CHAPTER 14

Monitoring Your Network

Date: 7/14/09

The ANM Monitor function allows you to monitor key areas of system usage. The following functionality is provided under Monitor:

- Devices—Provides statistics about devices including resource usage, traffic information, load balancing, and allows you to enable or disable polling. See Device Monitoring Features, page 14-3.

Note ANM does not support monitoring on chassis.

- Events—Lists events originated from devices through syslog, SNMP traps. See Monitoring Events, page 14-22.
- Device Audit Trail Logging—Lists device configuration and deployment changes to device, and associated descriptions for viewing and troubleshooting. See Device Audit Trail Logging, page 14-25.
- Alarm Notifications—Allows you to define thresholds and view alarms. See Configuring Alarm Notifications, page 14-27.
- Settings—Allows you to set global polling and SMTP configurations. See Setting Polling Parameters, page 14-20.
- Tools—Allows you to verify connectivity (using the ping command) between a virtual context and an IP address that you specify. See Testing Connectivity, page 14-34.

Before using the Monitoring functions, make sure your devices are properly configured for polling (see Setting Up Devices for Monitoring, page 14-2).

Setting Up Devices for Monitoring

In order for ANM to successfully monitor your devices, you must configure the devices correctly for polling as show in Table 14-1.

Table 14-1 Configuring Devices for Monitoring

Device Type	How to Configure	Parameters to Configure
ACE 1.0 modules	Configure parameters on each virtual context you want ANM to monitor.	• All devices must have a routable IP address from the ANM. • The management policy with the SNMP protocol must be associated to the IP address. • You must enable SNMPv2c with a matching SNMP community string between ANM and the devices to be polled. (See Configuring Virtual Contexts, page 3-1.) • Before using the Monitoring functions, you must enable monitoring on all devices that you want ANM to monitor (see Setting Polling Parameters, page 14-20).
ACE 2.0 modules	Configure parameters on the Admin context only.	
ACE appliances running images A1(8) and A3(1.0)	Configure parameters on each virtual context you want ANM to monitor.	
CSS	Configure parameters on the CSS devices you want ANM to monitor. You cannot use ANM to configure the devices.	• All devices must have a routable IP address from the ANM. • For CSS devices, you must enable SNMPv2c with a matching SNMP community string between ANM and the devices to be polled. (See Configuring CSS Primary Attributes, page 2-29.) • For CSM devices, you must enable SNMPv2c with a matching SNMP community string on the Cat6K chassis in which the CSM resides. (See Configuring CSM Primary Attributes, page 2-28.) • Before using the Monitoring functions, you must enable monitoring on all devices that you want ANM to monitor (see Setting Polling Parameters, page 14-20).
CSM	Configure parameters on the CSM devices you want ANM to monitor. You cannot use ANM to configure the devices.	

Related Topics

- Device Monitoring Features, page 14-3
- Monitoring Device Groups, page 14-3
- Monitoring Devices, page 14-4

Device Monitoring Features

ANM provides several features that allow you to monitor your devices:

- System View—Provides device information and a general overview of your system as a whole, including High Availability (HA) information and licensing information. See Monitoring the System, page 14-5.
- Resource Usage—Provides resource usage information on connections and features. See Monitoring Resource Usage, page 14-5. This feature is not available for CSS or CSM devices.
- Traffic Summary—Provides traffic information for your devices. See Monitoring Traffic, page 14-9.
- Load Balancing—Provides virtual server information and load balancing statistics. See Monitoring Load Balancing on Virtual Servers, page 14-13 and Monitoring Load Balancing Statistics, page 14-17.
- Application Acceleration—Displays optimization statistics for ACE appliances on which you have configured application acceleration functions. See Monitoring Application Acceleration, page 14-19. This feature is only available on ACE appliances.
- Polling Settings—Allows you to set polling parameters. See Setting Polling Parameters, page 14-20.

Related Topic

- Monitoring Device Groups, page 14-3

Monitoring Device Groups

You can display monitoring information for device groups that you create in ANM (see Configuring User-Defined Groups, page 2-61). When you select **Monitor > Devices > Groups > *device_group***, *all* monitoring features that are supported on any of the devices in the device group are displayed. Because some monitoring features, for example, Application Acceleration, are not supported on all device types, you can click the following buttons at the bottom of the Monitor screens to change what information is displayed:

- **Show Polled Devices**—By default, only the devices in the device group that support the specified feature are displayed.
- **Show All Devices**—All devices in the device group are shown on the Monitoring results screen, whether or not the feature you selected is supported on all the devices.

For example, if you create a device group that contains an ACE appliance and several other different device types, then select **Monitor > Devices > Groups > *device_group*> Application Acceleration**, by default, only the ACE appliance appears in the Application Acceleration screen because the other device types in the device group do not support this feature. If you click **Show Polled Devices**, all devices in the device group are displayed.

When viewing monitoring information, you might see *N/A* or an empty cell in the monitoring results:

- *N/A* indicates that ACE Device Manager was not able to obtain the specified value. In addition, the monitoring screen displays *N/A* in certain fields for which polling has not been executed.
- An empty cell indicates that the value is not applicable.

Related Topics

- Setting Up Devices for Monitoring, page 14-2
- Device Monitoring Features, page 14-3

- Monitoring Devices, page 14-4

Monitoring Devices

ANM monitors activities on ACE, CSS, and CSM devices. When you select **Monitor > Devices**, you can view device information. Using SNMP and CLI commands, ANM gathers information about your devices and displays the information.

Note ACE devices provide no direct statistics via SNMP MIBs in order to monitor the state of virtual servers. While there are ACE CLIs called by the ANM to give some visibility, these currently cannot be parsed for effective batch monitoring.

Note If you get a warning message indicating that monitoring is not enabled or functioning, you must enable statistic monitoring on the device. See Setting Polling Parameters, page 14-20.

Table 14-2 lists the features that appear under **Monitor > Devices**, depending on which device type you select in the device tree.

Table 14-2 Supported Monitor > Devices Features According to Device Type

Device Type Selected in the Device Tree		Supported Features Displayed Under Monitor > Devices					
		System View	Resource Usage[1]	Traffic Summary	Load Balancing	Application Acceleration	Polling Settings
ACE module		X	X	X	X		
	Admin context	X	X	X	X		X
	User context		X	X	X		X
ACE appliance		X	X	X	X	X	
	Admin context	X	X	X	X	X	X
	User context		X	X	X	X	X
CSS		X		X	X[2]		X
CSM		X			X		X
GSS							X
Groups[3]		X	X	X	X	X	

1. See Monitoring Resource Usage, page 14-5 for information about the options available under Resource Usage.
2. CSS devices support Virtual Servers only, so you do not see the **Load Balancing > Statistics** menu option.
3. By default, all monitoring features that are supported on any of the devices in the device group appear when you select a device group. See Monitoring Device Groups, page 14-3 for more information about monitoring various device types within a device group.

Related Topics

- Monitoring Device Groups, page 14-3
- Monitoring the System, page 14-5
- Setting Up Devices for Monitoring, page 14-2

- Setting Polling Parameters, page 14-20

Monitoring the System

ANM provides a System View that displays device information and a general overview of your system as a whole. If a module has crashed, you can use the System View to find out when and why the crash occurred and display information that affects the module. The System View also displays High Availability (HA) information and licensing information.

Note For ACEs, the System View is available in the Admin context only.

Note ANM does not support monitoring of chassis.

Procedure

Step 1 Select **Monitor > Devices >** *device* **> System View**. The information that is displayed depends on what device type you select in the device tree.

Step 2 The System View displays the following information:

- Device Information
- High Availability
- License Status
- Module Information (for CSS devices only)

Note You can sort the information displayed in the table by clicking on a column heading.

Step 3 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 4 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- Setting Up Devices for Monitoring, page 14-2
- Setting Polling Parameters, page 14-20
- Monitoring Traffic, page 14-9

Monitoring Resource Usage

ANM provides resource usage so that you can easily determine if you need to reallocate resources to a particular virtual context, view traffic usage in your contexts, or determine available usage for your contexts. There are two modes in which ANM provides resource usage for ACEs:

- Virtual-context based resource usage—You must select a virtual context from the device tree to view resource usage specific to the context (see Monitoring Virtual Context Resource Usage, page 14-6).
- System-wide resource usage—You must select an ACE module or appliance from the device tree to view system-wide information and to display the following options:
  - Connections—Displays traffic resource usage information. See Monitoring System Traffic Resource Usage, page 14-7.
  - Features—Displays non-connection based resource usage information. See Monitoring System Non-Connection Based Resource Usage, page 14-8.

See the "Configuring Virtualization" chapter of either the *Cisco Application Control Engine Module Virtualization Configuration Guide* or the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide* for the maximum resource usage value for each attribute.

Monitoring Virtual Context Resource Usage

ANM displays resource usage for virtual contexts as explained in the following steps.

See the "Configuring Virtualization" chapter of either the *Cisco Application Control Engine Module Virtualization Configuration Guide* or the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide* for the maximum resource usage value for each attribute.

Procedure

Step 1 Select **Monitor > Devices >** ***virtual_context*** **> Resource Usage**. The information in Table 14-3 is displayed.

Table 14-3 Virtual Context Resource Usage Field Descriptions

Field	Description
ACL Memory (Bytes)	ACL memory usage
Application Acceleration Connections (conn)	Number of application acceleration connections. **Note** This field displays if you selected an ACE appliance in the device tree.
Bandwidth (Bytes/Sec)	Bandwidth in bytes per second
Concurrent Connections (Connections)	Number of simultaneous connections
Connection Rate (Connections/Sec)	Connections per second
HTTP-comp rate	HTTP compression rate. **Note** This field displays if you selected an ACE appliance in the device tree.
Inspect Connection Rate (Connections/Sec)	RTSP/FTP inspection connections per second
MAC Miss Rate (Connections/Sec)	MAC miss traffic punted to CP packets per second
Management Connection Rate (Connections)	Number of management connections
Management Traffic Rate (Connections/Sec)	Management traffic bytes per second
Proxy Connection Rate (Connections)	Proxy connections
Regular Expression Memory (Bytes)	Regular expressions usage in bytes

Table 14-3 Virtual Context Resource Usage Field Descriptions

Field	Description
SSL Connection Rate (Transactions/Sec)	SSL (Secure Sockets Layer) connections per second
Syslog Buffer Size (Bytes)	Syslog message buffer size in bytes
Syslog Message Rate (Messages/Sec)	Syslog messages transmitted in messages per seconds.
Throughput (Bytes/Sec)	Displays through-the-ACE traffic. This is a derived value (you cannot configure it directly) and it is equal to the bandwidth rate minus the mgmt-traffic rate for the 1-Gbps and 2-Gbps licenses.
Translation Entries	Current number of network and port address translations

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- Monitoring System Traffic Resource Usage, page 14-7
- Monitoring System Traffic Resource Usage, page 14-7

Monitoring System Traffic Resource Usage

ANM displays system-wide traffic resource usage as explained in the following steps. See the "Configuring Virtualization" chapter of either the *Cisco Application Control Engine Module Virtualization Configuration Guide* or the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide* for the maximum resource usage value for each attribute.

Note You must select an ACE module or appliance from the device tree to view system-wide traffic resource usage information as shown in the following steps.

Procedure

Step 1 Select **Monitor > Devices >** ***ACE*** **> Resource Usage > Connections**.

The current resource usage information is displayed as shown in Table 14-4.

Note There might be a slight delay because the resource usage information is gathered real-time.

Table 14-4 Resource Usage Connections Field Descriptions

Field	Description
Context	Name of the virtual context
Conc. Conn. %	Number of simultaneous connections
Mgmt. Conn. %	Number of management connections

Table 14-4 Resource Usage Connections Field Descriptions

Field	Description
Proxy Conn. %	Proxy connections
Bandwidth(Bytes/S) %	Bandwidth in bytes per second
Throughput (Bytes/S)	**Note** This field displays if you selected an ACE 2.0 device in the device tree. Throughput in bytes per second
Conn. Rate(Conn./S) %	Connections per second
SSL Conn. Rate(Trans./S) %	SSL (Secure Sockets Layer) connections per second
Mgmt. Traffic Rate(Conn./S) %	Management traffic connections per second
MAC Miss Rate (Conn./S) %	MAC miss traffic punted to CP packets per second
Insp. Conn. Rate(Conn./S) %	RTSP/FTP inspection connections per second
App. Acc. Conn. %	Number of application acceleration connections. **Note** This field displays if you selected an ACE appliance in the device tree.
HTTP-Comp Rate %	HTTP compression rate. **Note** This field displays if you selected an ACE appliance in the device tree.

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- Monitoring Resource Usage, page 14-5
- Monitoring System Non-Connection Based Resource Usage, page 14-8

Monitoring System Non-Connection Based Resource Usage

ANM displays system-wide, non-connection-based resource usage as explained in the following steps.

Note You must select an ACE module or appliance from the device tree to view the non-connection based resource usage information as shown in the following steps.

Step 1 Select **Monitor > Devices >** ***ACE*** **> Resource Usage > Features**.

The current resource usage information is displayed shown in Table 14-5.

Note There might be a slight delay because the resource usage information is gathered real-time.

Table 14-5 Resource Usage Features Field Descriptions

Field	Description
Context	Name of the virtual context
Translation Entries %	Current number of network and port address translations
ACL Memory (Bytes) %	ACL memory usage in bytes
RegEx Memory (Bytes) %	Regular expressions memory usage in bytes
Syslog Buffer Size (Bytes) %	Syslog message buffer size in bytes
Syslog Message Rate (Messages/S) %	Syslog messages per second

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- Monitoring Resource Usage, page 14-5
- Monitoring System Traffic Resource Usage, page 14-7

Monitoring Traffic

ANM determines traffic information for your ACE and CSS devices by calculating the delta traffic values since the last polling cycle and displays the resulting values. You can view traffic summary information as shown in the steps below.

Note To get traffic data polled directly from a device, click on an interface name that is displayed in the Interface column. See Viewing Device-Specific Traffic Data, page 14-12.

Procedure

Step 1 Select **Monitor > Devices >** ***device*** **> Traffic Summary**. The information show in Table 14-6 is displayed.

Note You can click on any column heading to sort the table by that column.

Table 14-6 Traffic Summary Fields

Field	Description
Device	Fully-qualified device name. This field does not appear for CSS devices.
Interface	Name of the interface. Click on the interface hyperlink to get traffic data polled directly from the device as shown in Table 14-7.
Admin Status	User-specified status of the device, which can be one of the following states: • Up • Down • Testing, which indicates that no operational packets can be passed.
Operational Status	Current operational status of the device, which can be one of the following states: • Up • Down • Testing, which indicates that no operational packets can be passed • Unknown • Dormant, which indicates the interface is waiting for external actions (such as a serial line waiting for an incoming connection) • Not present, which indicates the interface has missing components
Packets In / Sec	This field appears for ACEs only. Per second, the number of packets delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
Packets Out / Sec	This field appears for ACEs only. Per second, the total number of packets that higher-level protocol requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
Bytes In / Sec	Number of octets received, including framing characters, per second.
Bytes Out / Sec	Number of octets per second transmitted out of the interface, including framing characters.
Errors In / Sec	Number of inbound packets discarded per second because they contained errors or because of an unknown or unsupported protocol
Errors Out / Sec	Number of outbound packets discarded per second because they contained errors or because of an unknown or unsupported protocol

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Step 4 Select a device, then click **Details** to see specific traffic information for the selected device. See Viewing Device-Specific Traffic Data, page 14-12

Related Topic

Viewing Device-Specific Traffic Data, page 14-12

Viewing Device-Specific Traffic Data

Procedure

Step 1 Select **Monitor > Devices >** *device* **> Traffic Summary**. Hyperlinked device names are displayed in the **Interface** column.

Step 2 Select a hyperlinked device name. **The Traffic Summary Details for Interface:** ***device name*** screen appears. The information shown in Table 14-7 is displayed.

Note You can click on a column heading to sort the table by that column.

Table 14-7 Traffic Summary Details Window Description

Device Type	Field	Description
ACEs and CSS	Bytes In	Total number of octets received on the interface, including framing characters
	Bytes Out	Total number of octets transmitted out of the interface, including framing characters
	Discarded Inbound Packets	Number of inbound packets which were discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol
	Discarded Outbound Packets	Number of outbound packets which were discarded even though no errors were detected to prevent their being transmitted
	Inbound Packet Errors	Total number of inbound packet errors
	Inbound Packets with Unknown Protocol	Total number of packets received via the interface which were discarded because of an unknown or unsupported protocol
	Outbound Packet Errors	Total number of outbound packet errors
	Packets In	Number of packets delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
	Packets Out	Number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
CSS only	Active TCP	Current number of active TCP flows on the interface
	Active UDP	Current number of active UDP flows on the interface
	FCB Count	Number of unused fastpath flow control blocks for the interface
	TCP Average	Five second moving average of TCP flows per second on the interface
	TCP Current	Number of new TCP flows within last second on the interface
	TCP High	Maximum number of TCP flows in any one second interval on the interface
	TCP Total	Total TCP flows on the interface
	UDP Average	Five second moving average of UCP flows per second on the interface
	UDP Current	Number of new UDP flows within last second on the interface
	UDP High	Maximum number of UDP flows in any one second interval on the interface
	UDP Total	Total UDP flows on the interface

Step 3 Click **OK** to close the window and return to the Traffic Summary screen.

Related Topic

Monitoring Traffic, page 14-9

Monitoring Load Balancing on Virtual Servers

ANM monitors load balancing and allows you to view the information as shown in the following steps.

You can view additional information about real servers, such as the number of servers that are functioning properly, and probes, such as viewing if an excessing number of probes are failing, by clicking the hyperlink in the respective columns in Table 14-8.

Step 1 Select **Monitor > Devices >** ***device*** **> Load Balancing > Virtual Servers**. Depending on the device type you selected in the device tree, the information described in Table 14-8 is displayed.

Note If you select a CSS device from the device tree, the navigation path does not include Load Balancing; the path is **Monitor > Devices >** ***CSS_device*** **> Virtual Servers**.

Table 14-8 Load Balancing Monitoring Information

Device Type	Field	Description
All	Device	Fully-qualified device name
	Virtual Server	Name of the virtual server **Note** If a virtual server is associated with primary and backup server farms, two entries appear in the table: One for the primary server farm and one for the backup server farm.
	IP Address	IP address of the virtual server
	Protocol	Protocol the virtual server supports, which can be: • Any—Indicates the virtual server is to accept connections using any IP protocol. • TCP—Indicates that the virtual server is to accept connections that use TCP. • UDP—Indicates that the virtual server is to accept connections that use UDP.
	Port	Port to be used for the specified protocol
ACEs, CSS, CSM	Service Policy	Policy map applied to the device
	Server Farm	Name of the server farm associated with the virtual server.

Table 14-8 Load Balancing Monitoring Information

Device Type	Field	Description
ACEs only	Algorithm	Type of predictor algorithm specified on the load balancer, which can be: • Roundrobin • Leastconn • Hash_url • Hash_addres • Hash_cookie • Hash_header
	Action	Indicates if the device is functioning as a primary server (Primary) or a backup server (Backup).
ACEs, CSS	Admin Status	User-specified status of the virtual server, which can be: • In Service—Indicates the server is in service. • Out of Service—Indicates the server is out of service.
All	# Rservers Up	Number of servers up/Number of total servers configured **Note** You can click on the hyperlink in this column to view statistics for the real servers configured for the specified virtual server. See Viewing Virtual Server Statistics, page 14-15.
ACEs, CSSs, CSM	# Probes Failed	Number of probes failed/Number of probes configured **Note** You can click on the number displayed to view the statistics for the probes configured for the specified virtual server. See Viewing Probes Statistics, page 14-16.
ACE 4710 running image A3(1.0) only	Operational Status	Whether appliance is activated or suspended.
	Current Connections	Current number of connections.
CSM	No. of Connections	Current number of connections
CSM	Total Connections	Total number of connections

Step 2 Click on a virtual server, then click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- Viewing Virtual Server Statistics, page 14-15
- Viewing Probes Statistics, page 14-16

Viewing Virtual Server Statistics

Step 1 Select **Monitor > Devices >** ***device*** **> Load Balancing > Virtual Servers**. The Statistic Viewer displays information about the virtual servers.

Step 2 In the # Rservers Up column, click on the number displayed. The Real Servers window displays the information shown in table Table 14-9.

Table 14-9 Real Server Statistics Details

Device Type	Field	Description
All	Virtual Server	Name of the real server.
	IP Address	IP address of the real server. This field appears only for real servers specified as hosts.
	Protocol	Transport protocol specified for the virtual server (Any, TCP, or UDP).
	Port	Port number used for the server port address translation (PAT).
	Server Farm	Primary server farm to use for load balancing.
	Action	Indicates if the virtual server is functioning as a primary server (Primary) or a backup server (Backup).
	Algorithm	Method assigned for selecting the next server in the server farm to respond to client requests.
	Total Connections	Number of total connections, including current, failed, and dropped connections.
ACE 4710 Running Image A3(1.0)	Current Connections	Number of current connections to this server. If this field indicates *N/A*, the database does not have any information about current connections. If this field is 0, the database received an SNMP response of 0.
	Connections Rate	Connections per second.
	Dropped Connections	Number of dropped connections.
	Dropped Connections Rate	Dropped connections per second.
	Weight	Weight assigned to the real server.
	Admin Status	The specified state of the server, which can be: • In Service—Indicates the server is in service. • Out of Service—Indicates the server is out of service. • In Service Standby—Indicates the server is a backup server and remains inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.
	Operational Status	The state of the server, which can be: • In Service—Indicates the server is in service. • Out of Service—Indicates the server is out of service. • In Service Standby—Indicates the server is a backup server and remains inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.

Step 3 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 4 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- Monitoring Load Balancing on Virtual Servers, page 14-13
- Viewing Probes Statistics, page 14-16

Viewing Probes Statistics

To check the health and availability of a real server, the ACE periodically sends a probe to the real server. If you notice an excessive number of probes failing, you can view the monitoring information as shown in the following steps.

Procedure

Step 1 Select **Monitor > Devices >** ***ACE*** **> Load Balancing > Virtual Servers**. The Statistic Viewer displays information about the virtual servers.

Step 2 In the # Probes Failed column, click on the number displayed. The Monitoring Probe Details window displays the information shown in table Table 14-10.

Table 14-10 Monitoring Probe Details Window

Field	Description
Name	Name of the probe
Type	Type of probe. For a complete list of probe types and their descriptions, see Table 5-9.
IP Address	IP address the probe is polling
State	State of the probe, which can active or inactive
Passed	Number of passed probes
Passed Rate	Rate of passed probes
Failed	Number of failed probes
Failed Rate	Rate of failed probes

Step 3 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 4 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- Monitoring Load Balancing on Virtual Servers, page 14-13
- Monitoring Load Balancing Statistics, page 14-17

Monitoring Load Balancing Statistics

You can monitor load balancing on your ACE and CSM devices as shown in the following procedure.

Procedure

Step 1 Select **Monitor > Devices >** ***device*** **> Load Balancing > Statistics**. The Statistic Viewer displays the information described in Table 14-11.

Table 14-11 Load Balancing Statistic Viewer Information

Device Type	Field	Description
All	Device	Name of the device
CSM only	Current Connections	Number of current connections
ACEs only	L4 Policy Conn.	Number of Layer 4 policy connections
	L7 Policy Conn.	Number of Layer 7 policy connections
All	Failed Conn.	Number of failed connections
	Dropped L4 Policy Conn.	Number of dropped Layer 4 policy connections
	Dropped L7 Policy Conn.	Number of dropped Layer 7 policy connections
	Rejected Conn. Due To No Policy Match	Number of connections rejected because they did not match policies
	Rejected Conn. Due To ACL deny	Number of connections rejected due to ACL parameters
	Rejected Conn. Due To L7 Config Changes	Number of rejected connections due to Layer 7 configuration changes
ACEs only	Conn. Timed Out	Number of connections that timed out
CSM only	Created Conn.	Number of created connections
	Established Conn.	Number of established connections
	Destroyed Conn.	Number of destroyed connections
	Server Initiated Conn.	Number of server initiated connections
	Failed Server Initiated Conn.	Number of failed server initiated connections
	Bad SSL Format Rejects	Number of connections rejected due to bad SSL form
	No Active Server Rejects	Number of connections rejected because there was no active server
	MaxParseLen Rejects	Number of connections rejected because they exceeded the maximum parse length.
	L7 ParserError Rejects	Number of connections rejected because of Layer 7 errors
	OutOfMemory Rejects	Number of connections rejected because of memory

Table 14-11 Load Balancing Statistic Viewer Information (continued)

Device Type	Field	Description
CSM only	Created Connections	Number of TCP and UDP connections created since SLB was configured
	Established Connections	Number of connections established through SLB (reached the ESTAB state)
	Destroyed Connections	Number of TCP and UDP connections destroyed by SLB, either by TCPIP teardown or timeout. UDP connections can only be timed out
	Server Initiated Connections	Total number of connections initiated by the servers
	Failed Server Initiated Connections	Number of server initiated connections that failed
	Bad SSL Format Rejects	Number of connections rejected because some invalid or unrecognized SSL format was detected
	No Active Server Rejects	Number of connections rejected because the chosen server farm did not have any active servers
	MaxParseLen Rejects	Number of connections rejected because the length of an HTTP request or response header exceeded the maximum L7 parse length configured for the matching virtual server
	L7 Parser Error Rejects	number of connections rejected because an error occurred while parsing the connection data at Layer 7
	Out of Memory Rejects	number of connections rejected because the SLB module could not allocate the required memory

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topic

Testing Connectivity, page 14-34

Monitoring Application Acceleration

If you have configured application acceleration functions on the ACE, you can monitor the optimization statistics as shown in the following steps.

Step 1 Select **Monitor > Devices >** ***device*** **> Application Acceleration**. The Application Accelerator information is displayed as shown in Table 14-12.

Note For connection-based syslogs, the following additional parameters are displayed: Source IP, Source Port, Destination IP, Destination Port, and Protocol Information. This allows you to sort and filter on these fields if desired.

Table 14-12 Application Acceleration Monitoring View

Field	Statistic	Description
Condenser Information	Total HTTP unoptimized requests received	Total number of end-user HTTP request the condenser has received that cannot be optimized
	Accumulated bytes received	Accumulated size (in bytes) of each end-user requested object
	Total responses in bytes	Accumulated size (in bytes) of responses, both for condensable and non-condensable end-user HTTP requests
	Total abandons of delta optimization	Total number of abandons of delta optimization requests
Cacheable Objects Statistics	Total objects served from cache	Total number of cacheable objects served from the cache, excluding the not-modified replies
	Accumulated bytes served	Accumulated size (in bytes) of the cacheable objects served from the cache, excluding not-modified replies
	Total objects not found in cache	Total number of cacheable objects not found in the cache
	Accumulated bytes not found	Accumulated size (in bytes) of the cacheable objects not found in the cache
	Total IMS requests for valid cache	Total number of IMS requests for valid copies of objects in the cache
	Total missed IMS Requests	Total number of IMS request for objects that either do not exist or are stale in the cache
	Total non-cacheable object requests	Total number of non-cacheable object requests
	Total requests with non modified responses	Total number of requests for stale objects that have the response from the origin server as not modified

Table 14-12 Application Acceleration Monitoring View

Field	Statistic	Description
Flash Forward Objects Statistics	Successful transformations	Total number of successful transformations for FlashForward objects
	Unsuccessful transformations	Total number of unsuccessful transformations for FlashForward objects
	Total HTTP requests	Total number of HTTP requests (excluding the IMS requests) for the transformed FlashForward objects
	Total IMS requests	Total number of IMS requests for transformed FlashForward objects

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topic

Configuring Application Acceleration and Optimization, page 12-1

Setting Polling Parameters

You set polling parameters differently depending on the device type:

- ACE devices—You set polling on specific virtual contexts or configure global polling.
- CSM devices—You specify a single polling setting used by ANM.
- CSS devices—You specify a single polling setting used by ANM.
- GSS devices—You specify a single polling setting used by ANM for VIP Answers operation and configuration states and DNS Rules configuration states.

When you select **Monitoring**, the monitoring data for your devices is extracted from cache. The Monitoring screen refreshes every two minutes as new monitoring data is gathered.

When you import a context or device into ANM, the polling interval is set to 5 minutes by default. You can modify the polling parameter on each device (see Enabling Polling on Specific Devices, page 14-21) or you can modify the global parameter polling setting to change the polling parameters for all devices (see Enabling Polling on All Devices, page 14-21).

Related Topics

- Enabling Polling on All Devices, page 14-21
- Enabling Polling on Specific Devices, page 14-21

Enabling Polling on Specific Devices

Procedure

Step 1 Select **Monitor > Devices >** ***context*** **> Polling Settings**.

Step 2 In the Polling Stats field, click **Enable**.

Step 3 From the Background Polling Interval field, select a polling interval.

Step 4 Click **Deploy Now** to save and apply the polling parameters.

Related Topics

- Enabling Polling on All Devices, page 14-21
- Disabling Polling on Specific Devices, page 14-21

Disabling Polling on Specific Devices

Procedure

Step 1 Select **Monitor > Devices >** ***context*** **> Polling Settings**.

Step 2 In the Polling Stats field, click **Disable**.

Step 3 Click **Deploy Now** to disable polling.

Related Topics

- Enabling Polling on Specific Devices, page 14-21
- Enabling Polling on All Devices, page 14-21

Enabling Polling on All Devices

You can enable polling and set the polling interval for all devices as shown in the following steps.

Note Currently this feature is available for any user under the ANM Inventory role task. When a user is assigned this task, global polling configuration changes made will apply to all devices, irrespective of the domains that are assigned for this user.

Procedure

Step 1 Select **Monitor > Settings > Global Polling Configuration**.

Step 2 In the Polling Stats field, click **Enable**.

Step 3 From the Background Polling Interval field, select a polling interval.

Step 4 Click **OK** to save and apply the polling parameters.

Related Topics

- Enabling Polling on Specific Devices, page 14-21
- Disabling Polling on All Devices, page 14-22

Disabling Polling on All Devices

You can disable polling all devices as shown in the following steps.

Procedure

Step 1 Select **Monitor > Settings > Global Polling Configuration**.

Step 2 In the Polling Stats field, click **Disable**.

Step 3 Click **OK**. Polling is disabled.

Related Topics

- Enabling Polling on All Devices, page 14-21
- Enabling Polling on Specific Devices, page 14-21

Monitoring Events

The events captured in the Events table include both ACE syslog events and SNMP trap events. A procedure for viewing both types of events and details of information extracted from the syslog are shown below. Fields providing traffic-oriented sorting capability, specifically the information signified by the column heads in the Events Fields screen, shown in Table 14-13 (Source IP, Source Port, Destination IP, Destination Port, and Protocol) are only available for the ACE syslogs.

Note We do not recommend that you send a high volume of syslogs to ANM. ANM will only process and persist syslogs at 100 messages per second. Any additional syslogs sent to ANM beyond that rate will be discarded. To address this behavior, set the syslog severity level to a setting that is no higher than the warning level (a severity level of 4-Warning). See the "Configuring Virtual Context Syslog Settings" section on page 3-13 for details.

Assumptions

To receive events from devices, the devices must have syslog and SNMP traps configured correctly. See Configuring Virtual Context Syslog Settings, page 3-13 and Configuring SNMP for Virtual Contexts, page 3-20.

Procedure

Step 1 Select **Monitor > Events**. ANM displays all events received from ACE for Syslog and SNMP traps for all virtual contexts. See Table 14-13 for a description of the displayed information, which is extracted from the syslog.

You can sort information in the table by clicking on a column heading. This allows you to group events and help troubleshooting traffic information.

Table 14-13 Monitor > Events Fields

Field	Description
Syslog ID/SNMP ID	Displays the Syslog ID and SNMP ID. If the event is a trap, this field is empty.
Severity	Indicates the syslog severity level as described in Table 3-4.
Origination Time	Date and time that the event was last changed in the database.
Source IP	Displays the source name that is reporting the event, for example, *<chassis/slot>:virtual_context*.
Source Port	Displays the source port.
Destination IP	Displays the IP address of the destination if available.
Destination Port	Displays the destination port if available.
Protocol	Protocol used in the syslog.
Detail	Provides additional detail about the event.

Table 14-14 displays the complete list of published ACE syslogs where source and destination IP, ports and protocols are parsed so that the designated table fields populate.

Note *Only* the ACE syslog messages shown in this table will populate the Events screen fields explained in Table 14-13. Syslogs and traps not in this table will populate fields with a 0.

Table 14-14 ACE Syslogs Fields with Parseable Traffic Oriented Sorting Information

Syslog	Message Contents
ACE-1-106021	*Deny protocol reverse path check from source_address to dest_address on interface interface_name*
ACE-4-106023	*Deny protocol number | name src incoming-interface:src-ip dst outgoing-interface:dst-ip by access-group "acl-name" (hash 1, hash 2)*
ACE-6-302022	*Built TCP connection id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)*
ACE-6-302023	*Teardown TCP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [reason]*
ACE-6-302024	*Built UDP connection id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)*
ACE-6-302025	*Teardown UDP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes*
ACE-6-302026	*Built ICMP connection for faddr/NATed_ID gaddr/icmp_type laddr/icmpID*
ACE-6-302027	*Teardown ICMP connection for faddr/NATed ID gaddr/icmp_type laddr/icmpID*
ACE-6-302028	*Built TCP connection id for interface: real-address/real-port (mapped-address/mapped-port) to interface: real-address/real-port (mapped-address/mapped-port)*
ACE-6-302029	*Teardown TCP connection id for interface: real-address/real-port to interface: real-address/real-port duration hh:mm:ss bytes bytes [reason]*
ACE-6-302030	*Built UDP connection id for interface: real-address/real-port (mapped-address/mapped-port) to interface: real-address/real-port (mapped-address/mapped-port)*
ACE-6-302031	*Teardown UDP connection id for interface: real-address/real-port to interface: real-address/real-port duration hh:mm:ss bytes bytes*
ACE-4-313004	*Denied ICMP type=icmp_type, from source_address on interface interface_name to dest_address:no matching session*
ACE-4-410001	*Dropped UDP DNS packet_type from source_interface:source_address/source_port to dest_interface:dest_address/dest_port; error_length_type length length bytes exceeds max_length_type limit of maximum_length bytes.*

Related Topics

- Device Audit Trail Logging, page 14-25
- Monitoring Devices, page 14-4

Device Audit Trail Logging

Certain configuration and deployment changes will be logged in the ANM database, and available for viewing according to your role restricted by device VC as established by RBAC. Log files are located /var/lib/anm/events/*date*/audit, where *date* is in YYYYMMDD format (for example, 20081109 for November 9, 2008).

The following changes will be logged in ANM:

- configuration deployments to devices
- device or VC sync operations
- device or VC import and deletions
- creation/updates/deletion of the to-be-deployed later by the virtual server

Procedure

Step 1 Select **Config >** *device(s) to view* **> Device Audit**. ANM displays all operations described above on the specified devices. See Table 14-15 for a description of the displayed information, some of which is extracted from the syslog.

You can sort information in the table by clicking on a column heading, adjust the viewable time range using the pulldown menu, and export the table for reporting and troubleshooting purposes.

Table 14-15 Config > Device Audit Fields

Field	Description
Time	ANM server timestamp when the action is complete.
Client IP	Source IP address initiating action.
User	Email address in the following format: *username@organization name* for example, admin@cisco.com.
Device	Device or VC target of user action.
Action	The action name of the operation, including the following: • add staging object • allocate vlan • change credential • create • create vc • create vc-template • create-vip • delete • delete-vip • deploy staging object • disable polling • enable polling • export-certificate-key • generate-csr • import device • import-certificate-key • import module • remove device • remove vc • restart monitoring • syncup config • syslog-setup • unmanage module • update • update staging object • update-vip
Target	Name of the target configuration object (for example, Serverfarm sf1).

Table 14-15 Config > Device Audit Fields

Field	Description
Status	Indicates whether operation succeeded or not.
Detail	CLI commands sent to the device and/or error messages.[1]

1. If the detail column contains more than approximately 4KB of CLI commands, the data will appear truncated, and not display properly.

Related Topics

- Configuring Audit Log Settings, page 15-73
- Monitoring Devices, page 14-4
- Monitoring Events, page 14-22
- Viewing Change Audit Logs, page 15-74

Configuring Alarm Notifications

To set up Monitoring alarm notifications, you define a threshold group and specify the statistics to be monitored by ANM for the threshold group. When the value for a specific statistic rises above the setting you specify, an alarm is issued to alert you.

Note CISCO-EPM-NOTIFICAITON-MIB is used for ANM alarms notification.

You can specify how you are notified when thresholds are crossed:

- Alarm notification, which you view at **Monitor > Alarm Notifications > Alarms**
- E-mail notification
- Traps

Note Threshold crossing is detected via periodic polling. If a threshold is crossed *between* polling cycles, it is possible that ANM might not issue an alert if the condition recovers before the next polling cycle.

Note ANM performs certificate expiration computations every 24 hours. The computation begins each time ANM is started. Every subsequent computation occurs 24 hours thereafter.

Assumption

For e-mail notification, you have configured SMTP. See Configuring SMTP for E-mail Notifications, page 14-34 for more information.

Procedure

Step 1 Select **Monitor > Alarm Notifications > Threshold Groups**, then click **Add**.

Step 2 In the Properties section, enter the name and description for the threshold group.

Step 3 In the Threshold Settings section, click **Add** and then enter the following information shown in Table 14-16.

Table 14-16 Threshold Settings Fields

Field	Description
Device Type	Select the device type to include in the threshold group. *VC* indicates virtual context.
Category	Select a statistic to include in the threshold group. Table 14-17 identifies and describes the types of statistics available for each device type.
Assert on Value	Enter a value to define the threshold. When the statistic exceeds this value, an alarm is issued. Some values are displayed as percentages as indicated by the percent sign (%). In the case of SSL certificate expiration, assert on value indicates the number of days before certificate expiration. Alarms will be updated daily to indicate the number of days remaining until certificate expiration. If the email is configured, you will be sent email daily alerting you to the number of days left before expiration.
Clear Value	Enter a value on which to clear the alarm. In the case of SSL certificate expiration, the setting has no relevance. When an expired certificate is deleted, the alarm is removed from ANM on the subsequent certificate evaluation. This happens every 24 hours.
Notify on Clear	Check the Notify on Clear check box to receive E-mail notification to the specified address when the alarm is cleared.
Severity	Select a severity level for this threshold, which can be Critical, Info, Major, or Minor.

Table 14-17 Monitoring Thresholds by Device Type

Category	Threshold	Description
ACE 4710 Running Images A1(8) or A3(1.0)		
	ACL Memory	Percentage of memory allocated for ACLs.
	Bandwidth	Percentage of throughput.
	Concurrent Connections	Percentage of simultaneous connections.
	Current Application Acceleration Connections	Percentage of application acceleration connections.
	Current Connection Rate	Percentage of connections of any kind.
	Current HTTP Compression Rate	Percentage of compression for HTTP data.
	Inspect Connection Rate	Percentage of application protocol inspection connections.
	MAC Miss Rate	Percentage of messages destined for the ACE that are sent to the control plane when the encapsulation is not correct in packets.
	Management Connections	Percentage of management connections.
	Management Traffic Rate	Percentage of management traffic connections.
	Proxy Connections Rate	Percentage of proxy connections.
	Regular Expression Memory	Percentage of regular expression memory.
	SSL Connection Rate	Percentage of SSL connections.
	Syslog Buffer Size	Percentage of the syslog buffer.
	Syslog Message Rate	Percentage of syslog messages per second.
	Translation Entries	Percentage of network and port address translations.
ACE 4710 VC		
Application Acceleration	Condenser State	State of the condenser.
Interface	Interface Operational State	Operational state of the interface.
Real Server	Real Server Current Connections	Number of current connections on a real server.
	Real Server Operational State	Operational state of a real server.
SLB Stat	Layer 4 Policy Connections	Number of Layer 4 policy connections.
	Layer 7 Policy Connections	Number of Layer 7 policy connections.
SSL Certificate Management	SSL certificate expiration (in days)	Number of days left before SLL certificate expires whose value minus one will send a warning email with the specified severity. ANM updates this field daily.

Table 14-17 Monitoring Thresholds by Device Type

Category	Threshold	Description
ACE Module		
	ACL Memory	Percentage of memory allocated for ACLs.
	Bandwidth	Percentage of bandwidth.
	Concurrent Connections	Percentage of simultaneous connections.
	Current Connection Rate	Percentage of connections of any kind.
	Inspect Connection Rate	Percentage of application protocol inspection connections.
	MAC Miss Rate	Percentage of messages destined for the ACE that are sent to the control plane when the encapsulation is not correct in packets.
	Management Connections	Percentage of management connections.
	Management Traffic Rate	Percentage of management traffic connections.
	Proxy Connections Rate	Percentage of proxy connections.
	Regular Expression Memory	Percentage of regular expression memory.
	SSL Connection Rate	Percentage of SSL connections.
	Syslog Buffer Size	Percentage of the syslog buffer.
	Syslog Message Rate	Percentage of syslog messages per second.
	Throughput	Percentage of throughput.
	Translation Entries	Percentage of network and port address translations.
ACE VC		
Interface	Interface Operational State	Operational state of the interface.
Real Server	Real Server Current Connections	Number of current connections on a real server.
	Real Server Operational State	Operational state of a real server.
SLB Stat	Layer 4 Policy Connections	Number of Layer 4 policy connections.
	Layer 7 Policy Connections	Number of Layer 7 policy connections.
SSL Certificate Management	SSL certificate expiration (in days)	Number of days left before SLL certificate expires whose value minus one will send a warning email with the specified severity. ANM updates this field daily.
CSM Module		
Real Server	Real Server Connections	Number of real server connections.
	Real Server Current State	Operational state of a real server.
SLB Stat	Current Opened Connections	Number of open connections.
	Layer 4 Policy Connections	Number of Layer 4 policy connections.
	Layer 7 Policy Connections	Number of Layer 7 policy connections.
SLB Virtual Server	Virtual Server Connections	Number of virtual server connections.
	Virtual Server State	Operational state of a virtual server.
System	CSM Fault Tolerance State	Fault tolerance state of the CSM.

Table 14-17 Monitoring Thresholds by Device Type

Category	Threshold	Description
CSS		
Interface	Average TCP Packets	Average number of TCP packets.
	Interface Operational State	Operational state of the interface.
	Max TCP Packets	Maximum number of TCP packets.
Real Server	Active Service Connections	Number of active real server connections.
	Real Server State	State of a real server.
System	CSS Fault Tolerance State	Fault tolerance state of the CSS.
	CSS Module State	State of a CSS module.
Virtual Server	Virtual Server State	Current state of a virtual server.

Step 4 Click **OK**.

Step 5 In Device Selection, select the device type to include in the threshold group. The available devices appear in the Available Items field.

Note Make sure that the device type you select in this field is supported by the threshold that you selected in the Category field in Step 3. If the device type you select is not supported by the threshold you selected, you will not receive alarm notifications.

Step 6 Click on a device in the Available Items field, then the arrow (>) to move the device to the Selected Items field.

Step 7 In the Notify By section, in the E-mail field, enter the E-mail address you want to receive notification E-mail. See Viewing E-mail Notifications, page 14-33 for information contained in the E-mail notifications. If you do not select this field, you must view alarm notifications by selecting **Monitor > Alarm Notifications > Alarm**.

Note You must configure the required host parameters, IP address and port, to send e-mail notifications. See Configuring SMTP for E-mail Notifications, page 14-34.

Step 8 In the Traps field, enter the host IP Address and port number of the machine to which the traps are sent. See Viewing Traps, page 14-34 for information contained in the traps.

Step 9 Click:

- **Save** to save the threshold group settings.
- **Cancel** to cancel the threshold group settings and return to the Threshold Groups page.

Related Topics

- Configuring SMTP for E-mail Notifications, page 14-34
- Viewing Alarm Notifications, page 14-32

Viewing Alarm Notifications

After you configure alarm notifications (see Configuring Alarm Notifications, page 14-27), when the value for a specific statistic rises above the setting you specified, an alarm is issued to alert you.

Depending on how you specified to be notified when a threshold is crossed, you can view the alarms

- By selecting **Monitor > Alarm Notifications > Alarm**. See Viewing Alarms in ANM, page 14-32.
- By viewing an E-mail notification. See Viewing E-mail Notifications, page 14-33.
- By viewing traps. See Viewing Traps, page 14-34.

Note Threshold crossing is detected via periodic polling. If a threshold is crossed *between* polling cycles, it is possible that ANM might not issue an alert if the condition recovers before the next polling cycle.

Related Topics

- Configuring Alarm Notifications, page 14-27
- Viewing Alarms in ANM, page 14-32
- Viewing E-mail Notifications, page 14-33
- Viewing Traps, page 14-34

Viewing Alarms in ANM

After you configure alarm notifications (see Configuring Alarm Notifications, page 14-27), when the value for a specific statistic rises above the setting you specified, an alarm is issued to alert you.

You can view alarms issued by selecting **Monitor > Alarm Notifications > Alarms**. Alarms issued by ANM are displayed with the following information shown in Table 14-18.

Note If an alarm has been cleared, it does not appear on the **Monitor > Alarm Notifications > Alarms** page. This page displays active alarms only.

:

Table 14-18 ANM Alarm Notification Content

Field	Description
Source ID	ANM server IP address that issued the alarm
Severity	Specified severity level of the threshold, which can be one of the following: • Info • Critical • Major • Minor
Origination Time	Time the alarm was issued
Threshold Group	Specified threshold group name
Category	Alarm name

Table 14-18 ANM Alarm Notification Content

Field	Description
Component	Component name, for example, VLAN20
State/Value	Specified state or value of the alarm
Detail	Displays additional information about the alarm.
Notes	Allows you to add any notes to this alarm.

Related Topics

- Configuring SMTP for E-mail Notifications, page 14-34
- Configuring Alarm Notifications, page 14-27
- Viewing E-mail Notifications, page 14-33

Viewing E-mail Notifications

After you configure alarm notifications (see Configuring Alarm Notifications, page 14-27) and specify to receive notification E-mail, when the value for a specific statistic rises above the setting you specify, ACE Device Manager sends an E-mail to alert you.

Table 14-19 describes the information contained in the E-mail alarm notification.

Table 14-19 E-mail Alarm Notification Content

Field	Description
ANM Server Host Name	ANM server host name
ANM Server IP Address	ANM server IP address
Device ID	Device name
Component Name	Component name, for example, VLAN20
Severity	Specified severity level of the threshold, which can be one of the following: • Info • Critical • Major • Minor
Time	Time the alarm was issued
Alarm Name	Specified name of the alarm
Alarm Value	Specified value of the alarm
Threshold Assert Value	Specified value on when to issue the alarm
Threshold Group Name	Specified threshold group name
Alarm State	State of the alarm which can be one of the following: • Active • Clear

Related Topics

- Configuring Alarm Notifications, page 14-27
- Viewing Alarm Notifications, page 14-32

Viewing Traps

After you configure alarm notifications (see Configuring Alarm Notifications, page 14-27) and specify to send traps to a trap receiver, when the value for a specific statistic rises above the setting you specify, ANM issues a trap to alert you.

Related Topics

- Configuring Alarm Notifications, page 14-27
- Viewing Alarm Notifications, page 14-32

Configuring SMTP for E-mail Notifications

You can specify that e-mail notifications be sent each time a monitoring threshold is crossed.

Note You must configure your SMTP server in order to receive e-mail notifications.

Assumption

You have configured threshold crossing alerts. See Configuring Alarm Notifications, page 14-27 for more information.

Procedure

Step 1 Select **Monitor > Settings > SMTP Configuration**.

Step 2 In the SMTP Server to Send E-mail Notifications field, enter your SMTP server.

Step 3 Click **Deploy Now** to apply the SMTP configuration.

Related Topics

- Monitoring Events, page 14-22
- Configuring Alarm Notifications, page 14-27
- Viewing E-mail Notifications, page 14-33

Testing Connectivity

Use the following steps to verify the connectivity (using the ping command) between ANM and the IP address you specify.

Note The Ping feature is disabled if you have not imported any devices into the ANM server.

Procedure

Step 1 Select **Monitor > Tools > Ping.**

Step 2 From the object selector field, select the device you want to test.

Step 3 Enter the information shown in Table 14-20.

Table 14-20 Ping Fields

Field	Description
IP Address	Enter the IP address of the real server to which you want to ping.
Elapsed Time	Elapsed time before the ping request is declared a failure.
Repeat	Enter how many times to repeat the test.
Datagram Size	Enter a value for the argument size (size of the packet) of the ping command.

Step 4 Click **Start** to run the connectivity test.

Step 5 After the test completes, the results are displayed. Click:

- **New** to enter new parameters and create a new ping test.
- **Restart** to rerun the connectivity test.

Related Topic

Setting Up Devices for Monitoring, page 14-2