CHAPTER 6

NAC Profiler Server Configuration

This chapter contains the following topics:

Overview

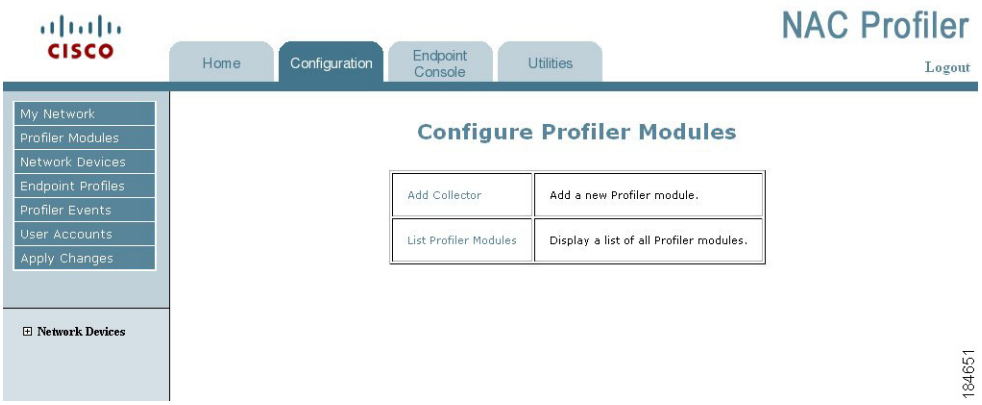
The next task associated with configuration of Cisco NAC Profiler is configuration of the NAC Profiler Server. Recall that the web-based management interface is served by the NAC Profiler Server and it provides management of all components of the system including modules running on the NAC Profiler Collectors. Correct configuration of this component at the outset ensures that the initial system configuration can be created and the system brought into service.

When the NAC Profiler Server is initialized as described in Chapter 4, “Installation and Initial Configuration”, a very basic system configuration is created, including initial configuration for the Server module itself. The basic server configuration includes default parameters that allow the system to come up and be managed via the web interface so that further configuration can be completed to enable the system for endpoint profiling and behavior monitoring in the target environment. The NAC Profiler Collector modules are initialized with the parameters required to communicate with the Server over the network in order to get their completed configuration and send data back to the Server for processing. Once the Server is configured as described in this chapter, communication with the Collectors will be established, and their configurations added to the system configuration and completed as described in the next chapter.

Profiler Module Configuration

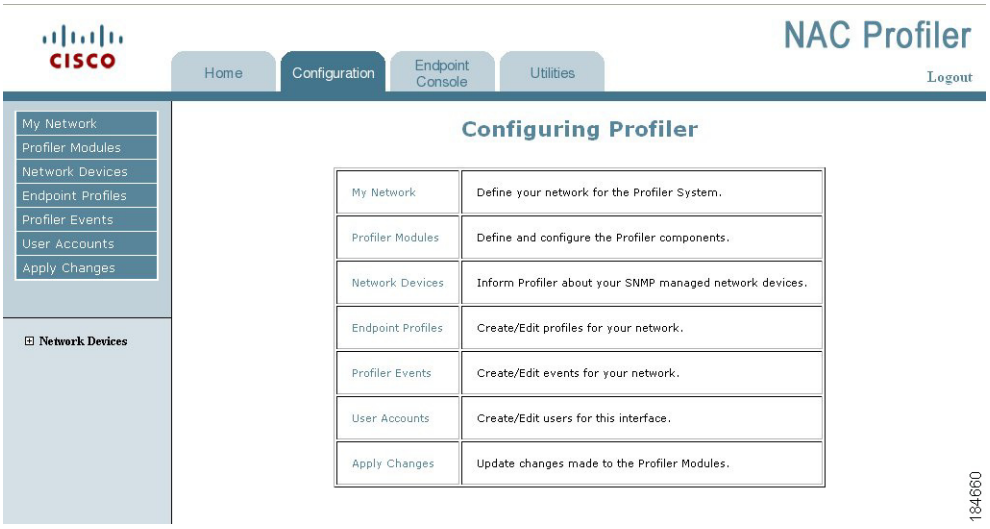
The configuration of Profiler module instances in Cisco NAC Profiler configuration is accomplished through the Configuration Tab of the management interface, by selecting the **Profiler Modules** option from the left hand navigation pane. Figure 6-1 shows a table in the main pane which contains a link for adding a Collector module, and another for listing the Profiler modules (e.g., Server and Collectors) currently saved to the system configuration.

Figure 6-1 Configure Profiler Modules Page



Selecting the List Profiler Modules link from the table in the main pane presents a page containing two tables: one showing the NAC Profiler Collector modules currently saved to the configuration and their respective status, and another showing the NAC Profiler Server and its status (see Figure 6-2). The Collector module names and Server are hot-links which if selected, open the edit/configuration view for the selected module.

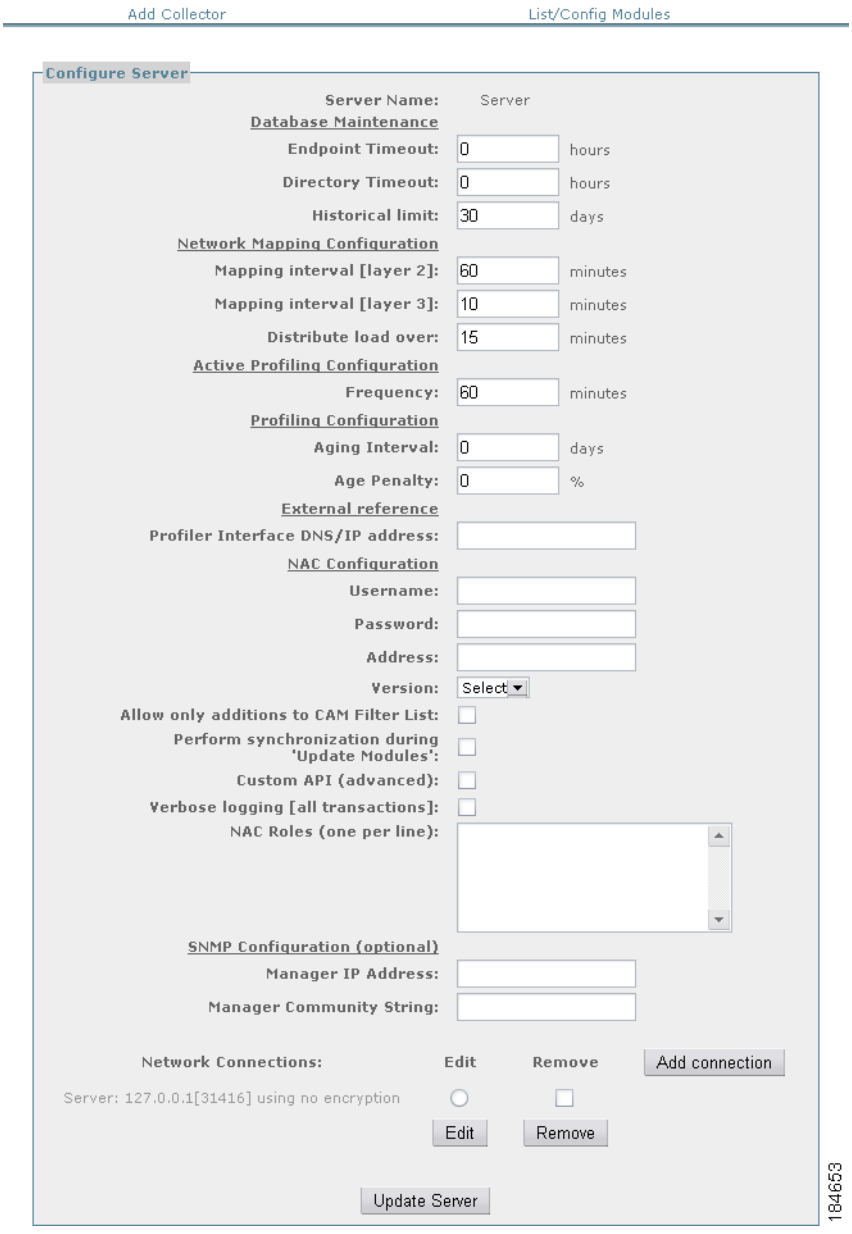
Figure 6-2 Table of Modules



Editing the Server Configuration

To edit a Server module, navigate to the Table of Modules as described above. Select the server name link ('Server') from the Table of Servers to bring up the Configure Server form (see Figure 6-3).

Figure 6-3 Server Configuration Form



The Configure Server form is divided into seven sections or areas of related configuration parameters that define how the Server module will operate, and a list of all Network Connections currently configured for the Server.

The first four sections are mandatory Server module configuration parameters and are populated with default values for Server modules initialized at appliance start-up. The second four sections are optional configuration parameters and are utilized as desired. There are no default values for these parameters.

The following outlines the purpose of each of the Server configuration parameters found in each of the eight sections as well as the Network Connections.

1. Database Maintenance

Endpoint Timeout

Specifies a time value (in hours) that the NAC Profiler engine will wait without a refresh of endpoint data before removing port mapping information for an endpoint, and disassociating IP information from the MAC address of the endpoint in the database. This parameter is designed specifically for environments in which NAC Profiler is unable to utilize SNMP traps for detecting the disconnection of an endpoint from an access port. It is designed specifically to prevent endpoint location data from becoming stale in the absence of real-time notifications of topological changes that would normally be indicated by SNMP traps from the edge infrastructure.

Note that endpoints that have their port mapping and IP data removed because of expiration of the Endpoint Timeout value are not removed from the NAC Profiler database completely. All information derived about the endpoint based on MAC address remains in the database.

The default value of this parameter is 0 hours, which is interpreted as no timeout value set which is typical for configurations where traps can be sent to NAC Profiler. If traps are not available, set the number of hours NAC Profiler will wait without a refresh before removing port mapping and IP information about endpoints from the database.

Directory Timeout

Specifies a time value (in hours) that the NAC Profiler engine will wait without a refresh of the data used for making a Profiling decision on an endpoint before timing the endpoint out of the Endpoint Directory. This timeout can be used to prune endpoints that have left the network and either have not returned to the network, or will not return. This can be used to prevent the endpoint directory from growing too large in dynamic environments. If the endpoint being timed-out of the Endpoint Directory is in a Profile that matches a CCA Event, the endpoint is removed from the Endpoint Directory and a Remove MAC event is triggered that results in the endpoint being removed from the Device Filter List of the CAM (see Chapter 11, “Integration with Cisco NAC Appliance,” for more information on NAC Profiler integration with NAC Appliance.

The default value of this parameter is 0 hours, which is interpreted as no timeout value set. If it is desirable to in the absence of regular refreshes of Profiling data on an endpoint to time the endpoint out of the Directory (and out of the Device Filter List if integration with NAC Appliance is configured), set this value to an appropriate value in hours. Consideration should be given to the rule(s) bound to the applicable Profile and the specifics of the environment and operating characteristics of the device to determine the value selected for this parameter.

Historical Limit

Specifies a time value (in days) that NAC Profiler will maintain historical data on endpoints in the database. The default value is 30 days which means that historical information about each MAC address and each IP address in the database is available within the system for up to 30 days into the past. Data older than 30 days is removed from the database, preventing the database from growing without bounds.

Increasing this parameter should take into consideration the number of endpoints and other environmental characteristics to ensure that the system does not exhaust hard disk space.

2. Network Mapping Configuration

Mapping Interval [Layer 2]

Defines how often (in minutes) the NetMap module(s) running on the NAC Profiler Collectors will poll Layer 2 devices (switches) for information via SNMP. (Default is 60)

Mapping Interval [Layer 3]

This parameter defines how often (in minutes) the NetMap module(s) running on the NAC Profiler collectors will poll Layer 3 devices (routers) in the database for information via SNMP. (Default is 10).

Distribute Load Over

Specifies a time value (in minutes) over which to distribute the SNMP polling of network devices in the system configuration. The NetMap module was designed to allocate the SNMP polling of network devices over a defined period of time to make efficient use of NAC Profiler system and network resources. This value specifies the time period over which that distribution should occur. The default value is 15 minutes.

For each NetMap module in the system, the number of network devices assigned for polling is divided that by the value of this parameter to determine how many devices will be polled each minute by the NetMap module. The NetMap module(s) will in turn spawn a worker for each device. If the number of devices is greater than the Maximum allowed workers as specified in the NetMap module configuration (see Chapter 7, "Configuring Cisco NAC Collector Modules"), NetMap will queue these requests. If the Distribute Load Over parameter is set to 1 it will do all requests at once.

The following example shows how this calculation is made for a given NetMap module with n number of network devices assigned to it, with this parameter set to the default value of 15 minutes.

```
Example:
Network Devices assigned to NetMap = 60
Distribute Load Over value = 15
Devices per Bucket = (60/15) = 4
```

Therefore at the top of each minute for a total of 15 minutes, 4 XML requests are sent to the NetMap module, initiating 4 NetMap workers, each worker polling a network device.

Note There could be more NetMap workers than devices per bucket at any given time, if the workers from previous minutes are still working. Additionally, workers may be spawned for traps that have been received. However, there should never be more than the maximum allowed workers (plus the main NetMap process).

3. Active Profiling Configuration

Frequency

Specifies the polling interval (in minutes) the NetInquiry module(s) running on the NAC Profiler Collectors will perform their active profiling function. (Default is 60 minutes).

See Chapter 7, "Configuring Cisco NAC Collector Modules," and Chapter 9, "Configuring Endpoint Profiles," for an in-depth discussion of both the NetInquiry module and the Active Profiling capabilities of Cisco NAC Profiler.

4. Profiling Configuration

These parameters are used to age the individual Profiling data elements gathered by Cisco NAC Profiler about an endpoint over time. Each element of Profiling data about an endpoint observed by NAC Profiler is tagged with a time-based confidence value which is set to 1.0 the first time the data

is seen, and reset to that value each time NAC Profiler observes the endpoint behavior. The parameters below specify how each of the individual Profiling data elements will be timed-out by NAC Profiler if they are not re-observed within a defined period of time.

a. **Aging Interval.** Specifies a time value (in days) to wait for a refresh before decrementing the confidence value for each data element.

b. **Age Penalty.** Specifies a value (%) to decrement the confidence value with the expiration of an Aging Interval without a refresh of Profiling data.

For example, if a DHCP request from an endpoint was observed by NAC Profiler at time = 0, that DHCP data element would be tagged with a confidence value of 1.0 (100%). If an Aging Interval was set to 4 days, with an Age Penalty of 25% and another DHCP request was not observed by NAC Profiler for four days, the confidence value of that data element would be decremented from 100% to 75%. If no DHCP request was observed for 4 Aging Intervals (e.g., 16 days), then the DHCP information would have a confidence value of 0, and that information would no longer be used for Profiling that endpoint.

5. External Reference (Required for integration with Cisco NAC Appliance)

Profiler Interface DNS/IP address

Enter the hostname (preferred) or IP address of the NAC Profiler Server. The hostname or IP address entered here will be made part of a web link that will be embedded in the description field of each entry that NAC Profiler creates in the CAM Device Filter List. These web links give the administrator the ability to easily link to the NAC Profiler endpoint database to find out more details about endpoints entered into the Device Filter List directly from the CAM interface.

6. NAC Configuration

The parameters in this section are specific to NAC Profiler integration with Cisco NAC appliance. Configuration of integration of Cisco NAC Profiler with NAC Appliance requires configuration of both Server module parameters, as well as configuration of endpoint events specific to NAC Appliance integration.

Refer to Chapter 11, "Integration with Cisco NAC Appliance," for a complete explanation of these parameters and instructions on configuration of Profiler integration with Cisco NAC Appliance.

7. SNMP Configuration (Optional)

Cisco NAC Profiler is capable of sending SNMP traps when endpoint events (see Chapter 11, "Integration with Cisco NAC Appliance") occur. Configure these parameters to instruct Cisco NAC Profiler to send traps to an external trap server such as the NMS.

Manager IP Address

Enter the IP address of the system that should receive SNMP traps from Cisco NAC Profiler if desired.

Manager Community String

Enter the community string for the trap receiving system specified above. This is required for the NAC Profiler traps to be received by that system.

Network Connections

This configuration parameter specifies how the NAC Profiler Server will communicate with the NAC Profiler Collectors deployed in the system.

During appliance start-up, the NAC Profiler Server will have a Network Connection added to the configuration by default. This Network Connection, added for purposes of enabling communication with the internal (non-configurable) Forwarder module running on the NAC Profiler Server, is identifiable by

the IP address specified: 127.0.0.1, the internal loop back interface, with a Connection Type of Server. This can be interpreted as specifying that the Server module listen on the internal loop back interface for sessions initiated on port 31416.

Note For NAC Profiler systems, the Network Connections section of the NAC Profiler Server configuration must be modified such that communications between the NAC Profiler Server and the Forwarders running on the NAC Profiler Collectors is enabled. To add a Network Connection to a Server module configuration, complete the procedure below.

As outlined in Chapter 3, "Preparing for Deployment," when configuring NAC Profiler systems it is necessary to have information about all components in the system such as IP addresses and desired encryption shared secrets readily available. This ensures that the configuration of Server to Collector communications can be accomplished readily.

Add a Network Connection to a Server

To add a new Network Connection to a Server module configuration, select the Add connection button. The Add network client/server form that allows specifying the configuration parameters of the Network Connection to be added to the server configuration is displayed in the main pane. See Figure 6-4.

Figure 6-4 Add Network Client/Server Form (Server)

This form allows the specification of each of the required parameters of the Network Connection being added to the Server module configuration which will enable bidirectional communications between the Server and another NAC Profiler module (typically the Forwarder modules on NAC Profiler Collector appliances) in the system. Each of these parameters is described in detail below.

Connection Type

The Connection Type specifies how this Network Connection between the Server module and external modules will be initially established. Selecting the **Server** radio button specifies that the Server module will expect the Network Connection(s) to be established by the *other* module and that it should listen for connections on the specified TCP port number. Selecting the **Client** radio button specifies that the Server module itself should initiate this Network Connection with the other module.

IP Address

For Connection Types specified as "Server" as described immediately above, enter the IP address of the local interface(s) on the appliance the Server module should listen on for connections from remote modules—typically its management interface, eth0. For example, if the Management interface of the NAC Profiler Server appliance edited was assigned the address 169.254.222.1,

adding a Network Connection with this address specified would result in the Server module listening for TCP connections on the specified port number on the Management interface of the appliance. Remote modules would be able to communicate with the Server by initiating TCP connections to the IP address of the Management interface of the appliance running the Server.

For Connection Types specified as “Client” the IP address entered should be the IP address of the remote module the Server will initiate a session. For example, when adding a Network Connection to a Server module to establish communication with a Forwarder module on a NAC Profiler Collector appliance, specify the IP address of the Management interface of that NAC Profiler Collector appliance in this field.

Port

For most cases the default TCP port number of 31416 should be accepted, however an alternative available layer 4 port value may be specified. This is the port number that the Network Connection being added will utilize for module-to-module communications.

Encryption Type

Select the desired encryption type for the Network Connection being added from the drop-down list. This parameter specifies either that the Network Connection will be unencrypted (select the None option), or the algorithm to use for encrypting the data being transmitted. Currently available encryption options are AES (default), Blowfish, or Twofish. The Network Connection of the modules at both ends of the Network Connection must have the same encryption algorithm selected in order for encrypted session to be successfully established.

Shared Secret

Specify the shared secret that should be used in establishing encrypted communications over the Network Connection to be added, if desired. The field should be left blank if the Network Connection will be unencrypted. The modules at both ends of the Network Connection must be configured with the identical Shared Secret in order for the encrypted session to be established successfully.

The NAC Profiler Collector appliances are configured at startup with the parameters they require such as Connection Type, Encryption Type, Shared Secret and address information as required to complete the configuration of the Forwarder end of the communication. This enables bidirectional communication with the Server module for the system so that the NAC Profiler Collectors are able to get their detailed configuration from the Server. It is good practice to plan and document these parameters for the entire system at the outset of system configuration to ensure system-level communication can be established efficiently. Refer to Configuring the Collector on the Clean Access Server, page 4-36 for additional details.

Select the Add Connection button to save the new Network Connection to the Server Configuration, and return to the Configure Server from, which should now display the Network Connection just added.

Editing a Server Network Connection

To edit an existing Network Connection in a Server module configuration, select the Edit radio button to the right of the Network Connection to be edited. Then select the Edit Button. The Edit network client/server form is displayed which reflects the current configuration and allows each of the Network Connection parameters to be edited as required (see Figure 6-5). Refer to the previous section for a description of each of these parameters.

Figure 6-5 Edit Network Client/Server Form

Once the desired changes are made to an existing Network Connection, select the Edit Connection button to save the edits to the configuration, and return to the Configure Server form.

Removing a Server Network Connection

To remove a Network Connection from a Server module configuration, select the Remove checkbox to the right of the Network Connection or Connections to be removed. Selecting the Remove button will result in the removal of the selected Network Connection or Connections from the Server module configuration.

Saving Edits to a Server Module

When all desired changes have been made to the configuration of the Server module being edited, select the Update Server button at the bottom of the Configure Server form. Selecting the Update Server button results in the browser returning to the Table of Modules page, and a message displayed at the top of the main pane that the server configuration has been saved.

The changes to the Server module configuration are not committed to the running configuration until the Apply Changes -> Update Modules procedure is performed as described at the end of the previous chapter.

Configuring NAC Profiler Server High Availability (HA)

NAC Profiler Server is capable of operating in a High Availability (HA) mode, where a second appliance acts as a backup to the primary NAC Profiler Server. When a NAC Profiler Server is initially set up as described in Chapter 4, "Installation and Initial Configuration," the system is set up as either a single appliance or High Availability pair. Refer to the step-by-step instructions in Configure a Cisco NAC Profiler Server HA Pair, page 4-18 to configure a High Availability NAC Profiler Server pair. The remainder of this section provides an overview of the operation of the High Availability feature.

The following key points provide a high-level summary of HA-NAC Profiler Server operation:

- The NAC Profiler Server high-availability mode is an Active/Passive two-appliance configuration in which a standby NAC Profiler Server acts as a backup to an active NAC Profiler Server.
- The active NAC Profiler Server performs all tasks for the system. The standby NAC Profiler Server monitors the active NAC Profiler Server and keeps its database synchronized with the active NAC Profiler Server's database.
- Both NAC Profiler Servers share a virtual Service IP for the eth0 (management) interface.
- The primary and secondary NAC Profiler Servers exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.
- The eth1 interface on the NAC Profiler Servers can be used for heartbeat packets and database synchronization.

NAC Profiler Server high-availability mode is an Active/Passive two-appliance configuration in which a standby NAC Profiler Server appliance acts as a backup to an active NAC Profiler Server appliance. While the active NAC Profiler Server carries most of the workload under normal conditions, the standby monitors the active NAC Profiler Server and keeps its data store synchronized with the active NAC Profiler Server's data. The data store includes system configuration information as well as the endpoint database.

If a failover event occurs, such as the active NAC Profiler Server is shut down or stops responding to the peer's "heartbeat" signal, the standby assumes the role of the active NAC Profiler Server.

When first configuring the HA peers, you must specify an HA-Primary NAC Profiler Server and HA-Secondary NAC Profiler Server. Initially, the HA-Primary is the active NAC Profiler Server, and the HA-Secondary is the standby (passive) NAC Profiler Server, but the active/passive roles are not permanently assigned. If the primary NAC Profiler Server goes down, the secondary (standby) becomes the active NAC Profiler Server. When the original primary NAC Profiler Server restarts, it assumes the backup role.

When the NAC Profiler Server starts up after HA is configured, it checks to see if its peer is active. If not, the starting NAC Profiler Server assumes the active role. If its peer is active as it starts up, the starting NAC Profiler Server becomes the standby.

Two NAC Profiler Servers may be configured as an HA pair at the same time as the system is implemented, or a new NAC Profiler Server may be added to an existing standalone NAC Profiler Server to create a high-availability pair at any time. In order for the pair to appear to the network and to the Clean Access Manager as a single entity, a **Service IP address** must be specified as the trusted interface (eth0) address for the HA pair.

To create the crossover network on which high-availability information is exchanged, the eth1 ports of both NAC Profiler Servers are connected and a private network address not currently routed in your organization (the default HA crossover network address is 192.168.0.252) is specified. NAC Profiler Server then creates a private, secure two-node network for the eth1 ports of each Server to exchange UDP heartbeat traffic and synchronize databases. Note that the NAC Profiler Server always uses eth1 as the UDP heartbeat interface.

Note To prevent any possible data loss during database synchronization, always make sure the standby (secondary) NAC Profiler Server is up and running before failing over the active (primary) NAC Profiler Server.

Before configuring high availability on a NAC Profiler Server pair, ensure that:

- Both NAC Profiler Servers are installed and configured.
- For heartbeat, each Server needs to have a unique hostname (or node name). For HA NAC Profiler Server pairs, this host name will be provided to the peer, and must be resolved via DNS or added to the peer's /etc/hosts file.
- The HA-Primary NAC Profiler Server is fully configured for runtime operation of Cisco NAC Profiler. This configuration is automatically duplicated in the HA-Secondary (standby) Server.
- Both NAC Profiler Servers are accessible on the network (try *pinging* them to test the connection).
- The NAC Profiler Server appliances both have Ethernet port (eth1) available.
- Port Security is not enabled on the switch interfaces to which the NAC Profiler Servers are connected. This can interfere with NAC Profiler Server HA and DHCP delivery.