CHAPTER 13

Cisco ANA Administration

These topics describe information to help you administer your Cisco ANA network by adding and moving VNEs, adding users and scopes, and so forth. These topics also explain how to maintain the machines on which Cisco ANA is running; for example, backing up the system, applying software updates, and checking overall system health using the diagnostics software.

Information describing backend services, processes, and logs that are part of the Cisco ANA system are described in *Cisco Active Network Abstraction Installation and Setup Guide*. The installation guide also lists the ports used by Cisco ANA.

For information on how to use the system health and diagnostic tools, which provides information about basic system and database health and other diagnostic information, see Cisco ANA System Health and Diagnostics, page 14-1.

Most of the administrative functions are performed from the Administration perspective. You must have Administrator privileges to use these functions:

- Managing Jobs, page 13-2
- Creating a Banner (Message of the Day), page 13-4
- Managing Polling Groups, page 13-5
- Managing Protection Groups and High Availability, page 13-9
- Trap Forwarding, page 13-23
- Specifying Global Settings for Cisco ANA Features, page 13-25
- Creating and Managing Users, Passwords, and Scopes, page 13-34
- System Security, page 13-45
- Backing Up and Restoring Data, page 13-47
- Installing Updates and Patches, page 13-50
- Understanding the Cisco ANA Registry, page 13-52

Managing Jobs

Administrators can perform all job management functions on all jobs; however, users can fully manage only the jobs that they create and own. Jobs are also limited by user scopes and security privileges. For example, if a workflow job is running on several devices, users can check the job status for only those devices within their scope. A job will fail if the creator is removed from the system before their jobs finish, or if their security privileges or scope is downgraded from what was set when the job started.

Use the Job Management function to administer jobs that have been scheduled, such as system backups. Jobs cannot be edited; to change it, you must delete the old job and create a new job.

See these topics for the following information:

- To familiarize yourself with the Job Management user interface and tool buttons, see Understanding the Job Management User Interface, page 13-2.
- For instructions on how manage a job (create, delete, suspend, and so forth), see Browsing and Controlling Jobs, page 13-3.

Understanding the Job Management User Interface

Figure 13-1 shows the Job Management user interface, listing the jobs that Cisco ANA is currently managing.

Figure 13-1 Job Management User Interface

The following tool buttons are located at the top right of the Job Management workspace.

Table 13-1 Job Management Icons

Icon	Tooltip	Description
📅	Schedule Job	Schedules a job to run immediately or at a future date
⏸	Suspend Job	Suspends a job after it has finished running
▶	Resume Job	Resumes a suspended job

Table 13-1 Job Management Icons

	Delete Job	Deletes a job from the Job Management workspace (without purging the historical information)
	Purge Job	Removes all historical job information after a user-specified number of days
	Cancel Job	Cancels a job (including all future invocations of the job) but does not remove it from the Job Management workspace

Roles Required to Use Job Management

If you created a job, you can perform all of the Job Management functions listed in Table 13-1, except for job purging. Only users with Administrator privileges can perform all Job Management functions. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Related Topic

- Browsing and Controlling Jobs, page 13-3

Browsing and Controlling Jobs

To browse and control jobs:

Step 1 In the Administration perspective, click the **Tasks** tab and click the **System Settings** drawer.

Step 2 Click **Job Management**. The Job Management page lists the following information:

Column Heading	Description	
Job Description	Description provided by the job creator.	
Job ID	A unique identifier assigned to the job by Cisco ANA. The ID stays the same throughout the job's life cycle.	
State	NOT_SCHEDULED_OR_NEW	The job was created but not scheduled.
	SCHEDULED	The job is scheduled to run in the future.
	RUNNING	The job is running.
	COMPLETED	The job is completed and no longer runs (terminal state).
	SUSPENDING	The job suspends upon completion of the current job.
	SUSPENDED	
	CANCELLING	The running job was canceled, and the processing is being terminated.
	CANCELLED	The job was canceled from any future invocations (terminal state).
Time Submitted	Date and time when the job was first created.	

Column Heading	Description
User	User who created the job. Only the user who created the job, or a user with Administrator privileges, can suspend, resume, cancel, or delete the job.
Priority	Level of importance (internally defined by Cisco ANA).

Step 3 For more information about a specific job, double-click the job. Cisco ANA displays the following information:

- The elapsed time (if the job is currently running), and the time the job is scheduled to run next.
- Historical information about the job.

Step 4 Right-click the job and choose one of the following choices, as needed: Cancel, Purge, Delete, Resume, Schedule, or Suspend.

Purging deletes all historical information. When you select Purge, Cisco ANA prompts you to specify the number of days to keep the information.

You can apply only one schedule to a job. When scheduling a job, you are prompted to indicate scheduling information such as start date, number of times the job should run, and delay interval between jobs (how long to wait between job initiations).

Step 5 Confirm your choice.

Related Topic

- Understanding the Job Management User Interface, page 13-2

Creating a Banner (Message of the Day)

You can configure a banner that is displayed whenever a user logs into the Cisco ANA system. You must acknowledge the message to use Cisco ANA.

Roles Required to Create a Message of the Day

You must have Administrator privileges to create a banner. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Creating a Banner

If you do not want to display a banner, simply leave the Message of the Day fields empty.

To create or edit a banner:

Step 1 In the Administration perspective, click the **Objects** tab and click the **System Settings** drawer.

Step 2 Click **Message of the Day**.

Step 3 Enter or change the title and the message text.

Step 4 To save your changes, click the Save icon in the main toolbar.

The message displays when any users log in to the Cisco ANA system.

Managing Polling Groups

When you add a VNE to Cisco ANA, one of the areas you configure is the polling settings. As described in Defining and Creating Individual VNEs, page 2-35, you have two options for specifying the polling parameters for the VNE:

- Click **Instance** and configure individual polling settings to be applied only to that network element
- Click **Group** to choose an existing polling group and use the group's settings

These topics describe the second option—polling groups—and how they work.

The units poll the network elements to discover and display accurate and up-to-date information about the network. The system periodically triggers polling at set intervals. The polling rates can be customized or optimized by a user with Administrator privileges. You can fine-tune the frequency with which information is retrieved from the managed elements to enable a high degree of control and flexibility over the amount of network traffic used by the various VNEs.

Cisco ANA polls only network elements that are in the Managed state.

Polling intervals depend on the type of information that is being queried. The intervals represent the amount of time between investigations of the network element for the data specified. You can adjust these intervals as described in Creating or Customizing a Polling Group, page 13-8. Two polling groups, and *slow*, are already configured with Cisco ANA, and are described in Table 13-2.

Table 13-2 Polling Rates for and Slow Polling Groups

		Settings	
Polling Type	**Description**	**"default" Group**	**"slow" Group**
Status	Sets the polling rate for status-related information, such as network element status (up or down), port status, admin status, and so on. The information is related to the operational and administrative status of the network element.	180 seconds (3 minutes)	360 seconds (6 minutes)
Configuration	Sets the polling rate for configuration-related information, such as VC tables, scrambling, and so on.	900 seconds (15 minutes)	1800 seconds (30 minutes)
System	Sets the polling rate for system-related information, such as network element name, network element location, and so on.	86,400 seconds (24 hours)	172,800 seconds (48 hours)
Layer 1	Sets the polling rate of the topology process as an interval for the Layer 1 counter. This is an ongoing process.	30 seconds	30 seconds
Layer 2	Sets the polling rate of the topology process as an interval for the Layer 2 counter. This process is available on demand.	30 seconds	30 seconds

Adaptive Polling

In addition to defined polling intervals, VNEs implement adaptive polling to make sure that the element is not overloaded. For example, if CPU usage is high, Cisco ANA may defer some polling to avoid overloading the managed element.

Note Adaptive polling is not supported on all devices. For information on the devices that do and do not support it, see *Cisco Active Network Abstraction VNE Reference*.

When a VNE exceeds the maximum CPU usage threshold value, an alarm is sent, and the VNE is automatically transferred to a slow polling interval. For example, the VNE is polled less regularly and a delay is added between the commands. When the CPU usage threshold values for the VNE fall below the clear threshold value, an alarm is sent and the VNE returns to normal polling.

Note Contact ask-ana@cisco.com if you want to customize the values (for example, minimum and maximum CPU usage threshold values).

When a VNE is using normal polling and CPU usage is high, Cisco ANA waits for the maximum CPU usage threshold value (upper tolerance level) to be exceeded 5 times (the default), and then the VNE adds a delay between , as shown in Figure 13-2.

Figure 13-2 Polling Threshold Levels

If the VNE is using slow polling after it has been checked 5 times, then it is checked 10 more times (the default) to see whether the CPU usage is still high. If usage remains high, the VNE is moved to Maintenance mode. When the VNE is in Maintenance mode, it is not polling the network element. (See Understanding VNE Status and VNE States, page 2-17.)

Note Once the VNE is in maintenance mode, you must manually set it back to normal polling (it does not automatically return to regular polling).

In Figure 13-3, CPU usage is polled 5 times. Because CPU usage is above the maximum value, the VNE introduces a delay between sending packets (SNMP) or CLI commands (Telnet/SSH). The CPU usage is then polled 10 more times. Because CPU usage remains above the maximum value, it is moved to Maintenance mode.

Figure 13-3 Polling and CPU Usage—VNE Remains at Unacceptable Level

When the VNE is using slow polling and CPU usage drops to an acceptable level (below the minimum threshold value), Cisco ANA continues to poll the VNE. If the VNE remains at that level for two consecutive polls, Cisco ANA returns the VNE to normal polling.

In Figure 13-4, CPU usage is polled 5 times. Because the usage remains above the maximum value, the VNE is moved to slow polling. However, in this case, CPU usage returns to an accepted level (below the minimum value). The VNE is polled twice more, and because CPU usage remains at an acceptable level, it is moved back to its normal polling.

Figure 13-4 Polling and CPU Usage—VNE Returns to Acceptable Level

If CPU usage is high and a slow polling interval is used, and the AVM goes down and is then restarted, the AVM maintains the slow polling interval for the VNE.

Related Topics

- Creating or Customizing a Polling Group, page 13-8

- Deleting a Polling Group, page 13-9

Roles Required to Manage Polling Groups

Table 13-3 lists the roles that are required to manage polling groups. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Table 13-3 Roles Required to Manage Polling Groups

Task	Role Required
Creating or editing a polling group	Administrator
Deleting a polling group	Administrator

Related Topics

- Managing Polling Groups, page 13-5
- Creating or Customizing a Polling Group, page 13-8
- Deleting a Polling Group, page 13-9

Creating or Customizing a Polling Group

Reviewers: Should we recommend that users do NOT change the ‘’ and ‘slow’ groups?

You can create a new polling group to be used when defining a VNE. For more information, see Managing VNEs, page 2-16. If you change an existing polling group, the changes affect all VNEs and network elements using that polling group.

Caution Changing the polling rates may result in excess traffic and network element crashes.

To create or customize a polling group:

Step 1 In the Administration perspective, click the **Objects** tab and click the **System Settings** drawer.

Step 2 Right-click Polling Groups and choose **New Polling Group,** or choose an existing polling group. You cannot edit the polling group.

Step 3 Complete the required information:

- General:
  - Name—A polling group name that you define.
  - Description—A description of the polling group.
- Polling Intervals (all rates are in seconds):
  - Status—Sets the polling rate for status-related information, such as network element status (up or down), port status, admin status and so on. The information is related to the operational and administrative status of the network element.
  - Configuration—Sets the polling rate for configuration-related information, such as VC tables, scrambling and so on.

- System—Sets the polling rate for system-related information, such as network element name, network element location and so on.
- Routing Forwarding—Sets the polling rate for routing table-related information, such as VRF and IGP/BGP routes.

- Topology (all rates are in seconds):
  - Layer 1—Sets the polling rate of the topology process as an interval for the Layer 1 counter. This is an ongoing process.
  - Layer 2—Sets the polling rate of the topology process as an interval for the Layer 2 counter. This process is available on demand.

Step 4 Click **OK**. The new polling group is displayed in the user interface.

The new polling group can be used when defining a new VNE. See Managing VNEs, page 2-16.

Related Topics

- Managing Polling Groups, page 13-5
- Roles Required to Manage Polling Groups, page 13-8
- Deleting a Polling Group, page 13-9

Deleting a Polling Group

You can delete polling groups as long as they are not being used by any VNEs or network elements. You cannot delete the polling group.

To delete a polling group:

Step 1 In the Administration perspective, click the **Objects** tab and click the **System Settings** drawer.

Step 2 Click **Polling Groups**, right-click the group you want to remove, andchoose **Delete**.

Step 3 Confirm that you want to delete the group.

The polling group is deleted from the Polling Group table.

Related Topics

- Managing Polling Groups, page 13-5
- Creating or Customizing a Polling Group, page 13-8
- Roles Required to Manage Protection Groups, page 13-12

Managing Protection Groups and High Availability

The high availability architecture ensures continuous availability of Cisco ANA functionality, by detecting and recovering from a wide range of hardware and software failures. The distributed design of the system enables the *impact radius* caused by a single fault to be confined. This prevents all types of faults from setting into motion a chain reaction that can lead to a crash of all the management services.

The high availability of the server backbone is achieved at several complementing levels:

- NEBS-3 compliant carrier-class server hardware.
- N+m warm standby protection for unit groups. For more information see Unit N+m High Availability, page 13-10.
- Internal watchdog protocol within each unit, in charge of monitoring (and, if necessary, automatically reloading) failed processes. For more information, see Watchdog Protocol and Process Monitoring, page 13-11.

The roles required to manage high availability are described in Roles Required to Manage Protection Groups, page 13-12. By , all the units in the Cisco ANA fabric belong to one group, the -pg protection group. A protection group is a collection of units, one of which is assigned to be the standby unit. The administrator can change the setup of the units by customizing protection groups (clusters) and then assigning units to these groups.

Note Cisco ANA does not provide a solution for the configuration of high availability for a Cisco ANA gateway. For information about your options, please contact ask-ana@cisco.com.

Unit *N+m* High Availability

Need to figure out what needs to be said about multiple AVM 100.

The clustered *N+m* high availability mechanism within the Cisco ANA fabric is designed to handle the failure of a unit. Such failures include hardware failures, operating system failures, power failures, or network failures, which disconnect a unit from the Cisco ANA fabric.

Unit availability is established in the gateway, running a Protection Manager process, which continuously monitors all the units in the network. Once the Protection Manager detects a unit that is malfunctioning, it automatically signals one of the *m* servers in its cluster to load the configuration of the faulty unit (from the system registry), taking over all its managed network elements. This design provides many possibilities for trading off protection and resources. These possibilities range from just segmenting the network into clusters without any extra machines, up to having a warm-swappable empty unit for each unit in the setup. We recommend that units be clustered according to geography and that an additional empty unit be added to heavily loaded clusters.

The switchover of the redundant standby unit does not result in any loss of information in the system, because all the information is autodiscovered from the network, and no persistent storage synchronization is required. This is because persistency files are also copies to redundant units. Hence, the redundant standby unit relearns all the information from the network elements, with no danger of persistent information corruption. Furthermore, where there is cluster saturation (when more than one unit in a cluster fails at the same time and there are no extra machines), the remaining units continue to operate and manage their network map normally. (For more information on information persistency, see Appendix F, “VNE Persistency Mechanism.”

When a unit is configured it can be designated as being an active or standby unit. The active units (excluding the standby unit) that are connected to the gateway are configured into a protection group. The standby unit that is configured for the gateway is linked to that protection group. The administrator can define more than a single protection group. Each protection group defined has a set of protected units and a protecting standby unit. If you have configured devices to forward traps to a unit, you should also configure the devices to forward traps to the standby unit (see Trap Forwarding, page 13-23).

Figure 13-5 shows to protection groups (a cluster) of units, which are controlled by one gateway. In each cluster, one unit is configured as the standby for the protection group. An alternative would be for the two groups to overlap, with the same unit acting as the standby.

Figure 13-5 Cisco ANA ***Gateway/Unit Architecture for High Availability***

In the above configuration, when the gateway determines that one of the units in the protection group has failed, it notifies the protection group's standby unit to immediately load the configuration of the failed unit. The standby unit loads the configuration of the failed unit, including all its AVMs, VNEs, maps, and running functions.

These events are all recorded in the system log, which enables you to take the necessary action to bring the failed unit up again. When the failed unit becomes operational, you can decide whether to configure it as the new standby unit or to reinstate it to the protection group and configure another unit as the standby unit.

Note The high availability mechanism attempts to load an AVM after it crashes (whether the AVM comes up or not), a maximum of 5 times. Thereafter, the high availability mechanism does not try to load this AVM again.

Watchdog Protocol and Process Monitoring

Each unit executes several processes: one control process and several AVM processes that execute VNEs. Each process within the unit is completely independent. The isolation concept is tailored throughout the design: a failure of a single process does not affect other processes on the same machine. The exact number of processes on each unit depends on the capacity and computational power of the unit.

The control process executes a *watchdog protocol*, which continuously monitors all other processes on the unit. This watchdog protocol requires each AVM process to continuously handshake with the control process. A process that fails to handshake with the control process after a number of times (one that is "stuck") is automatically stopped and reloaded. All of the watchdog protocol parameters are configurable.

The dynamic design of the control process implements runtime adaptation and escalation. The escalation procedure moves the AVM to suspended mode, and the process is suspended. An example of an escalation procedure is to stop reloading a process that has crashed more than *N* times within a given period, because it is suspected of having a recurring software problem.

The reload process is local to the unit, and thus very rapid, with a minimal amount of down time. Since the process can use its previous cache information (temporary persistence used to improve performance), once the stuck process is detected, reloading the process takes only a few seconds with no data loss.

All watchdog protocol activity is logged, and an alarm is generated and sent when the watchdog protocol reloads a process.

For information on how often Cisco ANA attempts to restart an AVM, see High Availability Events and Default Settings for Failover, page 13-21.

Roles Required to Manage Protection Groups

Table 13-4 lists the roles that are required to use the Administration perspective functions. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Table 13-4 Roles Required to Use Protection Groups Functions

Task	Role Required
Creating a protection group	Administrator
Deleting a protection group	Administrator
Switching to a standby unit	Administrator
Managing AVM watchdog protocol	Administrator

Related Topics

- Configuring High Availability for Units, page 13-17
- Managing the Watchdog Protocol on AVMs, page 13-20
- High Availability Events and Default Settings for Failover, page 13-21
- Estimating Down Time in Case of Failure, page 13-12

Estimating Down Time in Case of Failure

Reviewers: This section was added from the ANA 3.6.3 document.

When a failure occurs in a unit or AVM, the length of time that the system is down depends on the type of failure, how long it takes to detect that the component is not working, and how long is the recovery period during which the unit or AVM reloads and the system functions normally again.

Three types of failure can occur, as described in the following sections:

- Catastrophic Process Failure, page 13-13
- Timeout Process Failure, page 13-14
- Timeout Machine Failure, page 13-16

Catastrophic Process Failure

Each AVM has a log file which is constantly monitored by a Perl process for log messages about catastrophic failures, such as AVM processes running out of memory. When such a failure occurs, the Perl process restarts the AVM almost immediately, so the Mean Time To Repair (MTTR) is based on the AVM loading life cycle.

Table 13-5 describes the impact on different AVMs when experiencing such a failure:

Table 13-5 Catastrophic Process Failure Impact on AVMs

Process	Impact	MTTR	Probability of Failure
AVM 0 (switch AVM)	Loss of messages to and from the machine.	1 minute to reach bootstrap.	Messages are constantly being sent and received in the system, so the probability of failure is high.
AVM 99 (management AVM)	Loss of registry notifications on changes made to the Golden Source.	1 minute to reach bootstrap.	Registry modifications are made only when the VNE is first loaded into the system, so the probability of failure is low. Modifications are rarely made while the system is up and running.
AVM 100 (trap management AVM)	Loss of traps and syslogs from devices.	1 minute to reach bootstrap, plus time for all the VNEs to re-register for traps and syslogs.	Traps and syslogs are constantly received in a live, scaled system, so there is a high probability of losing traps and syslogs during the reloading period.
AVM 11 (gateway)	Loss of persistency of any kind.	6-10 minutes to reach bootstrap on a scale.	Since AVM 11 handles Oracle communication and various gateway functions such as alarm processing, there is a high probability of loss of events persistency during this period.
AVM101-999	Loss of management to a section of devices managed by the AVM.	1 minute to reach bootstrap, plus time to load the VNEs depending on the number and type of VNEs.	No alarm processing occurs while the AVM is down, so traps and syslogs sent to the VNEs are lost. The loss of traps and syslogs for a period of 1 minute is high.

Timeout Process Failure

Each AVM is constantly monitored by the management AVM (AVM99) using a watchdog protocol pulse message sent to the AVM at a preconfigured interval. When the AVM fails to respond to the pulse message after a preconfigured number of attempts, the management AVM restarts the process.

The management process also keeps a history of the number of times it has restarted the AVM. When it reaches the maximum number of preconfigured restart times, the management AVM stops restarting the AVM, because this indicates a serious problem with the AVM. Each restart is logged as a system event (except when AVM11 is restarted, because this AVM handles all persistency).

Failures on AVMs in the system are measured in a similar way to a catastrophic process failure (see Table 13-5), with the addition of the watchdog protocol overhead. This is measured by the pulse interval multiplied by the number of restart attempts.

Note

- The maximum number of preconfigured restart times is five, after which the management process will not try to reload the AVM.
- It takes approximately 1 minute for the system to detect that an AVM (including AVM100) is not working.
- The recovery period during which an AVM (including AVM100) reloads and the system starts to function normally again is approximately 5 minutes, depending on the number of VNEs per AVM, and the complexity of each.

Figure 13-6 provides a typical example of how the High Availability timer parameters work while monitoring the AVMs.

Figure 13-6 HA Parameter Timers and AVM Monitoring Example

Measuring Ticket Processing Down Time

When a failure occurs on an AVM, the time during which ticket processing is down is measured as the sum of the following factors:

- The time it takes to determine that the AVM has failed.
- The time it takes for the AVM to reload, depending on its number of VNEs.
- The time it takes to pass syslogs or traps to the VNEs (in the case of an AVM100), or to pass events to the gateway (in the case of an AVM101-999).

Note For the first 30 minutes after an AVM99 (the management AVM) has started, there is no monitoring of the system to find high availability issues. This is to allow the system enough time to get up and running.

Timeout Machine Failure

The Cisco ANA gateway constantly monitors the units by sending a watchdog protocol pulse message to the units' management AVM at a preconfigured interval. If the units' management AVM fails to respond to the pulse message after a preconfigured number of retries, the gateway loads the standby unit to replace it.

The impact of such a failure on the system is that the unresponsive unit does not manage the devices for a period of time. This "unmanaged" period of time is measured by the pulse interval multiplied by the number of retry times, plus the unit load time.

Note The unit load time depends on the AVMs and the load time taken for the VNEs to complete their modeling, as described in Table 13-5.

Figure 13-7 illustrates how the unit handles events during the loading time.

Figure 13-7 Stages in Event Handling through System Restart

Measuring Ticket Processing Down Time

When a failure occurs on a unit, the time during which ticket processing is down is measured as the sum of the following factors:

- The time it takes to determine that the unit has failed (depending on the ping interval).
- The time it takes for the unit to reload, depending on the number of AVMs and VNEs in the unit.
- The time it takes to pass correlated events to the gateway (a minimum of 5 minutes to get some device history, plus a variable time depending on the number of VNEs per AVM).

Configuring High Availability for Units

These topics describe customizing protection groups, configuring units for high availability, and configuring standby units. These are the steps you must perform to set up high availability:

1. Prepare a deployment plan. It should include:
   a. How many units will be deployed.
   b. How many protection groups to create, and how to cluster the units into a protection group. This should be based on the device type, geographical location, importance of the device, and the number of devices.
   c. How many standby units will be deployed.
   d. How the units, standby units, and protection groups will be deployed and allocated.
2. Creating a New Protection Group, page 13-17—Describes how to create and customize protection groups for units.
3. Changing an Active Unit into a Standby Unit, page 13-18—Describes how to assign a unit to a protection group, enable the unit for high availability, and enable another unit for standby status.
4. Checking and Changing the Assignment of Units to Protection Groups, page 13-19—Describes how to view the current assignments of units to protection groups.

These topics provide additional information on managing high availability:

- Viewing and Editing Protection Group Descriptions, page 13-20—Describes how to view or edit the properties of a protection group.
- Switching to a Standby Unit, page 13-19—Describes how to switch to the standby unit (manually or automatically).
- High Availability Events and Default Settings for Failover, page 13-21—Describes the high availability events that can occur on the Cisco ANA system.

Creating a New Protection Group

Administrators can change the setup of the units by customizing protection groups (clusters) and then assigning units to these groups. By , all units belong to the -pg protection group.

To create and customize a protection group:

Step 1 In the Administration perspective, click the **Objects** tab and click the **System Settings** drawer.

Step 2 Right-click **Protection Groups** and choose **New Protection Group,** or choose an existing protection group. You cannot edit the -pg protection group.

Step 3 Enter a name and (optional) description for the protection group.

Step 4 Click **OK**.

The new protection group is displayed in the workspace of the window.

Related Topics

- Changing an Active Unit into a Standby Unit, page 13-18
- Checking and Changing the Assignment of Units to Protection Groups, page 13-19
- High Availability Events and Default Settings for Failover, page 13-21

- Estimating Down Time in Case of Failure, page 13-12
- Switching to a Standby Unit, page 13-19
- Configuring AVMs for High Availability, page 14-21

Changing an Active Unit into a Standby Unit

When you create a unit, you can enable or disable high availability, or designate the unit to be a standby unit. This is done through choices that you make when you create the unit as described in Adding a New Unit (and Setting Up High Availability), page 2-5.

Note By default, all the units belong to the deefault-pg protection group, and high availability is enabled. Contact ask-ana@cisco.com if you want to enable or disable the watchdog protocol and timeouts.

This procedure describes how to configure an active unit to be a standby server:

Step 1 To change an active unit into a standby unit, you must first do the following:

a. Shut down all the VNEs of the active unit. See Changing AVM Status (Start or Stop), page 2-13.

b. Remove all the configurable AVMs of the active unit (AVMs below a value of 100 cannot be deleted). See Deleting an AVM, page 2-15.

c. Delete (remove) the active unit from the setup. See Removing a Unit, page 2-7.

Step 2 In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.

Step 3 Right-click **Servers** and choose **New ANA Unit**.

Step 4 Enter the required information:

a. Unit IP Address—Enter the unique IP address of the unit.

b. Gateway IP Address—Prepopulated IP address of the gateway server.

c. Unit Protection—Click Standby.

d. Protection Group—Choose the appropriate protection group from the drop-down list of available groups. (Protection groups are described in Managing Protection Groups and High Availability, page 13-9.)

Step 5 Click **OK**. The new unit is displayed in the tree pane and the workspace of the window. If the new unit is installed and reachable it starts automatically.

If devices were configured to forward traps to a unit, you should also configure the devices to forward traps to the standby unit. If a unit goes down, when the standby unit comes up, AVM 100 on the standby unit broadcast s to the VNEs, and the VNEs register to it to start receiving traps from the new AVM 100.

Related Topics

- Creating a New Protection Group, page 13-17
- Checking and Changing the Assignment of Units to Protection Groups, page 13-19
- High Availability Events and Default Settings for Failover, page 13-21
- Estimating Down Time in Case of Failure, page 13-12
- Switching to a Standby Unit, page 13-19

- Configuring AVMs for High Availability, page 14-21

Checking and Changing the Assignment of Units to Protection Groups

The administrator can view the protection groups to which the units are currently assigned. In so doing, the administrator can, at a glance, verify that the configuration or assignment matches the initial deployment plan.

To check the assignment of units to protection groups:

Step 1 In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.

Step 2 Click **Servers**. The properties of all gateway servers and units are displayed in the workspace, including the details of the protection group to which each unit and standby unit currently belongs. (If you have not configured any units, the gateway server acts as a unit and can have a protection group.)

Step 3 If you want to change the protection group for a unit:

a. Open the servers tree and select the unit.

b. Choose another protection group from the Protection Group drop-down list.

c. Close the Servers workspace and save your changes.

Related Topics

- Creating a New Protection Group, page 13-17
- Switching to a Standby Unit, page 13-19
- Viewing and Editing Protection Group Descriptions, page 13-20
- Configuring AVMs for High Availability, page 14-21
- Estimating Down Time in Case of Failure, page 13-12
- High Availability Events and Default Settings for Failover, page 13-21

Switching to a Standby Unit

If you have enabled high availability on a unit, when the gateway discovers that one of the active units has had a high availability event (such as a timeout), Cisco ANA automatically transfers all data from the failed unit to a standby unit in the same protection group. If you have configured more than one standby unit for a protection group, the gateway randomly chooses the redundant unit to activate.

You can also manually switch to a standby server (for example, when you want to temporarily shut down a unit for maintenance).

To manually switch to the standby unit:

Step 1 In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.

Step 2 Open the Servers tree, right-click the unit you want to switch to its standby, and choose **Switch**.

Step 3 Confirm your choice.

The standby unit becomes the active unit and is displayed in the Servers tree. The original unit is removed from the setup and can be safely shut down (note that it is no longer displayed).

Related Topics

- Creating a New Protection Group, page 13-17
- Checking and Changing the Assignment of Units to Protection Groups, page 13-19
- Viewing and Editing Protection Group Descriptions, page 13-20
- Configuring AVMs for High Availability, page 14-21
- Estimating Down Time in Case of Failure, page 13-12
- High Availability Events and Default Settings for Failover, page 13-21

Viewing and Editing Protection Group Descriptions

If desired, you can view and edit a protection group's description:

Step 1 In the Administration perspective, click the **Object**s tab and click the **System Settings** drawer.

Step 2 Click **Protection Groups**.

Step 3 Click the protection group you want to edit, and make your changes.

Step 4 Click the Save icon in the main toolbar.

Related Topics

- Creating a New Protection Group, page 13-17
- Checking and Changing the Assignment of Units to Protection Groups, page 13-19
- Switching to a Standby Unit, page 13-19
- Configuring AVMs for High Availability, page 14-21

Managing the Watchdog Protocol on AVMs

When you create an AVM, the New AVM dialog box contains a check box which controls whether the watchdog protocol should be enabled on the AVM. The watchdog protocol requires each AVM process to continuously handshake with the control process. Although users with Administrator privileges can disable the protocol, it is highly recommended that the protocol remain enabled.

To view or edit the watchdog protocol setting for an AVM:

Step 1 In the Administration perspective, click the **Objects** tab and click the **ANA Servers** drawer.

Step 2 Open the Servers tree, and click the gateway. The watchdog protocol status is listed in the AVM Protection Enabled column.

Step 3 If you want to change the setting, double-click the AVM in which you are interested, and click the AVM Protection Enabled check box at the top of the page.

Step 4 Click the Save button in the main toolbar.

Related Topics

- Watchdog Protocol and Process Monitoring, page 13-11
- High Availability Events and Default Settings for Failover, page 13-21
- Roles Required to Manage Protection Groups, page 13-12
- Configuring High Availability for Units, page 13-17

High Availability Events and Default Settings for Failover

Table 13-6 provides a list of the high availability events displayed in the Troubleshooting perspective and provides the s for the failover parameters.

Table 13-6 Settings for Failover

Description	Measured in Milliseconds	Entry Name in Registry
Grace period (time, from system startup, in which events are not raised)	1800000 (30 minutes)	Delay
Timeout for AVMs	300000 (5 minutes)	Timeout

Table 13-6 Settings for Failover (continued)

Description	Measured in Milliseconds	Entry Name in Registry
Timeout for units	300000 (5 minutes) **Note** This is the initial recovery period (defined in minutes), which includes network element polling and inventory build-up. End-to-end services such as RCA and topology may take longer to become available.	Timeout
AVMs repeatedly not responding	Tries a maximum of 5 times to restart the AVM, within 10800000 ms (180 minutes) (if more than 5, suspends the AVM).[1]	maxTimeoutReloadTime maxTimeoutReloadTries

[1] If an AVM is restarted, you can view the log files for more details. The log filenames are in the format *avm*.restart1, *avm*.restart2, and so forth, up to *avm*.restart5. If you want to change the number of restarts, contact ask-ana@cisco.com.

When an AVM initially starts, Cisco ANA waits until a grace period of 30 minutes has elapsed before attempting to restart the AVM. This is because an AVM can be very busy during initial startup, and may not respond to availability queries in a timely manner. If the AVM has not started by the end of the 30 minutes, Cisco ANA attempts to restart the AVM up to 5 times. If the AVM does not restart, Cisco ANA suspends the AVM and displays a message saying the AVM has been "suppressed." The AVM is displayed as Disabled. To re-enable the AVM, you must stop it and then start it again, as described in Changing AVM Status (Start or Stop), page 2-13. (If the AVM responds to any high availability queries during the 30 minute grace period, the grace period is skipped.)

This grace period also applies to units; in other words, Cisco ANA does not perform any high availability operations on AVMS or units until the 30 minutes has elapsed.

A list of the high availability events is provided in Table 13-7.

Table 13-7 High Availability Events

Event	Message	Severity
Watchdog Protocol Protection		
The AVM times out (see *Grace period* in Table 13-6)	AVM 107 not responding: ANA Unit = 1.1.1.1 AVM = 107 This is followed by one of the following:	Major
	AVM 107 is shutting down. ANA Unit = 1.1.1.1	Minor
	AVM 107 is starting. ANA Unit = 1.1.1.1	Minor
The AVM repeatedly does not respond (see *AVMs repeatedly not responding* in Table 13-6)	AVM 107 suppressed: ANA Unit = 1.1.1.1 AVM = 107	Major
Unit Protection		
The unit times out (when a standby unit is available) (see *Timeout for units* in Table 13-6)	Server 1.1.1.1 not responding. Raising Redundant machine = 3.3.3.3	Major

Table 13-7 High Availability Events (continued)

Event	Message	Severity
A unit times out (without a standby unit being available) (see *Timeout for units* in Table 13-6)	Server 1.1.1.1 not responding. No Redundant machine available	Major
Manually switching to the standby unit	Server 1.1.1.1 manual failover initiated No Redundant machine available	Major
	Server 1.1.1.1 manual failover initiated Raising Redundant machine = 3.3.3.3	Major

Related Topics

- Estimating Down Time in Case of Failure, page 13-12
- Roles Required to Manage Protection Groups, page 13-12
- Configuring High Availability for Units, page 13-17
- Managing the Watchdog Protocol on AVMs, page 13-20

Trap Forwarding

You can configure Cisco ANA to forward SNMP traps, alarms, and events from network elements to other destinations, so that OSS clients can receive these traps on their UDP or TCP ports. You can also create filters, so that only the traps that are of a certain severity or from a certain IP address are forwarded. Before they are forwarded, all traps are converted to SNMPv2, and are formatted according to the CISCO-EPM-NOTIFICATION-MIB. By , they are forwarded to port 162 on the destination machine, and the community string is set to public. If the destination is not available, the messages are dropped.

Note You can also forward traps in SNMPv1 format, with the community string set to private. Contact ask-ana@cisco.com for information on how to do this, since it cannot be done from the user interface at this time.

For information on supported traps, see Tracking Faults, page 12-1.

See these topics for the following information:

- To familiarize yourself with the user interface, see Understanding the Trap Forwarding User Interface, page 13-24.
- For instructions on how to configure trap forwarding, see Configuring a Trap Forwarding Service, page 13-24.

Understanding the Trap Forwarding User Interface

The following tool buttons are located at the top right of the Trap Forwarding Service workspace.

Table 13-8 Trap Forwarding Service Tool Buttons

Icon	Tooltip	Description
✚	New Trap Forwarding Service	Creates a new trap forwarding service.
✎	Edit Trap Forwarding Service	Edits an existing trap forwarding service.
🗑	Delete Trap Forwarding Service	Deletes an existing trap forwarding service.

Roles Required to Use Trap Forwarding

Table 13-9 lists the roles that are required to use the Trap Forwarding functions. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Table 13-9 Roles Required to Configure Trap Forwarding

Task	Role Required
Creating a new trap forwarding service	Administrator
Editing an existing trap forwarding service	Administrator
Deleting an existing trap forwarding service	Administrator

Related Topic

- Configuring a Trap Forwarding Service, page 13-24

Configuring a Trap Forwarding Service

Follow this procedure to set up trap forwarding. If you have configured unit high availability, you should also forward traps to backup units.

Reviewers: PRD1225 says: "A formal and explicit filtering mechanism, GUI-configurable, must be supplied so that incoming event notifications can be accepted or dropped. ANA MUST NOT require complex rules/registry editing for specifying the filters." How is this done?

Also - what else needs to be said about AVM 100?

Step 1 In the Administration perspective, click the **Object**s tab and click the **System Settings** drawer.

Step 2 Click **Trap Forward Management.** All of the current trap forwarding configurations are displayed.

Step 3 In the primary content area, click the **New Trap Forwarding Service** icon.

Step 4 In the New Trap Forwarding Service page, do the following:

a. Enter the destination IP address and port, and choose the connection type from the drop-down list (TCP or UDP). By , traps are sent to port 162 on all destinations. You can change the destination port as needed.

b. If you want to set up a filter so that only certain traps are forwarded to a destination, do the following:

- Choose the trap Severity (Critical, Major, Minor,and so forth) in which you are interested.
- From the Source IP list, choose the IP addresses in which you are interested, and click **Add**. (The Source IP list is populated with all of the IP addresses that the network has discovered.) The IP addresses are added to the Filter IP list.
- Click **OK**. Any traps matching the criteria is forwarded.

Step 5 To edit the trap forwarding service, choose the service you want to edit and right-click **Edit**. Follow the instructions for configuring a new service, in Step 4.

Step 6 To stop a trap forwarding service, choose the service you want to discontinue and right-click **Delete**.

Related Topic

- Understanding the Trap Forwarding User Interface, page 13-24

Specifying Global Settings for Cisco ANA Features

Administrators can configure specific preferences for Cisco ANA network resource management features, such as specifying the import directory for network element images, or the maximum number of network element configurations that can be archived. This is done using the functions in the Preferences drawer in the Administration perspective (which is under the Tasks tab). These topics describe how to specify the settings:

- Configuration Archive Preferences, page 13-25
- NEIM Preferences, page 13-28
- Reports Preferences, page 13-29
- Troubleshooting Perspective Preferences, page 13-30
- Command Builder Preferences, page 13-31

Configuration Archive Preferences

This topic explains how to set Configuration Archive to purge old archives and exclude specific commands when comparing configurations. Purging archives is disabled by .

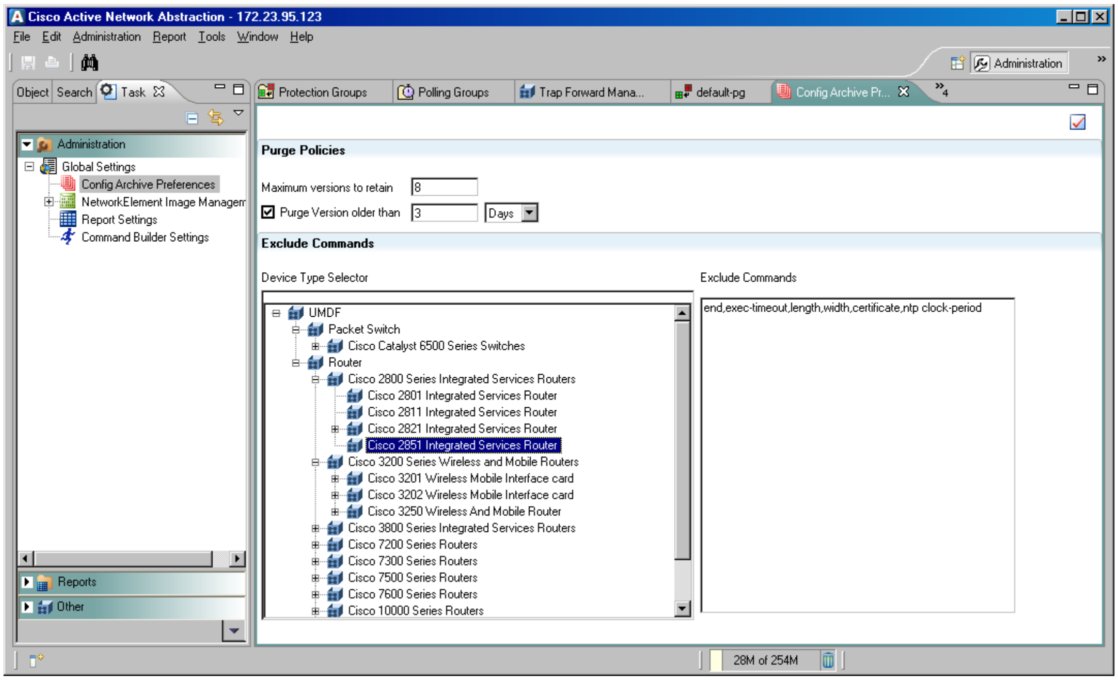
See these topics for more information:

- Understanding the Configuration Archive Preferences User Interface, page 13-26
- Adjusting Configuration Archive Preferences, page 13-27

Understanding the Configuration Archive Preferences User Interface

Figure 13-1 shows the Configuration Archive preferences user interface.

Figure 13-8 Configuration Archive Preferences User Interface



Purge Policies

Maximum versions to retain 8

☑ Purge Version older than 3 Days

Exclude Commands

Device Type Selector

- UMDF
  - Packet Switch
    - Cisco Catalyst 6500 Series Switches
  - Router
    - Cisco 2800 Series Integrated Services Routers
      - Cisco 2801 Integrated Services Router
      - Cisco 2811 Integrated Services Router
      - Cisco 2821 Integrated Services Router
      - Cisco 2851 Integrated Services Router
    - Cisco 3200 Series Wireless and Mobile Routers
      - Cisco 3201 Wireless Mobile Interface card
      - Cisco 3202 Wireless Mobile Interface card
      - Cisco 3250 Wireless And Mobile Router
    - Cisco 3800 Series Integrated Services Routers
    - Cisco 7200 Series Routers
    - Cisco 7300 Series Routers
    - Cisco 7500 Series Routers
    - Cisco 7600 Series Routers
    - Cisco 10000 Series Routers

Exclude Commands

end,exec-timeout,length,width,certificate,ntp clock-period

The following tool button is located at the top right of the Configuration Archive Preferences workspace.

Table 13-10 Configuration Archive Preferences Tool Button

Icon	Tooltip	Description
☑	Perform Now	Immediately applies your Configuration Archive settings

Roles Required to Use Configuration Archive Preferences

Table 13-10 lists the roles that are required to configure the preferences for Configuration Archive. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Table 13-11 Roles Required to Set Configuration Archive Preferences

Task	Role Required
Setting or editing Configuration Archive settings	Administrator

Related Topic

- Adjusting Configuration Archive Preferences, page 13-27

Adjusting Configuration Archive Preferences

Step 1 In the Administration or Monitoring perspectives, click the **Tasks** tab and click the **Administration** drawer.

Step 2 Open the Global Settings tree and click **Config Archive Preferences**.

Step 3 Specify when to purge archived running configurations. This frees disk space and keeps your archive at a manageable size.

Note By , purging the archive is disabled.

- Enter the maximum number of versions of each configuration Cisco ANA should retain. The oldest configuration is purged when the maximum number is reached. The is 5.
- Enter the age at which configurations should be purged. Cisco ANA does not purge configuration files unless there are more than two versions of the files in the archive.

Note Make sure that the configuration change detection schedule does not conflict with purging, since both processes are database-intensive. Also, back up your system frequently to prevent loss of versions.

Step 4 Specify the commands that should be excluded when Cisco ANA compares configurations:

a. Choose a network element category, family, or specific type:

- Device Category (for example, Cisco Routers)—Apply the **exclude** command to all device families in that category.
- Device Family (for example, Cisco 1000 Series Routers)—Apply the **exclude** command to all devices in that family; for example **end**, **exec-timeout**, **length**.
- Device Type (for example, Cisco 1003 Router)—Apply the **exclude** command to only that device type; for example, **end**, **exec-timeout**, **length**, **certificate**, **ntp clock-period**.

Note If you specify the **exclude** command for a device category and device family (for example, Cisco Routers and Cisco 1000 Series Routers), the **exclude** command is applied only to the device family, not to the whole category. If you use the **exclude** command at all three levels, the commands are applied only to the specific device type. In this way, commands you apply at a lower level are not applied at higher levels.

b. Enter a comma-separated list of commands. commands are provided for some network elements.

Step 5 Click the **Apply** icon at the top right of the workspace, or the save icon in the main toolbar.

Related Topic

- Understanding the Configuration Archive Preferences User Interface, page 13-26

NEIM Preferences

This topic explains how to configure the credentials required to log in to a vendor website and download a new network element image using Network Element Image Management (NEIM). It also explains how to change the directory into which network element images are imported.

See these topics for more information:

- Understanding the NEIM Preferences User Interface, page 13-28
- Adjusting NEIM Preferences, page 13-29

Understanding the NEIM Preferences User Interface

The following tool buttons are located at the top right of the NEIM preferences workspace.

Table 13-12 Network Element Image Management Preferences Tool Buttons

Icon	Tooltip	Description
Vendor Credential Settings		
✎	Update Credentials	Edits existing vendor credentials
🗑	Delete Credentials	Deletes existing vendor credentials
👤	Add Credentials	Adds new vendor credentials
Preferences (Import Directory)		
☑	Apply	Immediately applies your NEIM settings

Roles Required to Change NEIM Preferences

Table 13-13 lists the roles that are required to configure NEIM preferences. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Table 13-13 Roles Required to Set NEIM Preferences

Task	Role Required
Updating vendor credentials	Administrator
Deleting vendor credentials	Administrator
Adding vendor credentials	Administrator
Setting image import directory	Administrator

Related Topic

- Adjusting NEIM Preferences, page 13-29

Adjusting NEIM Preferences

Use this procedure to set vendor credentials so that you can log in to a vendor website to download network element images. Also use this procedure to change the import directory for these images.

Before You Begin

If you plan to change the import directory for network element images, make sure the directory is empty and has the proper permissions (anauser must have read, write, and execute permissions).

Step 1 In the Administration or Monitoring perspectives, click the **Tasks** tab and click the **Administration** drawer.

Step 2 Open the Global Settings tree and the Network Element Image Management tree.

Step 3 To configure vendor credentials, click **Vendor Credential Settings**. You can add, edit, or delete credentials by clicking the icons in the workspace (the icons are described in Table 13-12 on page 13-28). When finished, click the save icon in the main toolbar.

Step 4 To set the import directory:

- **a.** Click **Preferences**. By , Cisco ANA stores the images in *ANAHOME*/imageStageTemp (*ANAHOME* is normally /export/home/ana41).
- **b.** If you want to enter a new directory, enter the new directory information. Make sure the directory is empty and has the proper permissions (read, write, and execute permissions for anauser), because Cisco ANA does not validate this directory.
- **c.** Click the **Apply** icon at the top right of the workspace, or the save icon in the main toolbar.

Related Topic

- Understanding the NEIM Preferences User Interface, page 13-28

Reports Preferences

The Reports preferences function controls the number of archived reports stored by Cisco ANA.

See these topics for more information:

- Roles Required to Specify Preferences for Reports, page 13-29
- Adjusting Preferences for Reports, page 13-30

Roles Required to Specify Preferences for Reports

Table 13-14 lists the roles that are required to configure the preferences for Reports. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Table 13-14 Roles Required to Set Reports Preferences

Task	Role Required
Setting or editing report settings	Administrator

Related Topic

- Adjusting Preferences for Reports, page 13-30

Adjusting Preferences for Reports

The generated report is purged based on the purge policy you specify while creating the report job or by using the Report Setting in the Administration perspective.

You can purge reports based on two criteria:

- Number of versions to retain—Minimum and Maximum number of versions to retain.

  The oldest report is purged when the maximum number is reached. For example, if you set the maximum versions to retain to 10, when the eleventh version of a report is archived, the earliest (first version) is purged to retain the total number of latest archived report versions at 10.
- Delete report older than—Archived reports older than the number of days that you specify are purged.

Cisco ANA does not purge the archived reports if the number of archived reports is less than or equal to the specified minimum number of versions to retain.

The purge policy that you specify while creating the report job overrides the policy you specify here.

Step 1 In the Administration or Monitoring perspectives, click the **Tasks** tab and click the **Administration** drawer.

Step 2 Open the Global Settings tree and click **Report Settings**.

Step 3 Configure the following settings:

- Minimum Age Required check box—Check this box to activate the Age Required to Purge setting.
- Age Required to Purge—Purges all of the reports that are older than the configured number (in days). The is 30.
- Minimum number of versions—The minimum number of versions of each report to retain. The is 1.
- Maximum number of versions—The maximum number of reports to retain. The is 10. The oldest report is purged when this number is reached.

Step 4 To save your changes, click the save icon in the main toolbar.

If at any time you want to restore the settings to their defaults, click **Restore**.

Related Topic

- Roles Required to Specify Preferences for Reports, page 13-29

Troubleshooting Perspective Preferences

The Troubleshooting Preferences function controls the number of archived reports stored by Cisco ANA.

See these topics for more information:

- Roles Required to Specify Preferences for the Troubleshooting Perspective, page 13-31
- Adjusting Preferences for the Troubleshooting Perspective, page 13-31

Roles Required to Specify Preferences for the Troubleshooting Perspective

Table 13-14 lists the roles that are required to configure the preferences for the Troubleshooting perspective. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Table 13-15 Roles Required to Set Reports Preferences

Task	Role Required
Setting or editing Troubleshooting perspective settings	Administrator

Related Topic

- Adjusting Preferences for the Troubleshooting Perspective, page 13-31

Adjusting Preferences for the Troubleshooting Perspective

You can control how often Troubleshooting perspective tables are refreshed, and the default amount of information to be displayed in the different types of tables. These settings only control how much information is displayed in the perspective; they do not control how much information is saved by Cisco ANA. You can still search in the Troubleshooting perspective for more events than are currently displayed.

Step 1 In the Administration or Monitoring perspectives, click the **Tasks** tab and click the **Administration** drawer.

Step 2 Open the Global Settings tree and click **Troubleshooting Preferences**. Cisco ANA displays a list of all of the event tables in the Troubleshooting perspective (Service, Security, Tickets, and so forth).

Step 3 Configure the following display settings for each table type, as desired:

- Display Timeframe—Specifies how many hours' worth of events to display in a table (for example, the previous 2 hours, 4 hours, and so forth). .
- Auto Refresh Interval (Secs)—How often to refresh a table.

Step 4 To save your changes, click **Apply**. Otherwise, click **Cancel**.

Reviewers: Do the changes take effect immediately?

Related Topic

- Roles Required to Specify Preferences for the Troubleshooting Perspective, page 13-31

Command Builder Preferences

This topic explains how to configure parameters for Command Builder policies, so that the policies are applied to future Command Builder jobs.

See these topics for more information:

- Understanding the Command Builder Preferences User Interface, page 13-32.

- Adjusting Command Builder Preferences, page 13-33

Understanding the Command Builder Preferences User Interface

Figure 13-1 shows the Command Builder preferences user interface.

Figure 13-9 Command Builder Preferences User Interface

The following tool button is located at the top right of the Command Builder workspace.

Table 13-16 Command Builder Preferences Tool Button

Icon	Tooltip	Description
☑	Apply	Immediately applies your Command Builder settings

Roles Required to Use Command Builder Preferences

Table 13-17 lists the roles that are required to configure the preferences for Command Builder. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Table 13-17 Roles Required to Set Command Builder Preferences

Task	Role Required
Setting or editing Command Builder preferences	Administrator

Related Topic

- Adjusting Command Builder Preferences, page 13-33

Adjusting Command Builder Preferences

Use this procedure to adjust the preferences for Command Builder:

Step 1 In the Administration or Monitoring perspectives, click the **Tasks** tab and click the **Administration** drawer.

Step 2 Open the Global Settings tree and click **Command Builder Settings**.

Step 3 Configure your settings.

Note If you check the Allow User Configuration check box associated with a setting, users with job scheduling privileges are able to configure that setting when scheduling a Command Builder job from the Inventory perspective.

- Execution Policy—How to run on multiple network elements:
  - PARALLEL—Run the job on multiple network elements at the same time.
  - SERIAL—Run the job on multiple network elements in sequence.
- Failure Policy—What the job should do if it fails to run on a network element:
  - ROLLBACK_JOB—Rolls back the changes on all network elements and stops the job.
  - ROLLBACK_DEVICE_STOP—Rolls back the changes on the failed network elements and stops the job.
  - ROLLBACK_DEVICE_CONTINUE—Rolls back the changes on the failed network element and continues the job.
- Synch Archive Before Job Execution—Controls whether Cisco ANA should archive the running configuration before making configuration changes.
- Copy Running Config to Startup—Controls whether Cisco ANA should copy the running configuration to the startup configuration on each network element after configuration changes are made successfully.
- Fail on Mismatch Config Versions—Instructs Cisco ANA whether to consider the job a failure if there is a version mismatch between:
  - The most recent configuration version in the configuration archive, and
  - The most recent configuration version in the configuration archive at the time when the job is run.

Step 4 Click the **Apply** icon at the top right of the workspace, or the save icon in the main toolbar.

Related Topic

- Understanding the Command Builder Preferences User Interface, page 13-32

Creating and Managing Users, Passwords, and Scopes

Cisco ANA uses a variety of methods for managing authentication and authorization:

- User authentication managed by Cisco ANA, or by an external Lightweight Directory Access Protocol (LDAP) application. You can use either method to perform user authentication and manage all user passwords. You specify the method when creating a user account. See Creating and Managing Cisco ANA User Accounts, page 13-34.
- *Roles* control the actions a user is authorized to perform. Cisco ANA provides four predefined security access roles: Administrator, Configurator, Network Operator, and Viewer. See Creating and Managing Cisco ANA User Accounts, page 13-34.
- *Scopes*, or groups of network elements, control which elements a user is authorized to view and manage. Cisco ANA provides one predefined scope called All Managed Elements, which cannot be edited. Users cannot view *any* network elements in Cisco ANA until they are assigned a scope. See Creating and Managing Scopes, page 13-42.

Related Topics

- Creating User Accounts, page 13-36
- Creating a New Scope, page 13-43

Creating and Managing Cisco ANA User Accounts

User accounts are created by using the functions in the User Management drawer. This drawer is in the Administration perspective under the Objects tab. From this drawer you can manage the following:

- Username and password information, including the option to use an external LDAP application to perform user authentication and manage all user passwords
- Status of the account (whether or not it is enabled), and information about when the user last logged in
- Cisco ANA role (Viewer, Network Operator, Configurator, Administrator)
- GUI client lockout and log out times (due to client inactivity)
- Scopes assigned to the user (see Creating and Managing Scopes, page 13-42 for configuring user scopes)

These topics describe what you need to know to administer user accounts:

- Understanding User Roles and Authentication, page 13-34
- Roles Required to Manage User Accounts, page 13-36
- Creating User Accounts, page 13-36

Understanding User Roles and Authentication

Cisco ANA provides a set of four predefined roles for security and access control to allow different system functions.

Table 13-18 Cisco ANA Roles

Role	Description
Viewer	Views the network, links, events, and inventory. Has read-only access to the network and to nonprivileged system functions.
Network Operator	Performs most day-to-day business operations such as managing alarms, manipulating maps, viewing network-related information, and managing business attachments.
Configurator	Performs tasks and tests related to configuration and activation of services, through Command Builder, Configuration Archive, NEIM, and activation commands.
Administrator	Manages the Cisco ANA system and its security. Performs all administrative actions, including creating units, AVMs, and VNEs; and managing polling and protection groups, users, scopes, and maps.

Cisco ANA automatically creates two users, called “root” and “emergency.” Both have administrator privileges. The Cisco ANA root user account is used internally by multiple Cisco ANA components. This user account may become overloaded if you use it to log into the Cisco ANA GUI client; it may cause timeout-related issues that could affect system behavior. Cisco recommends that you create multiple superuser accounts and avoid using the root user account.

The emergency user is created for LDAP in case of problems with the external authentication system. If the LDAP system should go down, the emergency user is the only user that can log back in to Cisco ANA and change the authentication method back to local. This is because the emergency LDAP user is not required to authenticate from the external system, but only from Cisco ANA. Because user passwords are not synchronized between Cisco ANA (local) and LDAP (remote) systems, the emergency user will have to manually reset passwords on the internal system so that other users can log in.

If you are using LDAP, be sure to add

If you use an LDAP application to manage passwords and add a user to the application, but no user account exists in Cisco ANA, the user will only be given Viewer privileges for all scopes.

Cisco ANA uses LDAP protocol version 3.

See these topics for more information:

- Roles Required to Manage User Accounts, page 13-36
- Creating User Accounts, page 13-36
- Viewing and Changing User Passwords and Account Properties, page 13-40
- Deleting a User Account, page 13-42

Roles Required to Manage User Accounts

Table 13-19 lists the roles that are required to manage user accounts. For more information on roles, see Creating and Managing Cisco ANA User Accounts, page 13-34.

Table 13-19 Roles Required to Manage User Accounts

Task	Role Required
Creating a new user account	Administrator
Viewing user account properties	Administrator
Editing an existing user account	Administrator
Viewing a user's password	Administrator
Editing a user's password	Administrator
Deleting a user account	Administrator

Related Topics

- Creating and Managing Users, Passwords, and Scopes, page 13-34
- Creating User Accounts, page 13-36
- Viewing and Changing User Passwords and Account Properties, page 13-40
- Deleting a User Account, page 13-42

Creating User Accounts

Note Creating a new user through the New User dialog box is only part of the user account creation procedure. Once you create a user account by specifying the general properties (username, password, and so forth), the user account appears in the Cisco ANA UI, but you cannot view any network elements. To allow you to view elements, you must assign at least one scope to yourself. Scopes control which network elements users can view, and the degree to which they can manipulate those elements (for example, editing and deleting). The complete user account creation procedure is provided in Creating User Accounts, page 13-36.

When you create a new user, the user account has the following characteristics by default:

- No scopes are assigned to you (unless you are an administrator, in which case the All Managed Elements scope is assigned)
- The password must be changed every 90 days.

The Cisco ANA "root" user account is used internally by multiple Cisco ANA components. This user account may become overloaded if you use it to log into the Cisco ANA GUI client; it may cause timeout-related issues that could affect system behavior. Cisco recommends that you create multiple superuser accounts and avoid using the root user account.

Note If a user is created using the LDAP application, but no user account exists in Cisco ANA, the user will only be given Viewer privileges for all scopes.

Reviewers: If they want to use LDAP, what are the prerequisites? (The prereqs will be described in the installation guide, but we need to tell users what they are. I will add a cross-reference to the installation guide too.

Also, I noticed on a system that was NOT using LDAP, that there was an emergency user anyway. Is this user always created, even if LDAP isn't being used? (Perhaps the system was using LDAP earlier; I'm not sure.)

Before You Begin

Perform the following prerequisites before adding users:

- If you plan to use LDAP for user authentication, be sure to do the following:
  - Properly configure the LDAP application as described in *Cisco Active Network Abstraction Installation and Setup Guide*. For the SSL encyrption protocol, a certificate must be installed on the server on which JBoss is installed.

Reviewers: What ceritificate is this (per above statement)? The install guide mentions the "Unlimited Strength Java(TM) Cryptography Extension (JCE) Policy Files for the Java(TM) 2 Platform, Standard Edition Development Kit, v5.0." Is that the certificate?

  - If you want to authenticate root using LDAP, configure an LDAP account for root.
- If desired, configure a message that is displayed when users log in. See Creating a Banner (Message of the Day), page 13-4.

To create a user account:

Step 1 Decide whether you want to use LDAP (external) authentication or Cisco ANA (local) authentication:

- If you are using LDAP, proceed to Step 2.
- If you are using Cisco ANA authentication, proceed to Step 3.

Step 2 To set up LDAP authentication, go to the Administration perspective, click the **Object s** tab, and click the **System Settings** drawer.

a. Click **External Authentication**. The External Authentication dialog box opens.

b. Enter the following information.

Note After you configure the LDAP authentication, you must restart the JBoss process. You will do this in Step 10.

Reviewers: Please carefully check the rules for the prefix and suffix.
Since CSCso92750 is resolved, I can say the prefix & suffix are validated -- but when does validation actually happen? After they click OK when they create the user?

Field	Description
Authentication Type	- LDAP—Instructs Cisco ANA to perform user authentication using an external authentication. (The LDAP application must be installed; see *Cisco Active Network Abstraction Installation and Setup Guide*.) - ANA System—Instructs Cisco ANA to perform user authentication using the information entered in User Management dialogs and stored on the gateway. If this type is selected, you do not need to configure any settings on this page. Proceed to Step 3.
Hostname	LDAP server name, as in **ldap://*server-name*** The LDAP server must be reachable from the server on which JBoss is installed.
Port	LDAP server port number, as in **ldap://***server-name***:*port-number*** The LDAP server port number is normally 389 for nonencrypted and 636 for encrypted, but you must verify this.
Distinguished Name Prefix	LDAP distinguished name prefix in the following form: *Key*= (The actual format is *Key*=*Value*, but leave *Value* empty because the host name is concatenated as *Value*.) *Reviewers: Can there be multiple entries? Like this: Key=Value, Key=*
Distinguished Name Suffix	LDAP distinguished name suffix, in the form: ,*Key*=*Value*, *Key*=*Value* The form should: - Begin with a comma because it is concatenated with preceding information. - End with the form *Key*=*Value* (with no ending symbols).
Protocol	Protocol used for encryption. Currently only SSL is supported. Remember that a certificate must be installed on the server on which JBoss is installed.

Step 3 To create the user account in Cisco ANA, go to the Administration perspective, click the **Objects** tab, and click the **User Management** drawer.

Step 4 Right-click **Users** and choose **New User**. The Create User dialog box opens.

Step 5 Enter the following information:

Field	Description
Username	A unique name for a user. A username must meet the following criteria: - Contains a maximum of 20 characters - Does not contain special characters (for example, * # ? and so forth) - Does not contain a user password
Full name	(Optional) A maximum of 20 characters, but no special characters, may be used.
Description	(Optional) A free-text description of the user.

Field	Description
Password	Password for this user. User passwords have a age of 90 days. Administrators can change user passwords. See Creating and Managing Users, Passwords, and Scopes, page 13-34. A password must meet the following criteria: **Note** If Cisco ANA is using LDAP for user authentication, you must still create a strong password for each user. If the user has no password, they will only be granted Viewer permissions, and failover will fail if authentication is changed from external to local. • Contains from 8 to 80 characters • Contains at least one character from each of the following classes: lowercase letters, uppercase letters, digits, and special characters • Does not contain characters that are repeated consecutively three or more times • Does not contain the username or its reverse • Is not the same as the last password • Is not cisco, ocsic, or any variant obtained by changing the capitalization You will have to reconfirm the password.
User Role	A a security access role that is your permission. **Note** The permission only applies to activities or actions that are not related to a network element. For more information on the functionality that a user can perform, see Creating and Managing Users, Passwords, and Scopes, page 13-34.
Lock system after ___ minutes of user inactivity	Period of time after which Cisco ANA locks the GUI client and displays a warning dialog, informing the user they have been locked out. The dialog lists the time remaining until they are completed logged out (which is controlled by the Log Out field), and also provides a login field so users can reauthenticate and reconnect to the GUI client. The client inactivity period can be any value from 0 (never lock system) to ??? minutes. The default inactivity period is 30 minutes *Need info for range.*
Log user out ___ minutes after system lock	Period of time after which Cisco ANA logs the user out of the GUI client. The log out time period begins after the lock system (inactivity) period has passed. The log out period can be any value from 0 (never log user out) to ??? minutes. The default is 30. *Need info for range.*
Force password change at next login	Forces user to change their password when they log in next (check box).

Step 6 Click **OK**. The new username is displayed in the Users tree.

Note A user cannot do anything with Cisco ANA until you assign a scope to them. Cisco ANA provides one predefined scope called All Managed Elements. To create new scopes, see Creating and Managing Scopes, page 13-42.

Step 7 Click the new user in the Users tree and go to the Security area to apply scopes to the user:

a. Choose a security role from the drop-down list (if you do not choose a role, the Viewer role is applied).

b. In the Access Rights area, click **Add** and enter the following information:

- Available Scopes—Choose a scope from the list of predefined and unassigned scopes. For more information, see Creating and Managing Scopes, page 13-42.
- Security Level—Choose the required security access role for the defined scope. For more information, see Creating User Accounts, page 13-36.

Step 8 Click **OK**. The scope is added to the list of access rights.

Step 9 Click **Apply**.

Reviewers: Do we want to tell the admin to restart Jboss, or to restart Cisco ANA?

Step 10 If you configured LDAP authentication (in Step 2), you must stop and restart JBoss for your LDAP configuration to take effect. You must be logged in as anauser to use this command.

```
# cmpctl -jboss stop
# cmpctl restart
```

Related Topics

- Creating and Managing Users, Passwords, and Scopes, page 13-34
- Creating User Accounts, page 13-36
- Viewing and Changing User Passwords and Account Properties, page 13-40
- Deleting a User Account, page 13-42

Viewing and Changing User Passwords and Account Properties

You can manage or edit general user account information, including when passwords should be changed.

Users can change their own password by logging in to the GUI client and selecting **Tools > Change Passwor**. from the main menu.

If you are using an external LDAP application for user authentication, and you change a user's name using the Cisco ANA user interface, you must also change the name in the LDAP application. Otherwise, the LDAP application will not authenticate the user, and the user will only be granted Viewer permissions.

To view or change user account properties:

Step 1 In the Administration perspective, click the **Objects** tab and click the **User Management** drawer.

Step 2 Open the Users tree to list all current users.

Step 3 Click a user to view the user properties in the primary content area. The following information is listed in the General area:

Field	Description
General Area	
Name	User name. The username cannot be modified. (For username rules, see Creating User Accounts, page 13-36
Last Login	The date and time that the user last logged in
Full Name	User's full name, if supplied when account was created.
Description	A free-text description of the user, if supplied when account was created.
Lock system after ___ minutes of user inactivity	Time period of GUI inactivity after which Cisco ANA locks the GUI client and displays a warning dialog, informing the user they have been locked out. *Need info for range.*
Log user out ___ minutes after system lock	After system lock period expires, period of time after which Cisco ANA logs the user out of the GUI client. *Need info for range.*
Force password change at next login	Forces user to change their password when they log in next (check box).
Security Area	
Default	The user's security role that controls the features the user can access.
Security Area/Access Rights	
Scope Name	The name of the scopes for which the user has the privileges described in the Security Level field. This controls the network elements the user can access.
Security Level	The security access role defined for the scope. For more information, see Editing a Scope and Viewing Scope Properties, page 13-44

Step 4 If you want to add a scope to the access rights of the user, click **Add**.

- Available Scopes—Choose a scope from the list of predefined and unassigned scopes. For more information, see Creating and Managing Scopes, page 13-42.
- Security Level—Choose the required security access role for the defined scope. For more information, see Creating User Accounts, page 13-36.

Step 5 Click **OK**. The scope is added to the list of access rights in the Security tab of the User Properties dialog box.

Step 6 You can use the Remove and Edit buttons to control current scope settings. Changes take effect when you click **OK**:

- Remove—Deletes a selected scope from the user's access rights.
- Edit—Edits the user's security level for the selected scope.

Step 7 Click the save icon in the main toolbar. The changes take effect the next time the user logs in to the GUI client.

Related Topics

- Creating and Managing Users, Passwords, and Scopes, page 13-34
- Creating a New Scope, page 13-43
- Viewing and Changing User Passwords and Account Properties, page 13-40
- Creating User Accounts, page 13-36
- Deleting a User Account, page 13-42

Deleting a User Account

When you delete a user account, the user-related information is deleted from the database and a security event is generated. If the user is active when you delete their account, Cisco ANA will display a confirmation asking if you still want to delete the user.

Reviewers: What does the user see if they are in a client session, and their account is deleted from Cisco ANA?

Step 1 In the Administration perspective, click the **Objects** tab and click the **User Management** drawer.

Step 2 Open the Users tree, and right-click the user and choose **Delete**.

Step 3 Confirm your choice.

Related Topics

- Creating and Managing Users, Passwords, and Scopes, page 13-34
- Creating a New Scope, page 13-43
- Creating User Accounts, page 13-36
- Viewing and Changing User Passwords and Account Properties, page 13-40

Creating and Managing Scopes

A scope is a named collection of managed network elements that have been grouped to allow a user to view and manage the network elements according to a given role. Grouping can be based on geographical location, network element type (such as DSLAM, router, software, and so on), network element category (such as access, core, and so on), or any other division according to the administrator's requirements.

Users cannot view any information regarding network elements, including basic properties, inventory, and alarms, that are outside their scope. Users also cannot do anything with managed network elements until a scope is assigned to them.

Multiple scopes can be assigned to a single user, and a single scope can be assigned to multiple users. When the scope is assigned to a user, you must also designate the user's security access role in that scope. This controls the user's actions in that scope. See Editing a Scope and Viewing Scope Properties, page 13-44.

See these topics for more information:

- Roles Required to Manage Scopes, page 13-43
- Creating a New Scope, page 13-43
- Editing a Scope and Viewing Scope Properties, page 13-44
- Deleting a Scope, page 13-44

Understanding the Scopes User Interface

The Scopes function is located in the User Management drawer (under the Object s tab in the Administration perspective). When you click **Scopes**, all defined scopes are listed.

The following tool buttons are located at the top right of the Configuration Archive Preferences workspace.

Table 13-20 Scopes Tool Buttons

Icon	Tooltip	Description
➕	Add Elements to this Scope	Adds network elements to the scope
🗑	Remove Selected Element(s)	Deletes the scope

Roles Required to Manage Scopes

Table 13-21 lists the roles that are required to manage scopes. For more information on scopes, see Creating and Managing Scopes, page 13-42.

Table 13-21 Roles Required to Manage Scopes

Task	Role Required
Creating a new scope	Administrator
Viewing scope properties	Administrator
Editing an existing scope	Administrator
Deleting a scope	Administrator

Related Topics

- Creating a New Scope, page 13-43
- Editing a Scope and Viewing Scope Properties, page 13-44
- Deleting a Scope, page 13-44
- Viewing and Changing User Passwords and Account Properties, page 13-40

Creating a New Scope

To create a scope:

Step 1 In the Administration perspective, click the **Objects** tab and click the **User Management** drawer.

Step 2 Right-click **Scopes** and choose **New Scope**.

Step 3 Enter a name for the scope in the Scope Name field. The name must be unique.

Step 4 Open the network element tree and select at least one device. Use the control buttons to add devices to the Selected Network Elements field.

Step 5 When you have finished, click **OK**. The scope is saved and displayed.

Related Topics

- Understanding the Scopes User Interface, page 13-43
- Editing a Scope and Viewing Scope Properties, page 13-44
- Deleting a Scope, page 13-44
- Viewing and Changing User Passwords and Account Properties, page 13-40

Editing a Scope and Viewing Scope Properties

You can edit the details of a scope and view its properties using the following procedure:

Step 1 In the Administration perspective, click the **Objects** tab and click the **User Management** drawer.

Step 2 Open the Scopes tree to display all configured scopes.

Step 3 Click the required scope to display the scope properties. For more information about the Properties dialog box, see Creating and Managing Users, Passwords, and Scopes, page 13-34.

Step 4 Edit and view the properties as required.

Step 5 Click **OK**. The Properties dialog box is closed.

Related Topics

- Creating a New Scope, page 13-43
- Understanding the Scopes User Interface, page 13-43
- Deleting a Scope, page 13-44
- Viewing and Changing User Passwords and Account Properties, page 13-40

Deleting a Scope

Use this procedure to delete a scope.

Note Deleting a scope removes it from the access rights of all users who are granted access to the scope.

To delete a scope:

Step 1 Verify that the scope you want to delete is not assigned to any users; otherwise, the delete operation will fail. (See Viewing and Changing User Passwords and Account Properties, page 13-40 for information on deleting a scope from a user account.)

Step 2 In the Administration perspective, click the **Objects** tab and click the **User Management** drawer.

Step 3 Open the Scopes tree to display all configured scopes.

Step 4 Right-click the required scope and choose **Delete**. The scope is deleted and is removed from the workspace.

Related Topics

- Creating a New Scope, page 13-43
- Editing a Scope and Viewing Scope Properties, page 13-44
- Understanding the Scopes User Interface, page 13-43
- Viewing and Changing User Passwords and Account Properties, page 13-40

System Security

This topic describes the key elements of Cisco ANA security. The *Cisco Active Network Abstraction 4.1 Installation and Setup Guide* also provides security information on topics such as ports and protocols used by Cisco ANA, user privileges required for installation, and issues pertaining to GUI client security.

Licenses

Cisco ANA supports several different types of licenses, which control what can be done on the Cisco ANA system. When a license is nearing its expiration, the licensing framework starts generating messages to remind you to renew or upgrade your license.

Step 1 From the main menu of any perspective, click **Help > About Cisco Active Network Abstraction**.

Step 2 In the About Cisco Active Network Abstraction dialog box, click **Server Details**.

Step 3 In the Server Details dialog box, click **Licenses**.

The licenses box lists all currently installed licenses, including the type and expiration date. For complete information on licenses, see *Cisco Active Network Abstraction 4.1 Installation and Setup Guide*.

Audit Trails

Audit and security events are listed in the Audit table in the Troubleshooting perspective.

GUI Client Inactivity Timeout

By default, a GUI client session is terminated if there is no client activity for a period of time (normally 30 minutes). Before terminating the session, the GUI client displays a dialog box that warns you of the impending disconnection and the time remaining until you are logged out. If you do not reauthenticate, the session is terminated, unsaved changes are lost, and a dialog box reports that you were logged out. If you do reauthenticate, a new GUI client session is started, but state information is not maintained from the previous session. Administrators define both the client inactivity (lock out) and log out periods when they create user accounts. (For more information, see Creating User Accounts, page 13-36.)

Authentication and Authorization

Cisco ANA offers two methods for performing user authentication:

- Local method—Cisco ANA performs authentication using the information entered when the user account was created (see Creating User Accounts, page 13-36). After three invalid login attempts, Cisco ANA disables the user's account, and a message informs the user to contact the system administrator.
- External method—The LDAP application can manage all of your user passwords. After three invalid login attempts, the LDAP application disables the user's account, and a message informs the user to contact the system administrator. Authentication data passed to the LDAP server is encrypted.

When the LDAP application is installed, an emergency user is also created. This user is authenticated only against the information in the Cisco ANA gateway. In that way, should the LDAP server become unavailable, the emergency user can still log in to Cisco ANA.

Authorization is controlled through the administration of roles and scopes. A role defines the functions a user is allowed to perform and the network elements a user is allowed to see and manage. Cisco ANA provides four predefined security access roles that can be granted to a user to enable system functions. A scope is a collection of managed network elements. By default, Cisco ANA includes a preconfigured scope, *All Managed Elements*, which cannot be edited or deleted, for the administrator's use. This scope includes all the managed network elements. A user who is granted the All Managed Elements scope can view and manage all the network elements all the time according to the user role assigned to the scope. For more information on scopes, see Creating and Managing Users, Passwords, and Scopes, page 13-34.

After a scope and role are allocated to a user, the user can perform various activities on the network elements included in the scope, such as viewing network elements, inventory, and link properties, and adding network elements to a scope view. See Creating and Managing Users, Passwords, and Scopes, page 13-34, for more information.

By default, users are limited to three login attempts, after which they are locked out of the system. Administrators can unlock user accounts by deselcting the Lock field in the user's account page (see Viewing and Changing User Passwords and Account Properties, page 13-40).

File Permissions

By default, permissions are set to 755.

Encryption and Secure Communication

Reviewers: Please confirm. Should we add anything about how communication between rich client and server is over SSH? I am not sure of how much detail I should give here.

Secure Socket Layer (SSL) keys are used for encryption. Cisco ANA system components communicate using secure sockets for the following:

- Server-to-client communication—Between gateways and clients (also using HTTPS).
- Interserver encryption—Between gateways and units.

The secured sockets use the same SSL keys, which are created at installation. Encryption key length is 128 bits. Client machines do not save critical data, such as credentials, nor do they communicate directly with the database.

In addition, new SSH keys are generated when the gateway server is installed and are used for server-unit communication. The unit obtains the key when the unit installation script is run. For more information, see the **INSTALLATION GUIDE**.

Cisco ANA uses secured storage. Cisco ANA implements a secured repository for sensitive data, and the data can be encrypted and decrypted. Recoverable passwords are encrypted using 3DES/AES, and unrecoverable passwords are encrypted using MD5 or SHA.

Authentication data passed to the LDAP server is also encrypted.

Related Topics

- Creating a Banner (Message of the Day), page 13-4
- Creating and Managing Users, Passwords, and Scopes, page 13-34
- Checking Basic System Health (CPU, Memory, JBoss), page 14-7

Backing Up and Restoring Data

The Cisco ANA backup and restore mechanism ensures data integrity and minimizes data loss for Cisco ANA. You can schedule regular backups or perform an on-demand backup on the gateway. When you perform a backup, Cisco ANA backs up all of the data on the gateway.

See these topics for the following information:

- For information on how to use the anabackup.sh script to back up your data, see Backing Up Your Data, page 13-47.
- For instruction on how to use the anarest.sh script to restore your data from a backup, see Restoring Your Data, page 13-49.

Backing Up Your Data

Note Cisco ANA does not back up the database information; you must back up your database separately. When a backup (either on demand or scheduled) is initiated, a notification is sent to the user reminding them to back up the database.

Use the **anaback.sh** script to back up your system. The script is located in *ANAHOME*/Main/backup/resources/scripts (*ANAHOME* is normally /export/home/ana41). The script format is:

anaback.sh [[**-d** *dd:mm:yyyy*] [**-t** *hh*:*mm*:*ss*] [**-e** *email_id*] [**-f** *filename*] [**-h** *frequency*]]

When the backup is complete, the backup file is placed in *ANAHOME*/backup/BackupDir. Backup files are stored in a zip file that uses the following filename scheme:

SUCCESS_*yyyy_mm_dd_hh_mm_ss***_.gz**

If any file is not copied, the filenames are copied to the log file and the backup filename is:

FAIL_*yyyy_mm_dd_hh_mm_ss***_.gz**

The anaback.sh script has the following options:

anaback.sh Options	Description
-d *dd*:*mm*:*yyyy*	Perform the on the specified day. If you do not specify a time using the -t option, the backup is performed at the time at which you run the anaback.sh script.
-t *hh*:*mm*:*ss*	Perform the backup at the specified hour (24-hour clock). If you do not specify a date using the -d option, the backup is performed at the next instance of the time you specified (later that day, or the next day).
-e *email_id*	Send e-mail to *email_id* with details of the backup job scheduled, and details when the job is completed. email_id must be in the format username@domain.
-f *filename*	Name the backup file with *filename* in the name string. The resulting zip file will be named one of the following: SUCCESS_*yyyy_mm_dd_hh_mm_ss_filename*.gz, or FAIL_*yyyy_mm_dd_hh_mm_ss_filename*.gz
-h *frequency*	Frequency at which to run the backup. Can be daily, weekly, or monthly.

When the backup is complete, the backup file is placed in *ANAHOME*/backup/BackupDir. Backup files are stored in a zip file that uses the following naming scheme:

SUCCESS_*yyyy_mm_dd_hh_mm_ss*.gz

If any file is not copied, the filenames are copied to the log file and the backup file is named as follows:

FAIL_*yyyy_mm_dd_hh_mm_ss*.gz

Use this procedure to perform a backup:

Step 1 Run the anaback.sh script, using any of the options listed previously. For example, the following command schedules the backup to happen immediately, repeat on a daily basis (at the same time), and insert the word DAILY into the backup filename:

```
ANAHOME/Main/backup/resources/scripts/anaback.sh -f DAILY -h daily
```

Step 2 Enter your credentials at the following prompts. The Cisco ANA JMX (Java Management Extensions) username is **admin**. The JMX password is synchronized with the Cisco ANA root password during installation, so enter the Cisco ANA root password. (Either password can be changed.)

```
Please Input ANA JMX username [admin]: admin
Please Input ANA JMX password: password
```

The anaback.sh script lists your settings.

Step 3 Confirm your choices. Upon completion, the script responds with a success or failure message. (Once you have scheduled your job, you can check the job by going to the Administration perspective Tasks tab and choosing **System Settings > Job Management.**)

Step 4 Confirm that your backup file is in the *ANAHOME*/backup/BackupDir directory. In the example above, the backup file would be named similarly to the following:

```
SUCCESS_2007_06_20_19_36_18_DAILY.tar.gz
```

Step 5 If you have not already done so, back up your database using the database software.

Related Topic

- Restoring Your Data, page 13-49

Restoring Your Data

Use the anarest.sh script to restore your data from a backup. The Cisco ANA gateway and component processes must be stopped when you perform a data restore. Before beginning the data restore operation, Cisco ANA compares the current application registry against the backed-up copy to verify that the restore does not place the system in an inconsistent state. Cisco ANA displays the list of differences and offers you the option of continuing the restore operation.

If you have done a fresh installation of Cisco ANA, you can restore data from a different gateway onto the new machine, as follows:

1. Copy the backup file from the remote gateway into the backup directory of the new gateway.
2. Stop the new gateway and component processes and perform the restore, as described in the following procedure.

Use the **anarest.sh** script to restore the data on your system. The script is located in *ANAHOME*/Main/backup/resources/scripts. The script format is:

anarest.sh [**-f** *filename*] *filename*

To perform a restore using a backup file that is *not* in the backup directory, specify the filename in the command line. If you do not specify a filename, Cisco ANA checks the backup directory and lists the available files for you to choose from. You can specify the filename with or without the **-f** option; *filename* must contain the full pathname.

Use this procedure to restore data from a backup file:

Step 1 Stop the gateway and component processes using the following command:

cmpctl stop

Step 2 Run the anarest.sh script. The script is located in *ANAHOME*/Main/backup/resources/scripts (*ANAHOME* is normally /export/home/ana41).

anarest.sh

The anarest.sh script lists the files that are stored in the backup directory, and prompts you to choose one, as in the following example:

```
1) SUCCESS_2007_06_20_19_36_18_.tar.gz
2) SUCCESS_2007_06_20_20_10_10_.tar.gz
File?
```

(You can specify a backup file that is not in the directory. An example would be: **anarest.sh -f /tmp/SUCCESS_2007_08_21_13_40_19_.tar.gz**.)

Step 3 Enter the number of the backup file you want to use for the restore. The anarest.sh script lists your choice and prompts you for a confirmation.

Step 4 Confirm your choices. The anarest.sh script verifies the restore to make sure the system is not placed into an inconsistent state, unpacks the files, and prompts you for a confirmation to proceed.

Step 5 Confirm the process. Upon completion, the script responds with a success or failure message.

Step 6 Start the gateway and component processes using the following command:

cmpctl start

If you need to restore your database information, see the database vendor documentation. For information on the **cmpctl** command, see Managing the Gateway, page 2-1.

Related Topic

- Backing Up Your Data, page 13-47

Reviewers: We will have a new procedure for writing logs to a separate disk. That will probably go here, once we have the info.

Installing Updates and Patches

Cisco ANA updates can contain new Cisco ANA features and patches for existing problems. This topic describes how to apply updates and patches to the gateway server, units, and GUI clients.

Updates and patches are posted on Cisco.com as they become available. To view the current version of your software, choose **Help > About**.

Patches are installed on Cisco ANA using the patchmng script. The script checks for prerequisites; if the prerequisites are not met, the script exits. You do not have to stop any Cisco ANA components while installing patches. The log file for patch management is in *ANAHOME*/Main/logs/patchmng.log, and the patch management audit file is stored in *ANAHOME*/patch_audit.txt.

The syntax of the patchmng script is as follows:

patchmng -jar *patchfile* [**-cp APPSRV|LEGACY|CLIENT|NONE**] [**-extract**] [-**show**]

patchmng -uninstall *patchfile*

Table 13-22 patchmng Options and Arguments

patchmng Options	Description
-jar *patchfile*	Installs the patch *patchfile* on the gateway server (which in turn downloads the *patchfile* to all units). Patches are supplied in a jar format. *patchfile* should be the full pathname of the jar file.

Table 13-22 patchmng Options and Arguments

[-cp *desintation*]	Installs the patch on only certain parts of the Cisco ANA system. *desintation* can be any of the following:	
	APPSERV	Installs the jar file on the gateway server only (that is, the gateway AVMs and Jboss). If you use this option, you must restart the gateway server after applying the patch.
	LEGACY	Installs the jar file on the units only (that is, the unit AVMs only). If you use this option, you must restart the units after applying the patch.
	CLIENT	Installs the jar file on the GUI client only.
	NONE	Installs the jar file. This argument should only be used with the **-extract** option (which invokes additional scripts in the jar file so the scripts can perform special actions). For example: **patchmng -jar /tmp/ana41patch-1.0.jar -cp NONE -extract**
[-extract]	Installs large patches that contain scripts used during the installation process (refer to the patch Readme to verify whether you need to use this option).	
[-show]	Lists all installed patches, specifying on which part of the application the patch is installed (for example, APPSERV or CLIENT).	
[-uninstall *patchfile*]	Uninstalls the patch *patchfile*. If patchfile does not exist, Cisco ANA generates an error message.	

To install a patch:

Step 1 Log into the gateway server as the Cisco ANA root user **anauser** (this is the user that installed Cisco ANA and also has UNIX root privileges). If you are already logged in as the UNIX root, use the following command to log in as anauser:

```
# su - anauser
```

Step 2 Back up the gateway server data as described in Backing Up Your Data, page 13-47.

Step 3 Download the patch to a temporary location on the gateway server, such as /tmp.

Step 4 Move to the directory in which the patch resides. (In this example, the location is /tmp.)

```
# cd /tmp
```

Step 5 On the gateway machine, run the patchmng script to install the patch (see Table 13-22 for patchmng options and arguments). For example, the following command would install the jar file on :

```
# patchmng -jar  filename
```

For example:

```
# patchmng -jar /tmp/ana41patch-1.0.jar
```

If the patch installation is successful, you will see a confirmation message and a reminder to restart Cisco ANA for the patch to take effect. (If you install a patch on the GUI client only, Cisco ANA will automatically restart the GUI client.)

Step 6 Restart Cisco ANA on the affected components.

- To restart the gateway server and units:

  ```
  # cmpctl restart
  ```

- To restart the gateway only:

  # cmpctl restart -jboss

- To restart the units only:

  # cmpctl restart -unit *

Step 7 If desired, delete the downloaded patch from its temporary location (specified in Step 3).

Once a patch is installed on the gateway server, it is automatically downloaded to all units. The patch is only downloaded to GUI clients if the auto-update feature is enabled; however, this feature is disabled by default. If auto-update is enabled, when users subsequently log in, the GUI client checks for the availability of new software, installs the software, and prompts the user to restart the GUI client. Administrators can enable this auto-update feature by adding or editing the following line to the ana.ini file in the GUI client home directory (normally C:\Program Files\Cisco Systems\ANAClient):

```
-Dauto.update=true
```

Related Topics

- Backing Up and Restoring Data, page 13-47
- Managing the Gateway, page 2-1

Understanding the Cisco ANA Registry

The registry is the Cisco ANA system configuration repository. It stores configuration parameters and values for the Cisco ANA gateway and for all Cisco ANA units. The registry also stores client and network resource feature configurations.

The Cisco ANA registry is a type of database. It consists of:

- Hives—XML-formatted physical text files that support and correspond to the tree of registry keys, subkeys, and entries.
- Keys—Define the general classes of entities the system supports. A key always has a name, and usually a source from which it inherits subkeys and entries. Each key can contain a number of subkeys, and the whole is arranged in a tree structure.
- Entries—Subordinate to keys or subkeys. An entry always has a name and a value. The value defines the behavior of any entity that is an instance of the corresponding key.

Direct editing of the registry should only be performed by Cisco Advanced Services; contact ask-ana@cisco.com for more information.

Caution Direct editing of the registry by unauthorized personnel, and liability for the results of such editing, are strictly limited in accordance with the terms and conditions set out in the customer license agreement. Cisco Systems disclaims any responsibility for damages of any kind caused by direct editing of the registry by unauthorized personnel.

The Cisco ANA registry is distributed. In practice, this means each Cisco ANA unit maintains its own copy of the registry:

- The golden source registry is created on the Cisco ANA gateway at installation time, based on a template registry. The golden source registry is the master copy of the registry in use by the Cisco ANA fabric. The gateway replicates all changes in the golden source registry to each Cisco ANA unit's local registry. Units that temporarily lose contact with the gateway receive a cached copy of these changes when connectivity is restored.
- The local registry is a copy of the golden source registry that each Cisco ANA unit downloads from the gateway at unit startup. The local registry allows the unit to function even when it cannot contact the gateway. The local registry is notified of and downloads changes to the golden source registry as they occur. The gateway maintains a copy of any overrides made to the unit's local registry, and the unit also uploads changes to this copy whenever they are made. Whenever that unit restarts in future, it downloads a new copy of the gateway's current golden source registry, plus any local registry overrides recorded for that unit.
- The template registry is a special area in the golden source which serves as a template for all other golden source registry areas. All changes done in this directory are automatically copied to all other golden source directories (this means that changes in this directory are actually system-wide changes).

Related Topics

- How Changes Affect the Registry, page 13-53
- Storing Registry Hives, page 13-54

How Changes Affect the Registry

The registry mechanism behaves similarly to that of inheritance in Object-Oriented Programming Languages. In other words, when a key has a entry set, this is similar to a Class being extended in Java. A registry key data is therefore composed of two parts: concrete data (physically written in that key's location) and inherited data (coming from parent keys). If we continue with the Object-Oriented programming analogy, this is similar to concrete methods and inherited methods in a class. It is important to add that not only entries are inherited, but also subkeys. Because a key's data is composed of both concrete and inherited data, registering for changes on a specific key causes implicit registration on inherited keys (hence, changes to inherited data triggers notifications as well).

One special hive in the registry is called Site. Site is the place to concentrate all changes made to the registry on a customer site. Any first level key placed under site is added to the path during runtime. For example, if we have a key called Key1, extended by (that is, has a "" entry set to) ParentKey1 (path: Key1>ParentKey1), and we place under Site a key called ParentKey1, the path is now: Key1>site/ParentKey1>ParentKey1.

Related Topics

- Understanding the Cisco ANA Registry, page 13-52
- Storing Registry Hives, page 13-54

Storing Registry Hives

The golden source registry hives are located on the Cisco ANA gateway in *ANAHOME*/Main/registry/ConfigurationFiles. (*ANAHOME* is normally /export/home/ana41.)

Note Contact ask-ana@cisco.com if you want to change this path.

Subfolders of this path maintain the following hive files:

- The template registry hives, with the keys and values supplied with the installation, stored in subfolder /0.0.0.0. The keys and values in this base version of the registry are inherited by all other registry instances.
- The golden source registry hives, stored in /127.0.0.1.
- The local registry hives, stored in a subfolder with the IP address of the unit using that local registry.

Related Topics

- How Changes Affect the Registry, page 13-53
- Understanding the Cisco ANA Registry, page 13-52