CHAPTER 34

Third-Party Integration

Fabric Manager provides tools to facilitate integration with third-party applications and devices. This chapter contains the following sections:

Call Home Configuration

The actual configuration of Call Home depends on how you intend to use the feature. Some points to consider include:

- An e-mail server and at least one destination profile (predefined or user-defined) must be configured. The destination profile(s) used depends on whether the receiving entity is a pager, e-mail, or automated service such as Cisco AutoNotify.
- The contact name (SNMP server contact), phone, and street address information must be configured before Call Home is enabled. This is required to determine the origin of messages received.
- The Cisco MDS 9000 switch must have IP connectivity to an e-mail server.
- You must obtain an active service contract to use Cisco AutoNotify.

Cisco AutoNotify

If you have service contracts directly with Cisco Systems, automatic case generation with the Technical Assistance Center is possible by registering with the AutoNotify service. AutoNotify provides fast time to resolution of system problems by providing a direct notification path to Cisco customer support.

The AutoNotify feature requires several Call Home parameters to be configured, including certain contact information, e-mail server, and an XML destination profile as specified in the Service Activation document found on the Cisco.com website at:
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_3/service/serv332/ccmsrvs/sssrvact.htm

To configure a Cisco MDS 9000 Family switch to use the AutoNotify service, an XML destination profile must be configured to send messages to Cisco. Specific setup, activation, and e-mail address information is found on the Cisco.com website at:
http://www.cisco.com/warp/customer/cc/serv/mkt/sup/tsssv/opmsup/smton/anoti_ds.htm

To register, the following items are required:

- The SMARTnet contract number covering your Cisco MDS 9000 Family switch.
- Your name, company address, e-mail address, and Cisco.com ID.
- The exact product number of your Cisco MDS 9000 Family switch. For example, some valid product numbers include: DS-C6509 and DS-C9216-K9.
- The serial number of your Cisco MDS 9000 Family switch. This can be obtained by looking at the serial number label on the back of the switch (next to the power supply).

The ContractID, CustomerID, SiteID, and SwitchPriority parameters are not required by the AutoNotify feature. They are only intended to be used as additional information by Cisco customers and service partners.

Configuring Call Home

To configure Call Home, follow these steps:

Step 1 Expand the **Switches** folder in the Physical Attributes pane on Fabric Manager and choose **Events > Call Home**. You see the Call Home dialog box in the Information pane.

Or, choose **Admin > Events > Call Home** on Device Manager.

Step 2 Click the **General** tab to assign contact information and enable the Call Home feature. The Call Home feature is not enabled by default, and you must enter an e-mail address that identifies the source of Call Home notifications.

Step 3 Click the **Destinations** tab to configure the destination e-mail addresses for Call Home notifications. You can identify one or more e-mail addresses that will receive Call Home notifications.

Step 4 Click the **E-mail Setup** tab to identify the SMTP server. You need to identify a message server to which your switch has access. This message server will forward the Call Home notifications to the destinations.

Configuring Call Home Destination Profiles and Alert Groups

A destination profile contains the required delivery information for an alert notification. Destination profiles are typically configured by the network administrator. At least one destination profile is required. You can configure multiple destination profiles of one or more types.

Note If you use the Cisco AutoNotify service, the XML destination profile is required (see http://www.cisco.com/warp/public/cc/serv/mkt/sup/tsssv/opmsup/smton/anoti_ds.htm).

A destination profile consists of the following:

- Profile name—A string that uniquely identifies each user-defined destination profile and is limited to 32 alphanumeric characters. The format options for a user-defined destination profile are full-txt, short-txt, or XML (default).
- Destination address—The actual address, pertinent to the transport mechanism, to which the alert should be sent.
- Message formatting—The message format used for sending the alert (full text, short text, or XML).

- Message severity—Severity of messages that will trigger a Call Home message. Messages below this severity do not trigger Call Home messages.
- Alert group— A predefined subset of Call Home alerts supported in all switches in the Cisco MDS 9000 Family

Different types of Call Home alerts are grouped into different alert groups depending on their type. You can associate one or more alert groups to each profile as required by your network.

To configure Call Home profiles from the Fabric Manager, follow these steps:

Step 1 Choose **Switches > Events > Call Home** from the Physical Attributes tree and click the **Profiles** tab in the Information pane.You see Call Home profiles for multiple switches.

Step 2 Click the **Create Row** icon to add a new profile.

Step 3 Set the profile name, message format, size, and severity level.

Step 4 Check the check boxes for each alert group you want sent in this profile.

Step 5 Click **Create** to create this profile on the selected switches.

Call Home Message Severity Levels

You can filter Call Home messages based on their level of urgency. Each destination profile (predefined and user-defined) is associated with a Call Home message level threshold. Any message with a value lower than the urgency threshold is not sent. The urgency level ranges from debug (lowest level of urgency) to catastrophic (highest level of urgency), and the default is debug (all messages are sent).

Note Call Home severity levels are not the same as system message logging severity levels.

To set the message level for each profile for Call Home, follow these steps:

Step 1 Expand the **Switches** folder in the Physical Attributes pane on Fabric Manager and choose **Events > Call Home**. You see the Call Home dialog box in the Information pane.

Or, choose **Admin > Events > Call Home** on Device Manager.

Step 2 Click the **Profiles** tab and set the message level for each switch using the drop-down menu in the **MsgLevel** column.

Step 3 Click **Apply Changes** to save your changes or click **Undo Changes** to cancel your changes.

Event Triggers

This section discusses Call Home trigger events. Trigger events are divided into categories, with each category assigned commands to execute when the event occurs. The command output is included in the transmitted message. Table 34-1 lists the trigger events.

Table 34-1 Event Triggers

Event	Alert Group	Event Name	Description	Severity Level
Call Home	System and CISCO_TAC	SW_CRASH	A software process has crashed with a stateless restart, indicating an interruption of a service.	major
	System and CISCO_TAC	SW_SYSTEM_INCONSISTENT	Inconsistency detected in software or file system.	major
	Environmental and CISCO_TAC	TEMPERATURE_ALARM	Thermal sensor indicates temperature reached operating threshold.	critical
		POWER_SUPPLY_FAILURE	Power supply failed.	critical
		FAN_FAILURE	Cooling fan has failed.	major
	Switching module and CISCO_TAC	LINECARD_FAILURE	Switching module operation failed.	fatal
		POWER_UP_DIAGNOSTICS_FAILURE	Switching module failed power-up diagnostics.	fatal
	Line Card Hardware and CISCO_TAC	PORT_FAILURE	Hardware failure of interface port(s).	critical
	Line Card Hardware, Supervisor Hardware, and CISCO_TAC	BOOTFLASH_FAILURE	Failure of boot compact Flash card.	critical
	Supervisor module and CISCO_TAC	SUP_FAILURE	Supervisor module operation failed.	fatal
		POWER_UP_DIAGNOSTICS_FAILURE	Supervisor module failed power-up diagnostics.	fatal
Call Home	Supervisor Hardware and CISCO_TAC	INBAND_FAILURE	Failure of in-band communications path.	fatal
	Supervisor Hardware and CISCO_TAC	EOBC_FAILURE	Ethernet out-of-band channel communications failure.	critical
	Supervisor Hardware and CISCO_TAC	MGMT_PORT_FAILURE	Hardware failure of management Ethernet port.	major
	License	LICENSE_VIOLATION	Feature in use is not licensed (Cisco MDS SAN-OS Release 1.3.x), and is turned off after grace period expiration.	critical

Table 34-1 Event Triggers (continued)

Event	Alert Group	Event Name	Description	Severity Level
Inventory	Inventory and CISCO_TAC	COLD_BOOT	Switch is powered up and reset to a cold boot sequence.	notification
		HARDWARE_INSERTION	New piece of hardware inserted into the chassis.	notification
		HARDWARE_REMOVAL	Hardware removed from the chassis.	notification
Test	Test and CISCO_TAC	TEST	User generated test.	notification

Message Contents

The following contact information can be configured on the switch:

- Name of the contact person
- Phone number of the contact person
- E-mail address of the contact person
- Mailing address to which replacement parts must be shipped, if required
- Site ID of the network where the site is deployed
- Contract ID to identify the service contract of the customer with the service provider

Table 34-2 describes the short text formatting option for all message types.

Table 34-2 Short Text Messages

Data Item	Description
Device identification	Configured device name
Date/time stamp	Time stamp of the triggering event
Error isolation message	Plain English description of triggering event
Alarm urgency level	Error level such as that applied to system message

Table 34-3, Table 34-4, and Table 34-5 display the information contained in plain text and XML messages.

Table 34-3 Reactive Event Message Format

Data Item (Plain text and XML)	Description (Plain text and XML)	XML Tag (XML only)
Time stamp	Date and time stamp of event in ISO time notation: *YYYY-MM-DD*T*HH:MM:SS*. **Note** The time zone or daylight savings time (DST) offset from UTC has already been added or subtracted. T is the hardcoded limiter for the time.	/mml/header/time
Message name	Name of message.	/mml/header/name
Message type	Specifically “Call Home.”	/mml/header/type
Message group	Specifically “reactive.”	/mml/header/group
Severity level	Severity level of message.	/mml/header/level
Source ID	Product type for routing.	/mml/header/source
Device ID	Unique device identifier (UDI) for end device generating message. This field should empty if the message is non-specific to a fabric switch. Format: type@Sid@serial, where • Type is the product model number from backplane SEEPROM. • @ is a separator character. • Sid is “C” identifying serial ID as a chassis serial number. • Serial number as identified by the Sid field. Example: “DS-C9000@C@12345678	/mml/ header/deviceId
Customer ID	Optional user-configurable field used for contract info or other ID by any support service.	/mml/ header/customerID
Contract ID	Optional user-configurable field used for contract info or other ID by any support service.	/mml/ header /contractId
Site ID	Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service.	/mml/ header/siteId
Server ID	If the message is generated from the fabric switch, it is the unique device identifier (UDI) of the switch. Format: type@Sid@serial, where • Type is the product model number from backplane SEEPROM. • @ is a separator character. • Sid is “C” identifying serial ID as a chassis serial number. • Serial number as identified by the Sid field. Example: “DS-C9000@C@12345678	/mml/header/serverId
Message description	Short text describing the error.	/mml/body/msgDesc
Device name	Node that experienced the event. This is the host name of the device.	/mml/body/sysName
Contact name	Name of person to contact for issues associated with the node experiencing the event.	/mml/body/sysContact

Table 34-3 Reactive Event Message Format (continued)

Data Item (Plain text and XML)	Description (Plain text and XML)	XML Tag (XML only)
Contact e-mail	E-mail address of person identified as contact for this unit.	/mml/body/sysContactEmail
Contact phone number	Phone number of the person identified as the contact for this unit.	/mml/body/sysContactPhone Number
Street address	Optional field containing street address for RMA part shipments associated with this unit.	/mml/body/sysStreetAddress
Model name	Model name of the switch. This is the specific model as part of a product family name.	/mml/body/chassis/name
Serial number	Chassis serial number of the unit.	/mml/body/chassis/serialNo
Chassis part number	Top assembly number of the chassis.	/mml/body/chassis/partNo
Chassis hardware version	Hardware version of chassis.	/mml/body/chassis/hwVersion
Supervisor module software version	Top level software version.	/mml/body/chassis/swVersion
Affected FRU name	Name of the affected FRU generating the event message.	/mml/body/fru/name
Affected FRU serial number	Serial number of affected FRU.	/mml/body/fru/serialNo
Affected FRU part number	Part number of affected FRU.	/mml/body/fru/partNo
FRU slot	Slot number of FRU generating the event message.	/mml/body/fru/slot
FRU hardware version	Hardware version of affected FRU.	/mml/body/fru/hwVersion
FRU software version	Software version(s) running on affected FRU.	/mml/body/fru/swVersion
Command output name	The exact name of the issued command.	/mml/attachments/attachment/ name
Attachment type	Specifically command output.	/mml/attachments/attachment/ type
MIME type	Normally text or plain or encoding type.	/mml/attachments/attachment/ mime
Command output text	Output of command automatically executed.	/mml/attachments/attachment/ atdata

Table 34-4 Inventory Event Message Format

Data Item (Plain text and XML)	Description (Plain text and XML)	XML Tag (XML only)
Time stamp	Date and time stamp of event in ISO time notation: *YYYY-MM-DD*T*HH:MM:SS*. **Note** The time zone or daylight savings time (DST) offset from UTC has already been added or subtracted. T is the hardcoded limiter for the time.	/mml/header/time
Message name	Name of message. Specifically “Inventory Update.”	/mml/header/name
Message type	Specifically “Inventory Update.”	/mml/header/type
Message group	Specifically “proactive.”	/mml/header/group
Severity level	Severity level of inventory event is level 2.	/mml/header/level
Source ID	Product type for routing at Cisco. Specifically “MDS 9000.”	/mml/header/source
Device ID	Unique Device Identifier (UDI) for end device generating message. This field should empty if the message is non-specific to a fabric switch. Format: type@Sid@serial, where • Type is the product model number from backplane SEEPROM. • @ is a separator character. • Sid is “C” identifying serial ID as a chassis serial number. • Serial: The serial number as identified by the Sid field. Example: “DS-C9000@C@12345678	/mml/ header /deviceId
Customer ID	Optional user-configurable field used for contact info or other ID by any support service.	/mml/ header /customerID
Contract ID	Optional user-configurable field used for contact info or other ID by any support service.	/mml/ header /contractId
Site ID	Optional user-configurable field, used for Cisco-supplied site ID or other data meaningful to alternate support service.	/mml/ header /siteId
Server ID	If the message is generated from the fabric switch, it is the Unique device identifier (UDI) of the switch. Format: type@Sid@serial, where • Type is the product model number from backplane SEEPROM. • @ is a separator character. • Sid is “C” identifying serial ID as a chassis serial number. • Serial: The serial number as identified by the Sid field. Example: “DS-C9000@C@12345678	/mml/header/serverId
Message description	Short text describing the error.	/mml/body/msgDesc
Device name	Node that experienced the event.	/mml/body/sysName
Contact name	Name of person to contact for issues associated with the node experiencing the event.	/mml/body/sysContact
Contact e-mail	E-mail address of person identified as contact for this unit.	/mml/body/sysContactEmail

Table 34-4 Inventory Event Message Format (continued)

Data Item (Plain text and XML)	Description (Plain text and XML)	XML Tag (XML only)
Contact phone number	Phone number of the person identified as the contact for this unit.	/mml/body/sysContactPhoneNumber
Street address	Optional field containing street address for RMA part shipments associated with this unit.	/mml/body/sysStreetAddress
Model name	Model name of the unit. This is the specific model as part of a product family name.	/mml/body/chassis/name
Serial number	Chassis serial number of the unit.	/mml/body/chassis/serialNo
Chassis part number	Top assembly number of the chassis.	/mml/body/chassis/partNo
Chassis hardware version	Hardware version of chassis.	/mml/body/chassis/hwVersion
Supervisor module software version	Top level software version.	/mml/body/chassis/swVersion
FRU name	Name of the affected FRU generating the event message.	/mml/body/fru/name
FRU s/n	Serial number of FRU.	/mml/body/fru/serialNo
FRU part number	Part number of FRU.	/mml/body/fru/partNo
FRU slot	Slot number of FRU.	/mml/body/fru/slot
FRU hardware version	Hardware version of FRU.	/mml/body/fru/hwVersion
FRU software version	Software version(s) running on FRU.	/mml/body/fru/swVersion
Command output name	The exact name of the issued command.	/mml/attachments/attachment/name
Attachment type	Specifically command output.	/mml/attachments/attachment/type
MIME type	Normally text or plain or encoding type.	/mml/attachments/attachment/mime
Command output text	Output of command automatically executed after event categories (see).	/mml/attachments/attachment/atdata

Table 34-5 User-Generated Test Message Format

Data Item (Plain text and XML)	Description (Plain text and XML)	XML Tag (XML only)
Time stamp	Date and time stamp of event in ISO time notation: *YYYY-MM-DD*T*HH:MM:SS*. **Note** The time zone or daylight savings time (DST) offset from UTC has already been added or subtracted. T is the hardcoded limiter for the time.	/mml/header/time
Message name	Name of message. Specifically test message for test type message.	/mml/header/name
Message type	Specifically “Test Call Home.”	/mml/header/type

Table 34-5 User-Generated Test Message Format (continued)

Data Item (Plain text and XML)	Description (Plain text and XML)	XML Tag (XML only)
Message group	This field should be ignored by the receiving Call Home processing application, but may be populated with either "proactive" or "reactive."	/mml/header/group
Severity level	Severity level of message, test Call Home message.	/mml/header/level
Source ID	Product type for routing.	/mml/header/source
Device ID	Unique device identifier (UDI) for end device generating message. This field should empty if the message is non-specific to a fabric switch. Format: type@Sid@serial, where • Type is the product model number from backplane SEEPROM. • @ is a separator character. • Sid is "C" identifying serial ID as a chassis serial number. • Serial: The serial number as identified by the Sid field. Example: "DS-C9000@C@12345678	/mml/ header /deviceId
Customer ID	Optional user-configurable field used for contract info or other ID by any support service.	/mml/ header /customerId
Contract ID	Optional user-configurable field used for contract info or other ID by any support service.	/mml/ header /contractId
Site ID	Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service.	/mml/ header /siteId
Server ID	If the message is generated from the fabric switch, it is the Unique device identifier (UDI) of the switch. Format: type@Sid@serial, where • Type is the product model number from backplane SEEPROM. • @ is a separator character. • Sid is "C" identifying serial ID as a chassis serial number. • Serial: The serial number as identified by the Sid field. Example: "DS-C9000@C@12345678	/mml/header/serverId
Message description	Short text describing the error.	/mml/body/msgDesc
Device name	Switch that experienced the event.	/mml/body/sysName
Contact name	Name of person to contact for issues associated with the node experiencing the event.	/mml/body/sysContact
Contact e-mail	E-mail address of person identified as contact for this unit.	/mml/body/sysContactEmail
Contact phone number	Phone number of the person identified as the contact for this unit.	/mml/body/sysContactPhoneNumber
Street address	Optional field containing street address for RMA part shipments associated with this unit.	/mml/body/sysStreetAddress
Model name	Model name of the switch. This is the specific model as part of a product family name.	/mml/body/chassis/name
Serial number	Chassis serial number of the unit.	/mml/body/chassis/serialNo

Table 34-5 User-Generated Test Message Format (continued)

Data Item (Plain text and XML)	Description (Plain text and XML)	XML Tag (XML only)
Chassis part number	Top assembly number of the chassis. For example, 800-xxx-xxxx.	/mml/body/chassis/partNo
Command output text	Output of command automatically executed after event categories listed in .	/mml/attachments/attachment/atdata
MIME type	Normally text or plain or encoding type.	/mml/attachments/attachment/mime
Attachment type	Specifically command output.	/mml/attachments/attachment/type
Command output name	The exact name of the issued command.	/mml/attachments/attachment/name

Configuring SNMP Events

SNMP events are asynchronous notifications of status, performance, or configuration changes on the monitored switch. These events can be either traps or informs. Traps are unacknowledged, while informs use TCP to tell the sending switch that the event was received at the configured destination. The switch will retry an inform after the configured timeout period if the SNMP event destination does not return an acknowledgement of the SNMP event. Fabric Manager or Device Manager can enable or disable individual SNMP events for each switch to provide customized notifications.

Filtering SNMP Events

SNMP events cover a broad spectrum of features on the Cisco MDS 9000 Family switches. As an administrator, you may find some events are more important to your fabric management than others. Fabric Manager and Device Manager let you enable or disable individual SNMP events so that you only receive the SNMP events you are interested in at your SNMP event destinations.

To filter individual SNMP events, follow these steps:

Step 1 On Fabric Manager, choose **Switches > Events > SNMP Traps** and then click the **FC** or **Other** tab in the Information pane.

On Device Manager, choose **Admin > Events > Filters**.

Step 2 Check the check boxes for the SNMP events you want sent to your SNMP event destinations.

Step 3 Click **Apply Changes** on Fabric Manager, or **Create** on Device Manager to save and apply your changes.

Configuring SNMP Event Destinations

Cisco MDS 9000 Family switches, like other SNMP-enabled devices, send events (traps and informs) to configured destinations, called *trap receivers* in SNMPv2.

To configure SNMP event destinations, follow these steps:

Step 1 On Fabric Manager, choose **Switches > Events > SNMP Traps** and then click the **Destinations** tab in the Information pane.

On Device Manager, choose **Admin > Events > Destinations** and then click the **Addresses** tab in the SNMP dialog box.

Step 2 Click **Create Row** on Fabric Manager, or click **Create** on Device Manager to add a new SNMP event destination (that is, an SNMP trap receiver).

Step 3 Enter the IP address and port in dotted decimal notation (for example, 192.168.2.12/161) for the SNMP event destination in the **Address/Port** field.

Step 4 Choose the SNMP protocol level from the **Security** drop-down menu.

Step 5 Choose the SNMP event type (trap or informs). If you choose informs, set the timeout period and number of retries.

Step 6 Click **Create** to save and apply your changes.

Configuring Event Security

Caution This is an advanced function that should only be used by administrators having experience with SNMPv3.

SNMP events can be secured against interception or eavesdropping in the same way that SNMP messages are secured. Fabric Manager or Device Manager allow you to configure the message processing model, the security model, and the security level for the SNMP events that the switch generates.

To configure SNMP event security, follow these steps:

Step 1 On Fabric Manager, choose **Switches > Events > SNMP Traps** and then click the **Security** tab in the Information pane.

On Device Manager, choose **Admin > Events > Destinations** on Device Manager and then click the **Security (Advanced)** tab in the SNMP dialog box.

Step 2 Set the message protocol model, security model, security name, and security level.

Step 3 Click **Apply Changes** on Fabric Manager, or click **Create** on Device Manager to save and apply your changes.

Viewing the SNMP Events Log

To view the SNMP events log from the Device Manager, choose **Logs > Events > Current** or **Logs > Events > Older**. You see the Events Log dialog box with a log of events for a single switch.

Note The MDS syslog manager must be set up before you can view the event logs.

Caution Changing these values from different Fabric Manager workstations at the same time may cause unpredictable results.

Configuring RMON Using Threshold Manager

The RMON-MIB, as defined by the Internet Engineering Task Force (IETF), provides the Alarm, Log, and Events groups for monitoring appropriate statistics on the switch. The Threshold Manager in the Device Manager uses RMON in the switch to provide threshold monitoring for select statistics.

The Threshold Monitor allows you to trigger an SNMP event or log a message when the selected statistic goes over a configured threshold value. RMON calls this a rising alarm threshold. The configurable settings are:

- Variable—The statistic you want to set the threshold value on.
- Value—The value of the variable that you want the alarm to trigger at. This value is the difference (delta) between two consecutive polls of the variable by Device Manager.
- Sample—The sample period (in seconds) between two consecutive polls of the variable. Select your sample period such that the variable would not cross the threshold value you set under normal operating conditions.
- Warning—The warning level used by Device Manager to indicate the severity of the triggered alarm. This is a Fabric Manager and Device Manager enhancement to RMON.

Note To configure any type of RMON alarm (absolute or delta, rising or falling threshold) click **More** on the Threshold Manager dialog box. You should be familiar with how RMON defines these concepts before configuring these advanced alarm types. Refer to the RMON-MIB (RFC 2819) for information on how to configure RMON alarms.

Enabling RMON Alarms by Port

To configure an RMON alarm for one or more ports from the Device Manager, follow these steps:

Step 1 Choose **Admin > Events > Threshold Manager** and click the **FC Interfaces** tab.

Step 2 Click the **Selected** radio button to select individual ports for this threshold alarm.

a. Click **...** to the right of the Selected field to display all ports.

b. Choose the ports you want to monitor.

c. Click **OK** to accept the selection.

Alternatively, click the appropriate radio button to choose ports by type: **All** ports, **xE** ports, or **Fx** ports.

Step 3 Check the check box for each variable that you want to monitor.

Step 4 Enter the threshold value in the Value column.

Step 5 Enter the sampling period in seconds. This is the time between each snapshot of the variable.

Step 6 Choose one of the following severity levels to assign to the alarm: Fatal, Warning, Critical, Error, Information.

Step 7 Click **Create**.

Step 8 Confirm the operation to define an alarm and a log event when the system prompts you to define a severity event.If you do not confirm the operation, the system only defines a log event.

Step 9 Choose **More > Alarms** from the Threshold Manager dialog box to verify the alarm you created.

Enabling RMON Alarms for VSANs

To enable an RMON alarm for one or more VSANs from the Device Manager, follow these steps:

Step 1 Choose **Admin > Events > Threshold Manager** and click the **Services** tab.

You see the Threshold Manager dialog box with the Services tab selected.

Step 2 Enter one or more VSANs (multiple VSANs separated by commas) to monitor in the VSAN ID(s) field.

Step 3 Check the check box for each variable that you want to monitor.

Step 4 Enter the threshold value in the Value column.

Step 5 Enter the sampling period in seconds.

Step 6 Choose a severity level to assign to the alarm.

Step 7 Click **Create**.

Step 8 Confirm the operation to define an alarm and a log event when the system prompts you to define a severity event.

If you do not confirm the operation, the system only defines a log event.

Step 9 Choose **More > Alarms** from the Threshold Manager dialog box to verify the alarm you created.

Enabling RMON Alarms for Physical Components

To configure an RMON alarm for a physical component from the Device Manager, follow these steps:

Step 1 Choose **Admin > Events > Threshold Manager** and click the **Physical** tab.

You see the Threshold Manager dialog box with the Physical tab selected.

Step 2 Check the check box for each variable that you want to monitor.

Step 3 Enter the threshold value in the Value column.

Step 4 Enter the sampling period in seconds.

Step 5 Choose one of the following severity levels to assign to the alarm: Fatal, Warning, Critical, Error, Information.

Step 6 Click **Create**.

Step 7 Confirm the operation to define an alarm and a log event when the system prompts you to define a severity event.

If you do not confirm the operation, the system only defines a log event.

Step 8 Choose **More > Alarms** from the Threshold Manager dialog box to verify the alarm you created.

Managing RMON Events

To define customized RMON events from the Device Manager, follow these steps:

Step 1 Choose **Admin > Events > Threshold Manager** and click **More** on the Threshold Manager dialog box.

Step 2 Click the **Events** tab on the RMON Thresholds dialog box.

You see the RMON Events dialog box.

Step 3 Click **Create** to create a new event entry.

You see the Create Threshold Event Entry dialog box.

Step 4 Configure the RMON threshold event attributes by choosing the type of event (log, snmptrap, or logandtrap).

Step 5 Click **Create**.

Managing RMON Alarms

To view the alarms that have already been enabled from the Device Manager, follow these steps:

Step 1 Choose **Admin > Events > Threshold Manager** and click **More** on the Threshold Manager dialog box.

Step 2 Click the **Alarms** tab.

You see the RMON Alarms dialog box.

Step 3 Click **Create** to create a customized threshold entry.

You see the Create RMON Alarms dialog box.

Viewing the RMON Log

To view the RMON log from the Device Manager, follow these steps:

Step 1 Choose **Admin > Events > Threshold Manager** and click **More** on the Threshold Manager dialog box.

Step 2 Click the **Log** tab on the RMON Thresholds dialog box.

You see the RMON Log dialog box. This is the log of RMON events that have been triggered by the Threshold Manager.