint data maintained in the database is kept in synch on both members of the pair. Therefore, the process to restore the Profiler Database on an HA pair requires the restore on the Primary node, and reliance on the synchronization process to update the Secondary appliance database.

Tip In order to ensure that the database restore is performed on the Primary node, the restore process outlined in this section should be performed via SSH to the VIP for the HA-pair.

Follow these steps to restore a NAC Profiler Server database on an HA-pair:

Step 1 Copy the backup file to be restored to the /backup directory on the Cisco NAC Profiler Server Primary node via SCP if the desired backup to restore from is not already in the directory.

Tip The database restore script expects the database to be in the Gzip format (.gz file extension). The script will error out and not restore the database(s) that are not in the Gzip format in this release (3.1.1).

Step 2 Initiate a SSH session to the VIP of the HA-pair, and elevate to the root user via the **su**- command, then change directory to /usr/beacon/scripts/maint

```
cd /usr/beacon/scripts/maint
```

Tip Execution of database restore on a HA-pair requires root level privileges.

Step 3 Run the following script to restore the selected database backup on the Primary appliance of the HA-pair:

```
./restoreDB-HA.pl /backup/beacondb.gz
```

where beacondb.gz is the filename of the backup the HA system is to be restored to

Tip To utilize the most recent backup file, the symbolic link dailyDB-latest.gz can be passed as the argument to the database restoration script.

Step 4 Once the script has finished running, execute an Apply Changes -> Update Modules to restart the HA system using the restored database.

Cisco NAC Profiler Server HA-Pair Operations

The NAC Profiler Server system supports HA configuration as described in Chapter 2, "Overview: Cisco NAC Profiler Architecture." The HA protocol can be configured at system startup using the procedures outlined in Chapter 4, "Installing and Performing an Initial Configuration," or HA can be added to an operational standalone system using the procedure outlined in this section at any time. There are several operations that may need to be performed on an HA system from time to time. This section provides guidance on the management of an HA NAC Profiler Server system from the command line.

Determining which Appliance in a Cisco NAC Profiler Server Pair is the Primary

At any given time, only one appliance in the NAC Profiler Server HA-pair is running the NAC Profiler Server processes and serving as the Primary node. The Primary maintains the master Profiler database and maintains database synchronization on the Secondary node. The Primary appliance will hold the VIP/Service IP for the HA pair. To determine which appliance (by physical IP of the management interface or host name) is currently the Primary node and which is Secondary, perform the following steps to determine which appliance in the pair is currently holding the VIP IP for the pair via CLI:

Tip On the Cisco NAC Profiler Dashboard (Home tab) of the Cisco NAC Profiler UI, the host name of the current Primary node is indicated in the HA Status Table.

Step 1 SSH to the VIP for the HA pair as user beacon

Step 2 Issue the following command:

```
ifconfig eth0
```

to display the configuration of the interface on the appliance currently holding the VIP for the HA pair. An excerpt of the output from running this command on an appliance is shown below:

```
[beacon@BeaconHA1 ~]$ ifconfig eth0
eth0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=1db<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,POLLING,VLAN_HWCSUM,TSO4>
            ether 00:04:23:d6:5f:ba
            inet 10.174.80.240 netmask 0xffffff00 broadcast 10.174.80.255
            inet 10.174.80.242 netmask 0xffffffff broadcast 10.174.80.242
            media: Ethernet autoselect (1000baseTX <full-duplex>)
            status: active
```

Step 3 The interface named 'eth0' shows the IP address assigned to the management interface (eth0) of the appliance that is currently serving as the Primary for the pair. In the above example the IP address of the Management Interface of the Primary appliance is 10.174.80.240.

Note that the VIP (10.174.80.242 in the example) is also shown as the address for this interface on the Primary node.

Verifying HA-Pair Operation

Tip The HA System Status on the NAC Profiler Dashboard (Home tab of UI) provides at-a-glance verification of HA status. The “Secondary is Online” is a good indication that HA is operating normally and can be readily ascertained via the UI. The procedures in this section provides further verification that the protocols necessary for HA operation and database synchronization are operating normally at the system-level.

Verification of the proper functioning of the NAC Profiler Server HA protocol should be accomplished after configuration of HA to ensure the protocol is operating normally.

This section provides instructions for verifying the operation of the HA protocol: heartbeat and protocol (slon) operation and database synchronization. The HA protocol will update the database on the Secondary node continuously, once the HA initiation sequence is completed properly.

Tip Verification of database synchronization is the best test to ensure that the HA database synchronization protocol is operating normally for an HA-pair.

Check for Heartbeat and SLON Processes

The first check to verify proper operation of the HA process is to verify that both members of the pair are running the heartbeat and SLON processes which are required for normal HA operation. Complete the following steps to ensure these processes are running on both members of the HA pair:

Step 1 Initiate an SSH session with both the Primary and Secondary appliances on their respective management interface (eth0) IP addresses.

Step 2 Issue the following command on both appliances to determine the current status of the heartbeat service:

```
service heartbeat status
```

The command should return a result such as the following on both the current Primary and Secondary members of an HA pair:

```
heartbeat OK [pid 20960 et al] is running on beaconha1 [beaconha1]...
```

Step 3 Verify that both the Primary and Secondary have the required two slon processes running by issuing the following command:

```
ps aux | grep slon
```

This command should show a similar result on both members of an HA pair if the slon processes are running normally:

```
[beacon@BeaconHA1 /usr/beacon/sql/HA]$ ps aux | grep slon

beacon     4058  0.0  0.1  6000  2140  p0- I    20Feb09   0:00.00 /usr/local/bin/slon -d 0
-p /usr/beacon/working/slon.pid -s
beacon     4060  0.0  0.1 11888  2960  p0- S    20Feb09   4:26.44 /usr/local/bin/slon -d 0
-p /usr/beacon/working/slon.pid -s
beacon    13483  0.0  0.0  1632  1016  p0  R+   11:42AM   0:00.00 grep slon
```

If both of the preceding checks result in the desired output, proceed with the next step to verify database synchronization on the Secondary appliance. If either the heartbeat or slon processes are not running as indicated above on either member of the HA pair, proceed with the process outlined in "Repairing the Configuration of an HA Pair" section on page 18-14

Check Database Synchronization on Secondary Node

To verify that the database synchronization is occurring properly on an HA pair, follow these steps to ensure the Profiler database on the Secondary node was created properly and is being regularly updated via the HA database synchronization process.

Tip When performing this procedure on a newly configured HA-pair, it is essential to wait several minutes after the completing the HA setup process to ensure that the protocol has had ample time to complete the initial database synchronization on the Secondary member of the pair. The procedure below checks the status of the database tables that are synchronized last, therefore it is important to wait several minutes before using this check on newly configured HA-pairs.

Step 1 Determine the IP address of the eth0 (management) interface of the Secondary node in the HA pair, and initiate an SSH session to this system as the beacon user.

Tip If you are not sure which appliance in the pair is the Secondary, follow the procedures outlined earlier to determine which appliance is currently the Primary node.

Step 2 The database table named 'beacon_component" is among the last to be synchronized on the Secondary node of an HA pair. Query this table on the Secondary node of the HA pair to ensure that the table is present and being updated regularly by using the following command:

```
echo "select name,status_time from beacon_component" | psql
```

The following is example output from the execution of this step on an operational Secondary system in a NAC Profiler Server HA-pair:

```
[beacon@BeaconHA2 /usr/beacon]$ echo "select name,status_time from beacon_component" |
psql
     name     |         status_time
--------------+----------------------------
 BeaconHA1-nt | 2009-03-02 13:53:40.911178
 BeaconHA1-nw | 2009-03-02 13:54:04.242235
 BeaconHA1-fw | 2009-03-02 13:54:21.317064
 BeaconHA1-nm | 2009-03-02 13:54:31.639679
 BeaconHA1-ni | 2009-03-02 13:54:31.975007
 BeaconHA1-nr | 2009-03-02 13:54:36.78844
 Server       | 2009-02-26 09:45:28.921542
(7 rows)
```

As the example shows, the output of executing this command on the Secondary node shows all component modules of the HA pair, and the time of the last status message the system has processed for each of the Collector modules, which should be near the system time on the HA pair. Note that the Server Module status time on the Secondary device will not be updated, this is expected.

Tip If the error message "Error: relation "beacon_component" does not exist" results from the query, this is indicative of the HA protocol on the pair being incorrectly configured and that the database schema has not been set up correctly. Follow the procedure outlined in the "Repairing the Configuration of an HA Pair" section on page 18-14.

Step 3 Wait several minutes, and execute the query again. The status time should be increasing between queries. This indicates that the HA process is functioning normally, and that the Secondary node is ready to become Primary should the current Primary appliance fail.

Adding HA to an Operational Standalone System

An operational standalone NAC Profiler Server may have an HA peer added to it at any time. In the most common scenario, an operational standalone NAC Profiler Server appliance is to be converted to HA pair operation through the addition of a second appliance in order to provide protection for the NAC Profiler system against single appliance failure. Typically, the NAC Profiler Server appliance that is already operating and maintaining the database for the system will become the initial Primary node of the HA-pair, and a new, yet-to-be configured NAC Profiler Server appliance will be added as the Secondary node/HA peer, set up for that role via the startup scripts that initiate upon the first power-up of the appliance.

Tip This procedure is specifically for the case of adding an HA peer to an already operational standalone NAC Profiler Server. For the initial installation of an HA-pair on a new installation, the procedure in Chapter 4, "Installing and Performing an Initial Configuration" should be followed.

Note If the NAC Profiler Server appliance that will be added to an operating standalone in the HA pair configuration has been configured and used previous to its employment as a member of an HA pair, that appliance **must** first be re-imaged via ISO to ensure that all configuration and data is removed from the system. The completion of the "Return to Factory Defaults" procedure outlined later in this chapter is NOT recommended for preparation of an appliance. The appliance should be ISOed to the same version of NAC Profiler Server before it is employed in HA-pair operations.

Ensure that all passwords (for example, beacon and root system user accounts, and Web UI admin) for the Primary node are known prior to beginning configuration of the new Profiler Server appliance to be added as the Secondary node. When configuring the Secondary node of the HA pair, all passwords on both systems must match exactly.

Step 1 Prior to beginning the process, ensure that the following HA system configuration parameters are determined and readily available:

- Ensure NTP is configured on the Primary node (existing standalone) prior to adding HA, use the `service profiler setupntp` command if it was not configured at appliance startup.
- VIP/Service IP address to be used for the HA-pair
- Host name of the Secondary Profiler Server appliance being added as an HA peer, as well as the Host name of the Primary node.
- Local HA Network: the first three octets of a private network IP address (for example, 192.168.35) to be used for the heartbeat network between the two Profiler Server appliances (eth1 interfaces).
- HA Authentication Key: a text-string to be utilized by the appliances to authenticate. The HA Shared Key must be entered identically (case sensitive) on both appliances in order for the relationship to be established.
- Redundant Heartbeat Communication: the IP address of the management interface (eth0) of the alternate system.

- HA External Ping Host: a host IP address of another network device, preferably on the same subnet as the HA pair that will respond to ICMP echo requests from the Profiler Server Appliances. The Profiler Server Appliances in the HA-pair will continuously ping this device regularly to ensure that they still have network connectivity as a measure to detect the failure of their network interface.

Step 2 Install the crossover cable connecting the eth1 interfaces of the existing appliance (Primary) and the appliance being added as an HA peer. Prior to beginning the remaining steps, ensure that the NIC LEDs are indicating link between the appliances (for example, left LED on eth1 interface on both appliances solid amber). Lack of proper link indication is indicative of a problem with the cable used to create the heartbeat connection. Ensure that link is established before continuing.

Step 3 Begin the configuration of the HA pair with the configuration of the Primary appliance (operating standalone system) first. Initiate an SSH or console session with the Primary appliance, and elevate to the root user.

Step 4 Enter the command:

```
service profiler setupha
```

to initiate the HA portion of the appliance startup scripts on the Primary being sure to answer 'yes' when asked if this appliance is the Primary. The script will prompt then prompt for the entry of each of the parameters specified above.

Complete the HA setup of the Primary node.

Step 5 Complete the initial startup scripts on the new appliance being added as the Secondary member of the HA pair, which will run upon logging into the appliance as the root system user for the first time. Ensure that all passwords for the Secondary node are configured to be the same as those set on the Primary.,

Step 6 During the HA-specific portion of the startup script, ensure that 'no' is selected when the script asks if this will be the Primary, and ensure that the HA parameters such as VIP, Local HA Network, and HA authentication key are configured identically to what was configured in step #4 above on the Primary.

Wait several minutes after the completion of the configuration of the Secondary, then utilize the procedure outlined in "Verifying HA-Pair Operation" section on page 18-10 of this chapter to verify proper operation of the HA protocol. Once verification is completed successfully, failover may be tested by simulating failure of the current primary as described in"Forcing a Cisco NAC Profiler Server HA-Pair to Failover" section on page 18-16.

Repairing the Configuration of an HA Pair

From time to time it may be necessary to remove and reinstall the HA service on a NAC Profiler Server HA-pair. There are several scenarios which may cause the HA configuration to fail initially, for example the heartbeat network not being in place between the eth1 interfaces on the members of the pair, as a common example. If NTP is not configured or fails for appliances in an HA-pair and a large discrepancy in system time between the nodes occurs, this may also disrupt operation of an HA-pair.

Also, if key operating parameters of one or both members of an HA-pair such as management interface configuration changes, host name, etc., HA should be removed first and then re-configured once the changes are made.

When it becomes apparent via the HA-pair operation verification procedure describer earlier, or through some other means that the HA protocol is not operating normally, follow the procedure below to first remove the HA protocol on both members of the pair **beginning with the Secondary node**, and then re-initializing the HA configuration on both members.

Step 1 Initiate an SSH or console session with the Secondary node first. Elevate to the root user, and enter the following command to remove the HA protocol and base configuration from the Secondary node of the HA-pair:

```
/root/.resetProfiler  removeHA
```

Follow the on screen instructions, once the HA removal is completed, then proceed to the next step.

Step 2 Initiate an SSH or console session with the Primary node, elevate to root system user access, then use the same command in #1 above to remove the HA configuration from the Primary node.

Step 3 Follow the displayed instructions to permanently remove the HA configuration of the Primary node. When the process is complete, the Primary node becomes the standalone NAC Profiler Server for the system.

Note Performing the steps above results in the VIP being released--neither NAC Profiler Server appliance is using this IP address, both have reverted to the address assigned to their eth0 interfaces. Communication with the UI, and communications between the NAC Profiler Server and Collectors configured with Network Connections of type "Client," as well as communication with the onboard LDAP Server (if enabled) will be disrupted until HA operation is restored.

To re-configure HA on the pair, complete the steps outlined below:

Step 4 Ensure that the heartbeat network is properly configured with a crossover cable between the eth1 interfaces of both members, with link indicated.

Step 5 Prior to continuing the process, ensure that the following parameters specific to the HA pair are verified and readily available in order to complete the re-configuration of the HA pair:

- Verify that NTP is operational on both NAC Profiler Server appliances and that the system clocks are synchronized.
- VIP/Service IP address to be used
- Host name of the Secondary appliance being added as an HA peer, as well as the Host name of the Primary appliance.
- Local HA Network: the first three octets of a private network IP address (for example, 192.168.35) to be used for the heartbeat network between the two appliances (eth1 interfaces).
- HA Authentication Key: a text-string to be utilized by the appliances to authenticate. The HA Shared Key must be entered identically (case sensitive) on both appliances in order for the relationship to be established.
- Redundant Heartbeat Communication, which is the IP address of the alternate system.
- HA External Ping Host: a host IP address of another network device, preferably on the same subnet as the HA pair that will respond to ICMP echo requests from the Cisco NAC Profiler appliances. The Cisco NAC Profiler appliances will ping this device regularly to ensure that they still have network connectivity as a measure to detect the failure of their network interface.

Step 6 Reconfigure the HA protocol beginning with the **Primary** node first. As the root user, issue the following commands on the Primary:

```
service profiler setupha
```

Step 7 Complete the HA setup script for the Primary node e utilizing the parameters determined in step 5 above.

Step 8 Reconfigure the HA protocol on the Secondary node. As the root user, issue the following commands on the Secondary:

```
service profiler setupha
```

Step 9 Complete the HA setup script for the Secondary HA appliance utilizing the parameters determined in step 4 above.

Wait several minutes after the completion of the configuration of the Secondary, then utilize the procedure outlined in "Verifying HA-Pair Operation" section on page 18-10 to verify proper operation of the HA protocol. Once verification is completed successfully, failover may be tested by simulating failure of the current primary as described in the section of this chapter.

Forcing a Cisco NAC Profiler Server HA-Pair to Failover

It may be necessary to force a NAC Profiler Server HA pair to failover; that is to manually initiate the transfer of Primary node duties to the Secondary to ensure that the failover capability of the pair is fully operational. This may be desirable when the HA system is being tested for example, or at anytime it is determined that the Primary duties should be shifted to the other appliance in the HA pair.

Warning **Do not attempt to failover a NAC Profiler Server HA-pair by either of the following methods:**
1. Removing the "Heartbeat" network (eth1-to-eth1 connection between the appliances. This will not cause the pair to failover as heartbeat is maintained on eth1, but it will stop the database synchronization between the Primary and Secondary nodes.
2. Do not use system-level commands to disable the eth0 or eth1 interface on the appliances.

As is described earlier in this Guide, the NAC Profiler Server HA protocol is designed to protect the system implemented as an HA-pair from two potential failure modes:

1. Complete failure of the current Primary as indicated by the loss of heartbeat.
2. Loss of network connectivity by the Primary and determination that the Secondary has better network connectivity.

The latter failure mode is detected by the inability to ping the "ping host" specified in the HA configuration.

Tip Repeatedly forcing an HA pair to fail over without providing ample time for the system to stabilize between transfer of Primary node duties will result in undesirable behavior and may result in the necessity to remove and re-configure the HA protocol in order to return the system to stable operation.

Follow the procedure below to force the failover of an HA pair initiated from the current Primary node:

Step 1 SSH to the physical eth0 interface IP (**not** the VIP) of the current Primary appliance in the HA pair that is to be failed over as beacon system user. If the current Primary node is not known, utilize the procedure in this chapter for determining which node is Primary.

Tip The SSH session should be to the eth0 interface IP and not the VIP so that the session will remain active through the failover.

Step 2 Change directory to /usr/beacon/sql/HA, and run

```
./chk_status_master.sh
```

to verify that the system you are currently on is Primary (script returns “is master”).

Step 3 Switch user to root system user via the **su -** command and entry of the root password.

Step 4 Change directory (cd) to /usr/local/lib/heartbeat.

Step 5 When ready to force failover of the pair, and enter the following command to force the transfer of Primary node responsibilities to the Secondary node:

```
./hb_standby_all
```

Step 6 Wait several seconds, then return to an SSH session to the former Secondary node, which should now be the current Primary node. Verify that this is the case by running the following command as the beacon system user from /usr/beacon/sql/HA:

```
./chk_status_master.sh
```

To verify that the node is now the Primary, the script returns “is master” for the HA pair. At this point, the system should now be operating in HA mode after the swap of the Primary duties. Full verification of the operation of the HA protocol can be verified using the procedure outlined earlier in this chapter. If it desired to fail the system back, the procedure above can be repeated after ample time for database synchronization is allowed as outlined earlier in this section.

Tip Alternatively, the swap of Primary node duties can be initiated from the Secondary node of the HA pair. Verify the eth0 IP of the current Secondary node then SSH to the current Secondary node using that host IP, elevate to the root system user then change directory to /usr/local/lib/heartbeat. Enter the following command to force the Secondary node to take HA resources and become the Primary node:

```
./hb_takeover all
```

Temporarily Disabling HA

High Availability services can be temporarily disabled on an active HA pair. This process can be used to disable failover but not remove the base HA configuration from the members of the pair. To temporarily disable HA, follow these steps:

Step 1 Identify the current Secondary member of the pair, using the procedure specified in this chapter if necessary. Establish an SSH session to the system, and elevate to root access (su).

Step 2 Issue the following command to disable the HA system on the Secondary:

```
/root/.resetProfiler disableHA
```

Step 3 The system will display the following message and request confirmation:

```
[root@BeaconHA2 ~]# /root/.resetProfiler disableHA

This script will disable the HA system but not remove the base configuration.

If you wish to disable the HA system please type 'yes':
```

Step 4 Type 'yes' to continue with disabling the HA system. The following messages are displayed as the HA service is disabled on the Secondary:

```
Stopping the profiler
Cleaning up DB synch files

Starting the profiler

HA disabled on this system.
HA *must* be disabled on the alternate host to prevent
the DB from caching all changes until the drive fills up.

'/root/.resetProfiler restartHA' will restart the HA.
```

Note the message about disabling HA on the other member of the pair. It is important to also disable HA on the Primary node to prevent the Primary from continuing to run the HA service and attempting to keep the database on the Secondary updated after the HA service has been disabled. Without normal communications between the members of the pair, the Primary will cache uncompleted database synch attempts causing several tables in the database to grow large quickly in some cases. This can be prevented by disabling HA on the Primary as outlined below.

Step 5 Repeat the procedure to disable HA services on the Primary:

- **a.** SSH to the eth0 IP address of the Primary node, elevate to root
- **b.** Run the /root/.resetProfiler disableHA script on the Primary.
- **c.** Enter ‘yes’ to continue and observe the shutdown of HA services on the Primary.

Step 6 To restore the HA services using the existing base configuration, begin with the system that was Primary prior to disabling HA for the pair. As root, enter the following command:

```
/root/.resetProfiler restartHA
```

This will result in the following message being displayed:

```
[root@BeaconHA1 ~]# /root/.resetProfiler restartHA

This script will restart the HA system from the base configuration.

If you wish to restart the HA system please type 'yes':

Type ‘yes’ to continue and observe the following messages as the service restarts on the
Primary member of the pair:

Stopping the profiler
Restarting the HA

Stopping heartbeat.  This may take more than three minutes.
Stopping High-Availability services:
Done.
```

```
Starting High-Availability services:
2009/03/03_15:33:18 INFO:  Resource is stopped
Done.

HA *must* be running/restarted on the alternate host to prevent
the DB from caching all changes until the drive fills up.

[root@BeaconHA1 ~]#
```

Step 7 Repeat the same procedure on the Secondary to restart HA services on the other member of the HA pair, verifying the successful restart of the service on the Secondary.

The HA pair is now restored to normal operation and HA operation can be verified using the procedures outlined in this chapter.

Permanently Removing the HA Configuration

If it becomes necessary to remove HA services permanently on a Cisco NAC Profiler Server appliance, use the following procedure to completely remove the base HA configuration from the appliances that are currently operating in HA mode. This might be necessary when it is desirable to return an operating NAC Profiler Server back to a single appliance, stand alone mode.

Note that at the completion of this procedure, the appliance that was Primary for the pair at the outset is now configured to operate as the standalone NAC Profiler Server after removal of HA. The appliance that was the Secondary node of the pair, will require reconfiguration prior to re-employment of the appliance. Preferably the appliance should be re-imaged via ISO to ensure that the existing configuration and database are completely cleared.

Step 1 SSH to the appliance eth0 IP address of the current Secondary node in the HA pair and elevate to root access.

Step 2 Run the following script to permanently remove the HA base configuration on the Secondary node:

```
/root/.resetProfiler  removeHA
```

Step 3 Perform the steps above on the Primary node to remove the base HA configuration on the Primary.

Step 4 Restart the Primary system using

```
service profiler restart
```

Step 5 Upon the restart, the former Primary node of the pair is now acting as a standalone NAC Profiler Server.

Step 6 Remove the crossover network cable connecting the appliances previously in the HA pair configuration.

Step 7 If the appliance that was the Secondary prior to the removal of the HA configuration is to be re-used, it is highly recommended that the appliance have the NAC Profiler Server software re-installed via ISO on that appliance to ensure that all configuration and database data is removed before reconfiguration.

Returning a Cisco NAC Profiler Server to Factory Defaults

In some cases it may be desirable to delete all configuration information on a Cisco NAC Profiler Server appliance to return it to a "factory default" state. For example, when a serious error in configuration is made and it is desirable to start from a clean configuration this procedure will stop, remove and replace the Profiler Server system, allowing the startup scripts to be run again to correct the configuration issues.

Tip Note that this procedure is **not** intended for use on systems that have been configured and used in lab or production environments. The proper way to return systems that have been configured and used is to re-image the appliance via ISO.

The following procedure will restore a Cisco NAC Profiler Server appliance to factory defaults during the configuration process:

Step 1 Initiate a console session to the system to be restored to factory defaults and elevate to root access. (SSH can be used as well, as long as the IP parameters of the appliance will remain unchanged.)

Step 2 Enter the following command to initiate the factory default script:

```
/root/.resetProfiler factory
```

Step 3 When the script initiates, it will display the following message at the terminal and requires user input to continue:

```
This script will stop, remove, and replace the Profiler. Its intended use is to clean up
an incorrectly configured installation. It should not be used on a system that has already
been installed and used in a production network.

If you wish to reset the Profiler please type 'yes':
```

Step 4 To proceed, type 'yes' at the colon and press Enter.

Step 5 At the completion of the script, the command prompt will return. Logout of the system entirely, and then re-login as root. (The passwords for the root and beacon system users will **not** be changed by the factory default reset script). The appliance startup scripts will initiate with the following message at the terminal upon logging back in as root.

```
Welcome to the Beacon Endpoint Profiler.

Hit any key to create the initial configuration (or ^c to exit):
```

Step 6 Press enter to continue with the configuration of the Cisco NAC Profiler Server appliance.

Changing the beacon and root System User Account Passwords

Each Cisco NAC Profiler Server appliance has two system user accounts used for command-line operations with the appliance.

The password for the beacon and or root system user accounts used on a Cisco NAC Profiler appliance can be changed using the following procedure:

Step 1 Start a console or SSH session with the target appliance as root user (elevate to root using su if using SSH) and enter the following command:

`passwd beacon` - to change the beacon password

`passwd root` - to change the root password

Note The above procedure requires knowledge of the root system user password for the appliance. If it is lost, a password recovery process is required to reset the root system user password. Contact the Cisco TAC for the system user password recovery procedures.