Operations Center

Event Manager Guide

September 2016

Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Contents

About This Guide

The *Event Manager Guide* provides instructions for administering the Event Manager adapters.

Audience

This guide is intended for system administrators who are responsible for setting up and administering the Event Manager within the Operations Center environment. It is assumed that you are familiar with Operations Center and its user interface.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the *User Comments* feature at the bottom of each page of the online documentation.

Additional Documentation & Documentation Updates

This guide is part of the Operations Center documentation set. For the most recent version of the *Event Manager Guide* and a complete list of publications supporting Operations Center, visit our Online Documentation Web Site at Operations Center online documentation.

The Operations Center documentation set is also available as PDF files on the installation CD or ISO; and is delivered as part of the online help accessible from multiple locations in Operations Center depending on the product component.

Additional Resources

We encourage you to use the following additional resources on the Web:

- NetIQ User Community (https://www.netiq.com/communities/): A Web-based community with a variety of discussion topics.

- NetIQ Support Knowledgebase (https://www.netiq.com/support/kb/?product%5B%5D=Operations_Center): A collection of in-depth technical articles.
- NetIQ Support Forums (https://forums.netiq.com/forumdisplay.php?26-Operations-Center): A Web location where product users can discuss NetIQ product functionality and advice with other product users.

Technical Support

You can learn more about the policies and procedures of NetIQ Technical Support by accessing its Technical Support Guide (https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and).

Use these resources for support specific to Operations Center:

- Telephone in Canada and the United States: 1-800-858-4000
- Telephone outside the United States: 1-801-861-4000
- E-mail: support@netiq.com (support@netiq.com)
- Submit a Service Request: http://support.novell.com/contact/ (http://support.novell.com/contact/)

Documentation Conventions

A greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path. The > symbol is also used to connect consecutive links in an element tree structure where you can either click a plus symbol (+) or double-click each element to expand them.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a forward slash to preserve case considerations in the UNIX* or Linux* operating systems.

A trademark symbol (®, ™, etc.) denotes a NetIQ trademark. An asterisk (*) denotes a third-party trademark.

1 Introduction

Operations Center Event Manager™ gathers and processes alarms and informational messages from different sources to produce events and alarms derived from customized rule sets. You can create custom rule sets directly in the Event Manager.

This guide explains how to configure and manage the Event Manager, which is an add-on to Operations Center, and how to create and manage rulesets using the Operations Center Event Manager Ruleset Editor (known simply as the Ruleset Editor). It also describes the product architecture and explains the many features the Event Manager has to offer, as well as the purpose and structure of rulesets and using the Ruleset Editor.

The Event Manager processes alarms in accordance with rulesets, which are sets of instructions that describe how to parse and extract useful information from events. Define rulesets directly in the Event Manager through the Event Manager Ruleset Editor. Alternatively, define rulesets outside the Event Manager and import them into the Event Manager.

For example, the thresholding facility within the rules definition language enables creating a rule that generates a derived alarm only when all of the following occur:

- Processing of five derived events of the same type
- All five events originate from the same source
- Processing of all five events within a specified number of minutes

Derived alarms are informational messages that refer to the changing operational conditions of elements. Standard information contained in each alarm includes its severity, priority, affected element, the time at which the alarm occurred, a text message and a unique identification (ID) number for that alarm.

In addition, depending on the alarm’s source, each alarm can contain a varying set of additional information, such as a text message, a class of service, and other information that can help the user identify the source and nature of the problem represented by the derived alarm.

Event Manager Rule sets are compatible with BMC™ Software MAX/Enterprise™ Rule sets.

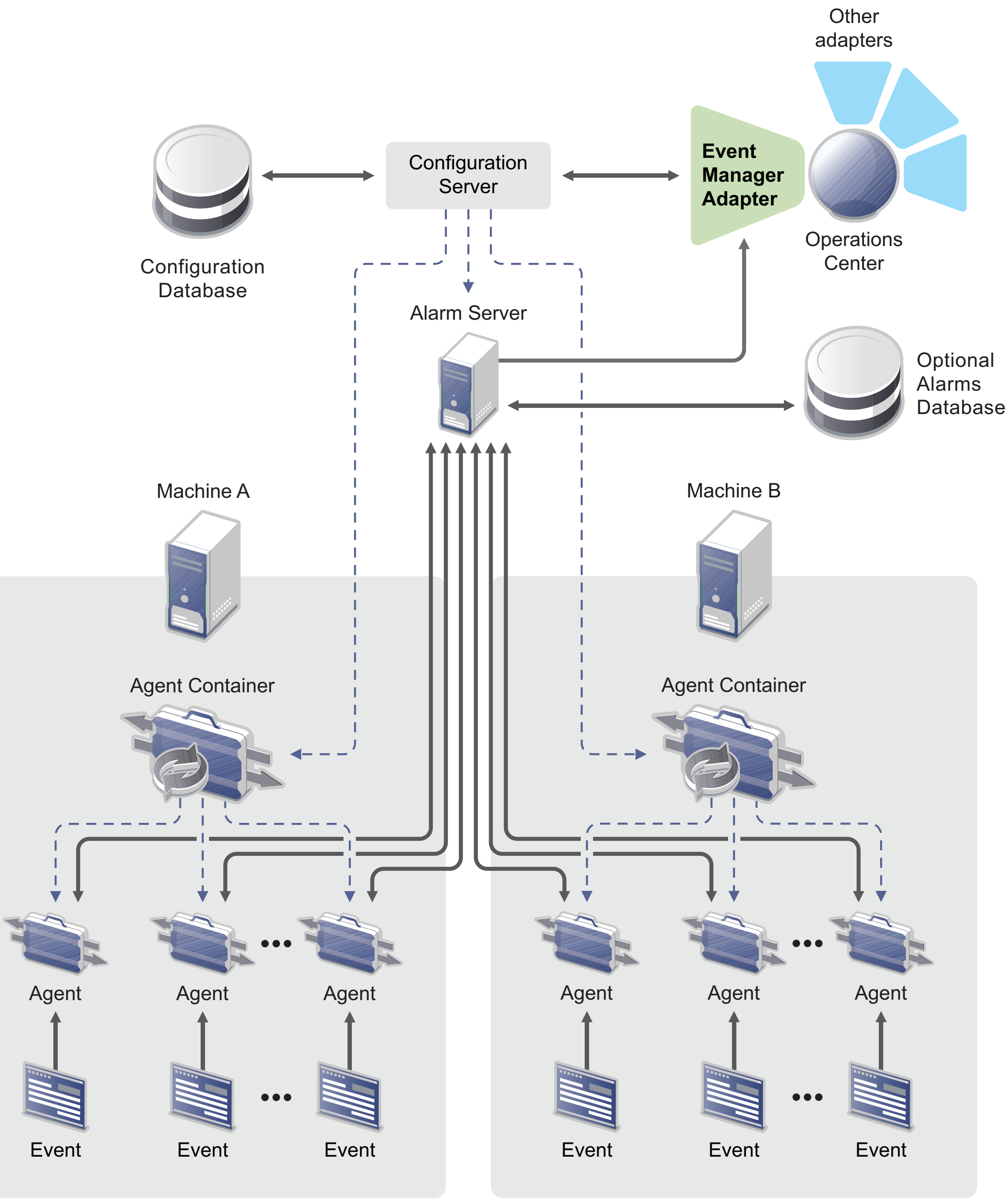
2 Examining the Architecture

The Event Manager works in conjunction with Operations Center to process and gather line-oriented ASCII data from a wide variety of sources. From this raw data, Event Manager can generate derived events and alarms. Alarms are lines of text that refer to the changing operational conditions of elements. Basic information contained in each alarm includes its severity, priority, affected element, the time when the alarm occurred, a text messages and a unique identification (ID) number for that alarm.

The Event Manager processes these alarms using predefined rulesets and passes the output of this processing to Operations Center. Additionally, alarms can consist of standard alarm messages that provide the status of network components, messages that create or delete elements, or messages that initiate certain actions. The end result is that, from an input of potentially thousands of messages, a very limited number of alarms—perhaps only several dozen—are forwarded to Operations Center.

The components that comprise the Event Manager are shown in Figure 2-1:

***Figure 2-1** Event Manager Architecture*



Agents are on a single machine or distributed across multiple machines.

The Event Manager's architecture consists of the following components:

- Section 2.1, "Configuration Server," on page 13
- Section 2.2, "Agents and the Agent Container," on page 13
- Section 2.3, "Alarm Server and Event Manager Adapter," on page 14

These components are described in detail in subsequent sections of this guide.

2.1 Configuration Server

The Configuration Server (not to be confused with the Operations Center Configuration Manager) holds sets of configuration data that it receives from the configuration database. These data sets are called configuration profiles; and while several might exist, only one configuration profile can be active. A configuration profile consists of various information, such as:

- A set of agents
- The source with which each agent must communicate
- The rulesets to apply to the information from the sources (see Working with Rulesets, for more information)

The Configuration Server sends the appropriate configuration profile data to the Event Manager's agents and to the Event Manager's Alarm server.

2.2 Agents and the Agent Container

Agents collect and process data using rulesets in order to pass alarms to the Alarm Server. To conserve system resources, agents use a common process called an Agent Container. The Agent Container is a simple container that works behind the scenes to house all the agents in a single process.

The following outlines the basic process of using the Event Manager to collect and deliver alarm information:

1. The agents for the Event Manager are configured to collect data (ASCII or binary data) from a specific source, such as a server port, a client port, a device type (such as a modem or a router), a SNMP trap, or a process.
2. The agents apply rulesets to the source data and distills the information to create events and alarms.

   During agent creation, the Configuration Server assigns rulesets to agents. This information includes the sources to communicate with and the rulesets to run.
3. The agents then deliver the derived events and alarms to the Alarm server, which then manages the state.

For example, a device sends an alarm at regular intervals until the alarm is fixed. A ruleset determines how the data is converted into alarms, and the agent forwards them to the alarm server. The alarm server escalates alarm severity if an operator or a technician does not acknowledge or fix the alarm within a certain amount of time.

There is no limit on the number of agents or Agent Containers that can send alarms to the Alarm server.

The maximum number of alarms an Agent Container can hold in its outbound queue is set to 4,000. After reaching this limit, it discards the oldest alarms. For example, if the Alarm server is unavailable and cannot forward alarms, it discards the oldest alarms. To customize this setting, see Section 3.4, “Setting Custom Properties for Alarm Server Connectivity and Alarm Server Functions,” on page 22.

2.3 Alarm Server and Event Manager Adapter

The Alarm server communicates directly with Operations Center. The communication between the Alarm server and Operations Center takes place through the Event Manager adapter, which is the interface between Operations Center and the Event Manager’s management system.

The Alarm server receives a stream of processed events, called alarms, from the agents and sends these alarms to Operations Center. One option is storing all alarms generated by the Alarm server in a database so that the current set of alarms persists across multiple runs of the Alarm server. For details on configuring an Alarm server database, see Chapter 9, “Configuring the Alarm Server Database,” on page 89.

The alarms received by the Alarm server can perform the following actions:

- Create elements and element hierarchies
- Create alarms
- Clear other alarms

3 Event Manager Installation

The Event Manager and the Event Manager Agent are automatically installed with Operations Center. For step-by-step instructions on installing Operations Center, see the *Operations Center Server Installation Guide*.

There are various properties set in the Operations Center Configuration Manager for Event Manager and Event Integration Agents. If you are running the standard installation with Operations Center, you do not need to modify these settings from their defaults. For more information about Operations Center Configuration Manager settings related to Event Manager and agents, see Section 3.3, “Configuration Properties for Event Manager and Event Manager Agent,” on page 17.

However, you may want to customize various settings for Alarm Server Connectivity and Alarm Server Functions. To create a custom properties files and learn more about properties that can be configured, see Section 3.4, “Setting Custom Properties for Alarm Server Connectivity and Alarm Server Functions,” on page 22.

The following topics cover basic configuration properties and installing the Event Manager agent on a remote host:

- Section 3.1, “Installing the Event Manager Agent on a Remote Host,” on page 15
- Section 3.2, “Checking the Status of the Remote Host Server,” on page 16
- Section 3.3, “Configuration Properties for Event Manager and Event Manager Agent,” on page 17
- Section 3.4, “Setting Custom Properties for Alarm Server Connectivity and Alarm Server Functions,” on page 22
- Section 3.5, “Applying Patches to Event Manager Agents,” on page 24

3.1 Installing the Event Manager Agent on a Remote Host

Generally Event Manager and Event Manager Agent are installed as part of the Operations Center install on the same server as Operations Center.

Alternately, you can install Event Manager agents on remote hosts.

IMPORTANT: When installing a remote Event Manager agent, another instance of the Operations Center server cannot run on the same machine.

To install an Event Manager agent on a remote host that is not running Operations Center:

1. Run the Operations Center installer and select the *Event Manager Agent* option in the *Custom Install Options* page.

   For instructions on installing Operations Center, see the *Operations Center Server Installation Guide*.

   The agent installation also installs the Operations Center daemon (mosdaemon).

2. The Configuration Manager automatically launches. If not, on the remote server, launch the Configuration Manager by doing one of the following:

   - On Windows, at the DOS prompt, run `customizer` from the `\`*`eventmanageragent_install_path`*`\bin` directory.
   - On Unix, at a command prompt, run `Customizer` from the `/`*`eventmanageragent_install_path`*`/bin` directory.

3. Select *Event Manager Agent* in the left panel and specify the following settings for the agent:.

   - **Configuration Server Host:** Specify the host name for the server where Event Manager is installed and the Event Manager Configuration Server is running.

     For more information about the Event Manager Configuration Server, see Chapter 5, “Setting Up an Event Manager Configuration,” on page 31.
   - **Configuration Server Daemon Port:** The daemon port that the Configuration Server runs under. This setting must match the Daemon Port setting in the Operations Center Configuration Manager.

   All other Configuration Manager properties on this panel do not usually require any changes from the default values.

   For more information about Event Manager and Event Manager Agent Configuration Manager properties on the Operations Center server, see Section 3.3.3, “Understanding Event Manager Agent Properties,” on page 19.

4. Select *Security* in the left panel and specify the following settings for the agent:

   - **Client/Server Communication Mode:** Specify the level of security to use for communications. The selected level must match the setting as assigned in the Configuration Manager for the Operations Center server.

     If running a remote Event Manager agent in secure mode (*Client/Server Communications Mode* is set to either *Secured communications using SSL* or *Support both secured and unsecured communications*), you must also set up a keystore for the agent. This is set up the same way as for the Operations Center server. For information, see *Keystore and Trust Store Configuration* in the *Operations Center Security Management Guide*.

   All other Configuration Manager properties on this panel do not usually require any changes from the default values.

   For more information on security settings, see the *Operations Center Security Management Guide*.

5. Continue to Section 3.4, “Setting Custom Properties for Alarm Server Connectivity and Alarm Server Functions,” on page 22.

3.2 Checking the Status of the Remote Host Server

Use the `mosstatus` command from the Operations Center server to query the status of the remote host where an Event Manager agent is installed and running. To query the remote host, enter the following at the command line:

```
mosstatus -h remoteagenthost
```

3.3 Configuration Properties for Event Manager and Event Manager Agent

The Operations Center Configuration Manager contains settings related to both the Event Manager and Event Manager agents.

For information on the Configuration Manager, see “Updating Server Settings Using the Configuration Manager” in the *Operations Center Server Configuration Guide*.

Because Event Manager agents receive their configuration data from a central Configuration Manager, you can configure all Event Manager agents from the main Operations Center Configuration Manager without having to update agents configurations directly on each remote host.

For information on creating an Event Manager agent, see Chapter 8, “Creating and Defining Agents,” on page 79.

- Section 3.3.1, “Accessing Event Manager and Agent Configuration Settings,” on page 17
- Section 3.3.2, “Understanding Event Manager Properties,” on page 17
- Section 3.3.3, “Understanding Event Manager Agent Properties,” on page 19

3.3.1 Accessing Event Manager and Agent Configuration Settings

If selected during the installation process, the Operations Center Configuration Manager automatically opens during the installation process. Use the Configuration Manager to configure Event Manager and Event Manager agent properties.

To access the Configuration Manager:

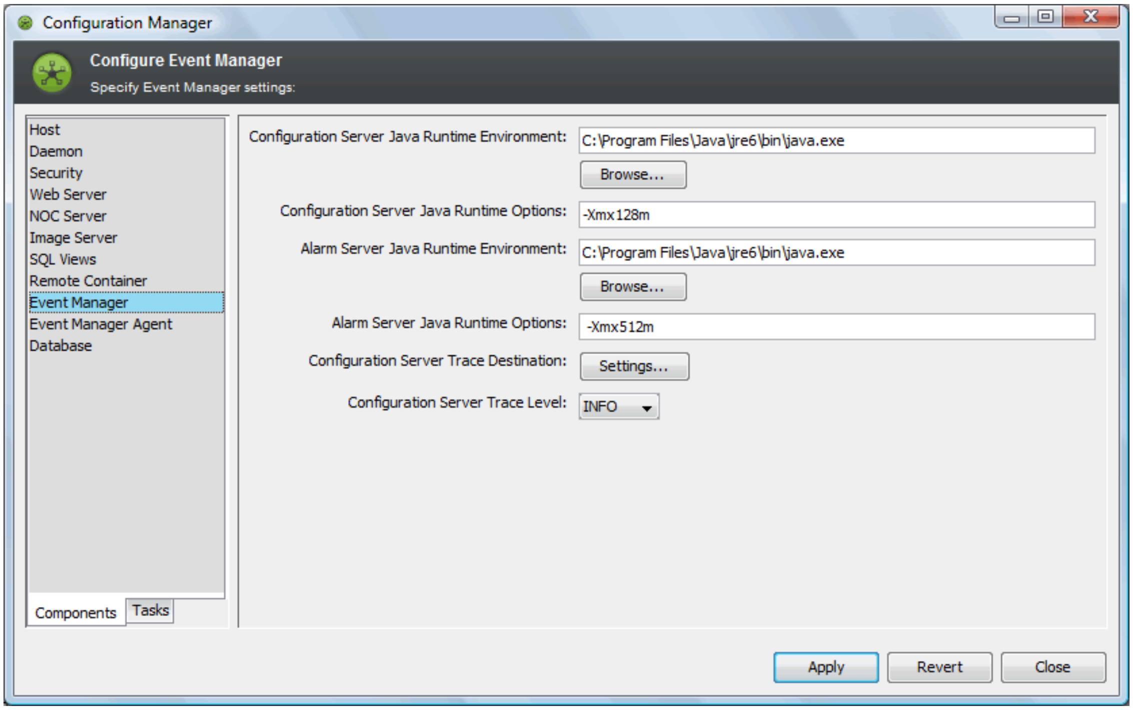
1. Do one of the following:
   - Click the Windows *Start* button, select *Programs* > *NetIQ Operations Manager*, then click *Configure NetIQ Operations Manager*.
   - To access the Configuration Manage for an agent on a remote host, do one of the following:
     - **On Windows:** At the DOS prompt, run `customizer` from the `\`*`install_path`*`\bin` directory.
     - **On Unix:** Run `Customizer` from the `/`*`install_path`*`/bin` directory.
2. For information on Event Manager properties, continue to Section 3.3.2, “Understanding Event Manager Properties,” on page 17.

   For information on agent properties, continue to Section 3.3.2, “Understanding Event Manager Properties,” on page 17.

3.3.2 Understanding Event Manager Properties

Event Manager related settings are updated in *Event Manager* section of the Operations Center Configuration Manager.

Figure 3-1 Event Manager settings showing in the Operations Center Configuration Manager



Configuration Server Java Runtime Environment: C:\Program Files\Java\jre6\bin\java.exe

Configuration Server Java Runtime Options: -Xmx128m

Alarm Server Java Runtime Environment: C:\Program Files\Java\jre6\bin\java.exe

Alarm Server Java Runtime Options: -Xmx512m

Configuration Server Trace Destination:

Configuration Server Trace Level: INFO

Table 3-1 describes the settings in the Operations Center Configuration Manager related to Event Manager. For more information on the Configuration Manager, see the *Operations Center Server Configuration Guide*.

Table 3-1 Configuration Manager Event Manager Settings

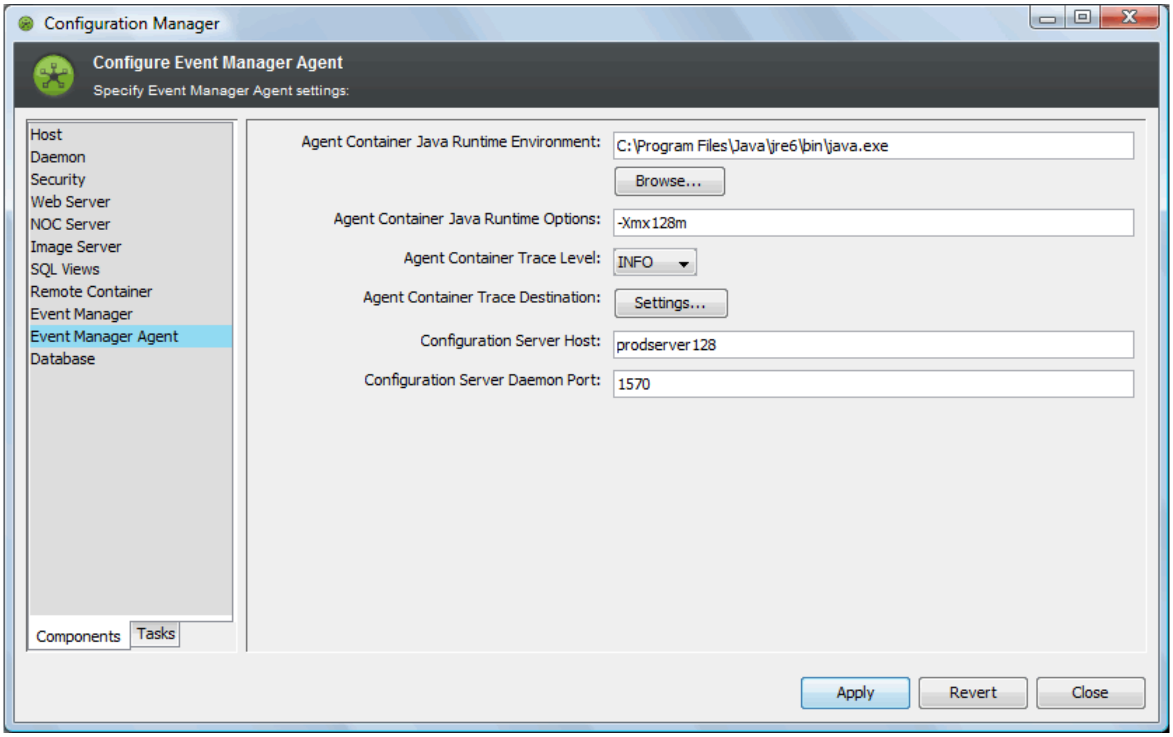
Setting	Windows Default	UNIX Default	Description
Configuration Server Java Runtime Environment	`C:\`*`OperationsCenter_install_path`*`\jre\bin\java.exe`	`/`*`OperationsCenter_install_path`*`/jre/bin/java.exe`	Executable for the Java Runtime Environment for the Event Manager Configuration Server. Click *Browse* to navigate to the location of the JRE. For more information about configuring Java and Memory, see the *Operations Center Server Configuration Guide*.

Setting	Windows Default	UNIX Default	Description
Configuration Server Java Runtime Options	`-server -Xmx128m`	`-Xmx128m`	Option for running VM for the Event Manager Configuration server. For more information about configuring Java and Memory, see the *Operations Center Server Configuration Guide*.
Alarm Server Java Runtime Environment	`C:\`*`OperationsCenter_install_path`*`\jre\bin\java.exe`	`/`*`OperationsCenter_install_path`*`/jre/bin/java.exe`	Executable for the Java Runtime Environment for the Event Manager Alarm Server. Click *Browse* to navigate to the location of the JRE. For more information about configuring Java and Memory, see the *Operations Center Server Configuration Guide*.
Alarm Server Java Runtime Options	`-server -Xmx256m`	`-server -Xmx256m`	A setting for VM for the Event Manager Alarm server. Usually does not need changing.
Configuration Server Trace Destination	`\`*`OperationsCenter_install_path`*`\logs`	`/`*`OperationsCenter_install_path`*`/logs`	The settings for the Event Manager server trace logs.
Configuration Server Trace Level	INFO	INFO	These settings control how much information is passed to the Event Manager server trace logs.

3.3.3 Understanding Event Manager Agent Properties

Event Manager Agent related settings are updated in *Event Manager Agent* section of the Operations Center Configuration Manager.

Figure 3-2 Event Manager Agent settings showing in the Operations Center Configuration Manager



Agent Container Java Runtime Environment: C:\Program Files\Java\jre6\bin\java.exe

Agent Container Java Runtime Options: -Xmx128m

Agent Container Trace Level: INFO

Agent Container Trace Destination: Settings...

Configuration Server Host: prodserver128

Configuration Server Daemon Port: 1570

Table 3-2 describes the settings in the Operations Center Configuration Manager related to Event Manager Agents. For more information on the Configuration Manager, see the *Operations Center Server Configuration Guide*.

Table 3-2 Configuration Manager Event Manager Agent Settings

Setting	Windows Default	UNIX Default	Description
Agent Container Java Runtime Environment	`C:\`*`OperationsCenter_install_path`*`\jre\bin\java.exe`	`/`*`OperationsCenter_install_path`*`/jre/bin/java.exe`	Executable for the Java Runtime Environment for the Event Manager Agent Container. Click *Browse* to navigate to the location of the JRE. For more information about configuring Java and Memory, see the *Operations Center Server Configuration Guide*.

Setting	Windows Default	UNIX Default	Description
Agent Container Java Runtime Options	`-server -Xmx128m`	`-server -Xmx128m`	Options for running VM for the Event Manager Agent Container server. Usually does not need changing. For more information about configuring Java and Memory, see the *Operations Center Server Configuration Guide*.
Agent Container Trace Level	INFO	INFO	These settings control how much information is passed to the Event Manager Agent trace logs. For more information about configuring trace logs, see the *Operations Center Server Configuration Guide*.
Agent Container Trace Destination	`\`*OperationsCenter_install_path*`\logs`	`/`*OperationsCenter_install_path*`/logs`	The location in which to save the Event Manager agent trace log files. For more information about configuring trace logs, see the *Operations Center Server Configuration Guide*.
Configuration Server Host	*IP address for localhost*	*IP address for localhost*	IP address for the Event Manager Configuration Server for the agent. When an agent is installed with Operations Center or a Remote Container, this defaults to the local server. When the agent is stand alone, it must be populated.

Setting	Windows Default	UNIX Default	Description
Configuration Server Daemon Port	`1570`	`1570`	The daemon port that the Configuration Server runs under. Note that this value must match the Operations Center server Daemon Port setting in the Operations Center Configuration Manager.

3.4 Setting Custom Properties for Alarm Server Connectivity and Alarm Server Functions

Create a custom properties file to handle customized settings for the Event Manager.

- Section 3.4.1, “Creating a Custom Properties File,” on page 22
- Section 3.4.2, “Properties Related to Alarm Server Connectivity,” on page 22
- Section 3.4.3, “Custom Properties Related to Alarm Server Functions,” on page 23

3.4.1 Creating a Custom Properties File

To create a custom properties file:

1. Create a file named `Eve.custom.properties` and save it in the `/`*`OperationsCenter_install_path`*`/config` directory.
   - Do not add an extension to the file name.
   - If the same property is in both the `Eve.custom.properties` file and the `Eve.properties` file, the Event Manager uses the value as specified in the `Eve.custom.properties` file.
   - When the Operations Center Configuration Manager runs, it does not overwrite the `Eve.custom.properties` file. The Operations Center Configuration Manager overwrites the `Eve.properties` file.
2. Modify existing properties to meet requirements and add properties as necessary.

   For information to make these modifications, see Section 3.4.2, “Properties Related to Alarm Server Connectivity,” on page 22 and Section 3.4.3, “Custom Properties Related to Alarm Server Functions,” on page 23.

3.4.2 Properties Related to Alarm Server Connectivity

Add any of the following properties to the `Eve.custom.properties` file to help manage data streams after losing Alarm server connectivity.

The Event Manager Server controls the alarm queue based on the percentage of free memory available. Otherwise, supply a value with the com.mosol.Eve.Agent.Xmx property. Using the Xmx value, the server queues events until the VM has 10 percent or less free space available. To increase or decrease this minimum free memory ratio, use the `com.mosol.Eve.Agent.storeAndForwardAlarmsMinFreeMemoryRatio` property.

The following lists AlarmServer connectivity custom properties:

- **com.mosol.Eve.Agent.storeAndForwardAlarms:** This property enables/disables storage and forwarding of alarms to managed data streams. The default is True. To disable storage and forwarding, set it to False.
- **com.mosol.Eve.Agent.storeAndForwardAlarmsMax:** This property is only used if it cannot discover the `-Xmx` setting for the VM. It sets the maximum number of alarms to store while the managed data stream is down.

  Set the value to a number that equals the maximum number of alarms that are queued when Alarm server connectivity is lost. When it reaches the specified number of alarms, it discards the oldest alarm and keeps the newest alarm until the managed data stream can be contacted again. To queue all alarms, set the value to -1. To not queue any events, set to 0. The default is 10000 alarms.
- **com.mosol.Eve.Agent.storeAndForwardAlarmsMinFreeMemoryRatio:** This property controls the alarm queue based on the percentage of free space in the VM.

  The calculation used is: actual memory used divided by maximum memory available. If that percentage is greater than the supplied value, it queues the alarm; otherwise, it discards the oldest alarm and queues the alarm.

  The default is 10 percent. The maximum value allowed is 51. If a larger value is specified, it is automatically reset to 10.
- **com.mosol.Eve.Agent.alarmQueueSize:** This property sets the maximum number of alarms an Agent Container can hold in its outbound queue. The default value is 4000.

3.4.3 Custom Properties Related to Alarm Server Functions

Add any of the following properties to the `Eve.custom.properties` file to help manage Alarm server functions.

WARNING: The following settings in the `Eve.properties` file control the flow of events between the Alarm server and the Event Manager adapter. Do not change or try to override these values.

- Eve.Max.Dispatch.Events.Block.Size=1000
- Eve.Max.Dispatch.Events.Pause.In.Millis=100

The following lists the Alarm server function custom properties:

- **com.mosol.Eve.AlarmServer.usedatetime:** If `True`, the event date and time stamps are taken from alarm data versus the current date/time when the event is processed. The default is `False`. When `True`, you must:
  - Add this property to the `Formula.custom.properties` file and set to `True`.

    For information about the Formula.custom.properties file, see “Making Custom Changes” in the *Operations Center Server Configuration Guide*.
  - The DATETIME system variable must be set properly for all rules within rulesets you want to use the Alarm data for event date and time stamp. For information, see “Understanding the System Variables for the Ruleset Editor” on page 56.

- **com.mosol.Eve.AlarmServer.delayedAlarmsPreCloseRules:** If `True`, events that create a delayed alarm perform Close Rule functions as soon as the event arrives in the alarm server. If False, Close Rule functions are not performed until the delayed alarm becomes active. The default is `True`.
- **com.mosol.Eve.AlarmServer.resetDelayedAlarmsTime:** If `True`, a delayed alarm's initial date and time, and its most recent date and time are set to the date and time that the alarm became active. If `False`, a delayed alarm's initial date and time is set to the date and time the event arrived in the alarm server and its most recent date and time is set to the date and time that the alarm became active. In both cases, the alarm's date and time in Operations Center is the most recent date and time. The default is `False`.
- **com.mosol.Eve.AlarmServer.useEMSClassToClose:** If `True`, alarms are closed across the EMS_class as defined in the agent as the hierarchy class. If `False`, alarms are closed using the EMS as defined in the agent as the agent's name. (Note: Setting EMS in the rule set does not work at this time). The default is `False`.
- **com.mosol.Eve.AlarmServer.updateAllFieldsOnAccumulation:** If `True`, updates all the alarm's properties on accumulation. This includes, but is not limited to, severity, priority, and alarm text. If False, only the accumulation counter, the most recent date and time, and the alarm's timeout value are updated. The default is `True`.

  Accumulated alarms that have escalated or de-escalated will not have their severity or priority properties updated.
- **com.mosol.Eve.AlarmServer.journalInactive Events:** If `True`, pending delayed and threshold alarms are stored in the external Event Data Store database. The default is `True`.
- **com.mosol.Eve.AlarmServer.timeout.schedule:** The scheduled time, in milliseconds, to check for alarm timeouts. The default is `30000` (30 seconds).
- **com.mosol.Eve.AlarmServer.delay.schedule:** The scheduled time, in milliseconds, to evaluate delayed events. The default is `30000` (30 seconds).
- **com.mosol.Eve.AlarmServer.escalation.schedule:** The scheduled time, in milliseconds, to evaluate time escalated alarms. The default is 30000 (30 seconds).
- **com.mosol.Eve.AlarmServer.maxActiveAlarms:** The maximum number of active alarms that signals the Event Manager adapter to set the severity state and warnings about the number of active Event Manager alarms. This is not the maximum number of alarms for the Alarm server. The Alarm server holds as many alarms as machine resources allow. The default is 100000.

For additional explanations of these properties and examples, see Section 7.4.9, "Configuring Alarms," on page 70.

3.5 Applying Patches to Event Manager Agents

The Event Manager installation automatically distributes a patch to all remote agents. However, you must perform the following steps:

1. Before a patch distribution is applied, it is necessary to remove the `/`*`OperationsCenter_install_path`*`/html/eiagent/cache` directory.
2. Apply the patch distribution.
3. After the patch installation completes, stop and start Operations Center on any server running an Agent Container.

4 Working with Event Manager Adapter

An adapter is a Operations Center interface with the underlying management systems in a technology infrastructure. It is necessary to define an adapter for each instance of the Event Manager in the network. Only one Event Manager adapter can exist on a given machine.

4.1 Creating an Event Manager Adapter

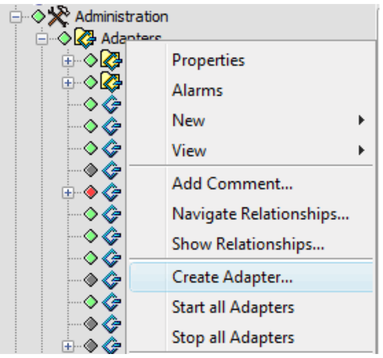
Create only one Event Manager adapter on each machine.

For information about the Experience Manager adapter properties, see "Creating an Event Manager Adapter" in the *Operations Center Event Manager Guide*.

To create an Event Manager adapter:

1 In the *Explorer* pane, expand the *Administration* root element.

2 Right-click *Adapters*, then select *Create Adapter* to open the Create Adapter dialog box:



3 Click the *Type* drop-down list, then select *Event Manager*.

A default name of the Event Manager adapter (Adapter: Operations Center Event Manager™) displays in the *Name* field. Default adapter properties specific to the Event Manager display in the Properties table.

4 In the *Name* field, replace the default name with one that defines your system.

5 Enter values for the Event Manager properties in the Properties table:

AddAgentElements: If True, all Event Manager agents (EMS) appear in the hierarchy and never time out. If False, the EMS agents appear only when they are generated via alarms and they time out like an ordinary alarm.

AgeOutTime: If there are no open alarms, and the element's condition hasn't changed in the last n seconds, and the element has no children, then the element disappears from the display after the specified time (where n is the number of seconds). If another alarm is generated for this element, the element reappears. The default is 300.

- **AgeOutTime < 0:** Never age out.
- **AgeOutTime = 0:** Age out immediately.
- **AgeOutTime > 0:** Age out after specified time expires.

AlarmColumns: A comma-separated list that determines which alarm columns display and the order that the alarm items (date and time, rule, and so on) display in the Alarms view. The default is:

Number,Rule,Description

For Alarm column aliasing you can assign new names to alarm columns using the format:

display_name=*current_name*

For example, `Class=Rule` displays rule data in a column named *Class*.

A list of all the possible Event Manager AlarmColumns: *Number*, *AssignedTo*, *Class*, *Description*, *EnRouteTo*, *Group*, *InitDateTime*, *Priority*, *Rule*, and *SuppressAutomations*.

AutomationsOnReload: This property is only meaningful if Event Manager Alarm Persistence is enabled. This adapter property configures the behavior of reloaded alarms regarding the Alarm Create type of event automations.

When the Event Manager Alarm server starts up, it marks alarms read in from the persistent alarm store as "reloaded."

If True, reloaded alarms fire Alarm Create type of event automations. The default is False.

HierarchyFile: A file in the `/`*`OperationsCenter_install_path`*`/database/` directory that contains an XML description of the hierarchy of elements that is built beneath the element that represents the adapter. The default is `examples/EveHierarchy.xml`.

Before modifying the hierarchy file, copy the example file to the `/`*`OperationsCenter_install_path`*`/database` directory and change the location reference. This protects changes from being overwritten during software updates. For information, see *Using the HierarchyFile* in the *Operations Center Adapter and Integration Guide*.

NonClearableRules: A comma-separated list of rule names. No users are allowed to close an alarm generated by one of the named rules. This is desirable for certain classes of alarms that the system creates and destroys, and in cases where allowing users to close alarms is undesirable.

Script.onError: Enter a script that executes if the adapter fails for any reason. The script can print the reason for the failure as a "msg"; for example:

```
log.info(msg)
```

Script.onInitialized: A script that executes when the adapter first initializes. All the `Script.`*`nnn`* properties are optional.

Script.onStarted: A script that executes when the adapter starts, either manually or automatically when the Operations Center server starts.

Script.onStopped: A script that executes after manually stopping the adapter.

Server: The hostname of the server where the management software is installed. The default is com.mosol.ORB.Eve.AlarmServer.

StylesheetFile: The stylesheet file to apply against the HierarchyFile as a style markup and produce the final output. It is located in the `/OperationsCenter_install_path/database` directory.

UseAlarmTimesForCondition: Specifies the date and time stamp to use for any alarm data stored by the data warehouse. If True (the default), the date and time information originates directly from the alarm information. If False, the date and time is when the Operations Center server received the alarm.

6. Click *Create*.
7. To start the adapter whenever the Operations Center server starts, leave the *Start Adapter Automatically* check box selected.
8. Click *Start* in the *Commands* section to start the adapter.

   After the adapter starts, the *Close* button becomes available.
9. Click *Close* to close and exit the dialog box.

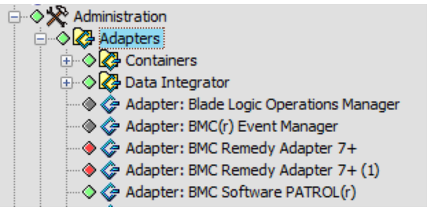
   The new adapter displays in the list of elements in the *Explorer* pane, under *Administration* > *Adapters*.

4.2 Checking the Adapter Status

Check an adapter's color-coded condition indicator to quickly identify critical situations.

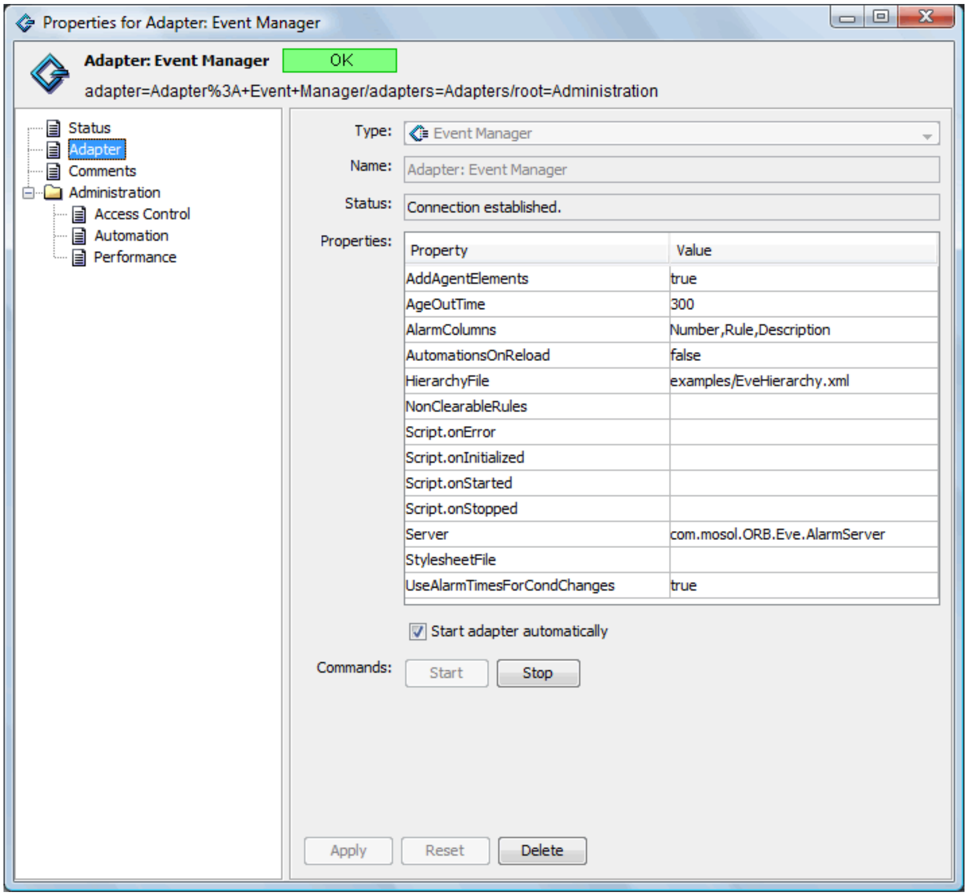
Figure 4-1 illustrates color-coded condition indicators identifying the current adapter status:

Figure 4-1 *Explorer Pane*


Administration
Adapters
Containers
Data Integrator
Adapter: Blade Logic Operations Manager
Adapter: BMC(r) Event Manager
Adapter: BMC Remedy Adapter 7+
Adapter: BMC Remedy Adapter 7+ (1)
Adapter: BMC Software PATROL(r)

To view the Event Manager adapter properties:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters*.
2. Click *Event Manager Adapter*, then select *Properties* to open the Status property page:



Adapter: Event Manager OK

adapter=Adapter%3A+Event+Manager/adapters=Adapters/root=Administration

Type: Event Manager

Name: Adapter: Event Manager

Status: Connection established.

Properties:

Property	Value
AddAgentElements	true
AgeOutTime	300
AlarmColumns	Number,Rule,Description
AutomationsOnReload	false
HierarchyFile	examples/EveHierarchy.xml
NonClearableRules	
Script.onError	
Script.onInitialized	
Script.onStarted	
Script.onStopped	
Server	com.mosol.ORB.Eve.AlarmServer
StylesheetFile	
UseAlarmTimesForCondChanges	true

☑ Start adapter automatically

Commands:

3. Click *Adapter* to view and if necessary, edit the adapter properties.

4.3 Manually Starting and Stopping the Adapter

To start or stop an adapter manually:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters*.
2. Right-click an adapter, then select *Start Adapter* or *Stop Adapter*.

   The adapter starts or stops.

4.4 Deleting an Event Manager Adapter

To delete an event manager adapter:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters*.
2. Right-click the *Event Manager* adapter, then select *Delete Adapter* to open a confirmation dialog box.
3. Click *Yes* to delete the adapter.

4.5 Configuring the Event Manager Adapter

After creating the Event Manager adapter, follow the steps in this section to configure and use the adapter. Each step is explained in detail in the subsequent sections of this document.

To configure the Event Manager adapter:

1. Start the Configuration Server.

   For instructions, see Section 5.1, “Starting the Configuration Server,” on page 31.

2. Create and activate configurations.

   For instructions, see Section 5.3, “Creating a Configuration,” on page 32.

3. Create the necessary hosts.

   For instructions, see Section 6.1, “Creating Hosts,” on page 35.

4. Define sources for the hosts.

   For instructions, see Section 6.3, “Creating Sources,” on page 36.

5. Create (or import), define, and validate rulesets.

   For instructions, see Chapter 7, “Working with Rulesets,” on page 43.

6. Create and start agents.

   For instructions, see Chapter 8, “Creating and Defining Agents,” on page 79.

7. Configure the Alarm server.

   For instructions, see Chapter 9, “Configuring the Alarm Server Database,” on page 89.

8. Test the configuration by sending simulated events to the agent ports and verify that the events matched the rules and activated alarms.

   For instructions, see Chapter 10, “Testing the Configuration,” on page 103.

9. Restrict access to the Event Manager.

   For instructions, see Chapter 11, “Restricting Access to the Event Manager,” on page 105.

5 Setting Up an Event Manager Configuration

After creating the Event Manager adapter, the next step is to configure it. Operations Center automatically creates a container object named Configurations for the adapter. This container object includes the Configuration Server and the configuration file.

5.1 Starting the Configuration Server

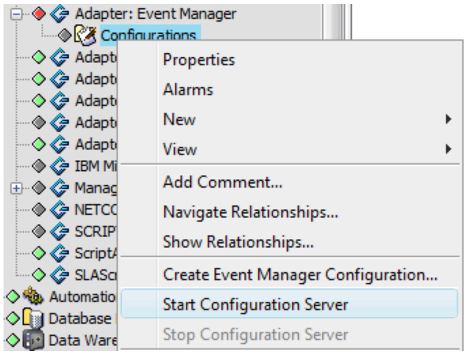
The Event Manager Configuration Server does not start automatically. It is necessary to start the Configuration Server before defining the configuration and defining components such as hosts, ports, and rulesets. Start the Configuration Server from:

- Operations Center
- The command line, by typing the `eve.bat` command from the `/`*`OperationsCenter_install_path`*`/bin` directory

To start the Configuration Server from Operations Center:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter.

2 Right-click *Configurations*, then select *Start Configuration Server*.



5.2 Stopping the Configuration Server

The Event Manager components are not necessarily interdependent. Stopping the Configuration Server doesn’t automatically stop the adapter, the Agent Container, or the Alarm server. To shut down everything for the Event Manager after stopping the Configuration Server, it is necessary to stop, in the following order:

1. The adapter
2. The Agent Container
3. The Alarm server

To stop the Configuration Server:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter.
2. Right-click *Configurations*, then select *Stop Configuration Server*.

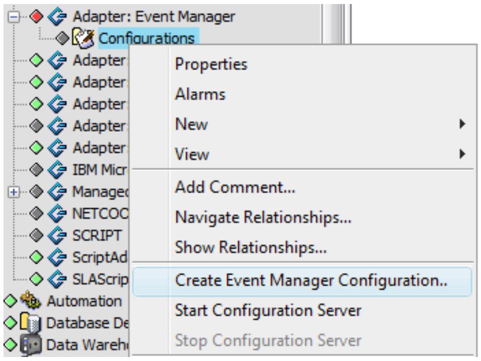
5.3 Creating a Configuration

Configuration files reside in the Configurations container for each Event Manager adapter. Within each configuration, define hosts, ports, and rulesets, and start the Alarm server for the adapter.

After starting the Configuration Server, create and define the configuration.

To create an Event Manager configuration file:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter.
2. Right-click *Configurations*, then select *Create Event Manager Configuration*.



3. In the Create Event Manager Configuration dialog box, specify a name for the configuration file in the *Configuration Name* field.

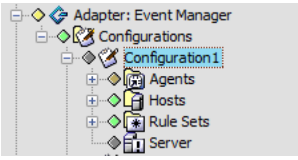
   In this example, `Event Manager Configuration 1` is the file name.
4. Select the *Active Configuration* check box to make this the active configuration.

   Multiple configurations can exist under *Event Manager Configurations*, but only one configuration file can be active. By default, the first configuration created is the active configuration.

   If this is the first configuration defined, the *Active Configuration* check box is selected by default. In this case, this option is dimmed and cannot be edited.

5 Click *Apply*.

Operations Center adds the new configuration, `Event Manager Configuration 1`, under *Configurations* in the *Explorer* pane, and automatically adds *Agents*, *Hosts*, *Rule Sets*, and *Server* categories to the new configuration file:



At this point, no agents or rulesets exist.

By default, the host that is local to the Event Manager Configuration Server is in the *Hosts* category.

The *Server* element is the *Alarm* server that was specified in the *Server* field when creating the Event Manager adapter.

5.4 Activating a Configuration

The Event Manager might only have one active configuration. By default, the first configuration created is active. However, it is easy to select a different configuration as the active configuration.

To select an active configuration:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations*.
2. Right-click a configuration element, then select *Activate Configuration*.

   The configuration becomes the active configuration.

5.5 Deleting a Configuration

To delete a configuration:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations*.
2. Right-click a configuration element, then select *Delete Configuration*.

   The element disappears from the *Explorer* pane.

5.6 Overview of Configuration Components

The first steps for setting up the Event Manager adapter are starting the Configuration Server and creating a configuration. Next, define all the configuration components for the new configuration file. These configuration components include hosts, ports, rulesets, agents and the Alarm server. The subsequent sections of this guide step through the process of defining the configuration components:

- Chapter 6, “Defining Hosts and Sources,” on page 35
- Chapter 7, “Working with Rulesets,” on page 43
- Chapter 8, “Creating and Defining Agents,” on page 79
- Chapter 9, “Configuring the Alarm Server Database,” on page 89

6 Defining Hosts and Sources

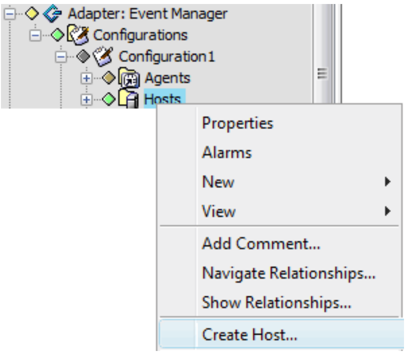
After creating the Event Manager adapter and defining a configuration for the adapter, the next step is setting up the required hosts and the sources. Hosts are the machines configured with Event Manager components. Depending on your architecture, a host can house the Alarm server or run an agent. Sources are the communication channels for the hosts; they provide notification information to the agents.

6.1 Creating Hosts

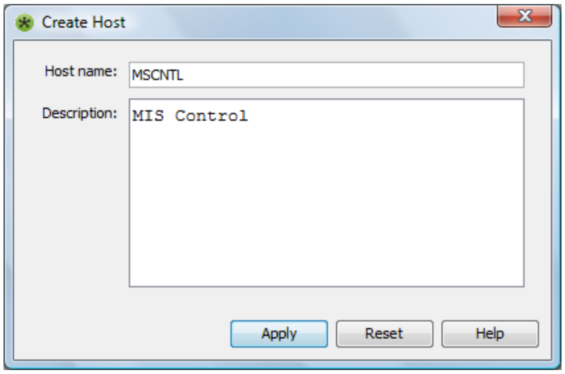
Define one or more hosts for each configuration.

To create a host:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations*, then select a particular configuration.
2. Right-click *Hosts*, then select *Create Host* to open the Create Host dialog box:



3. Specify the hostname in the *Hostname* field and a description in the Description text area:



Host name: MSCNTL

Description: MIS Control

4. Click *Apply*.

   In this example, a host named MSCNTL is created.

6.2 Deleting Hosts

To delete a host:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a particular configuration > *Hosts*.
2. Right-click a host, then select *Delete Host*.

   The host disappears from the *Explorer* pane.

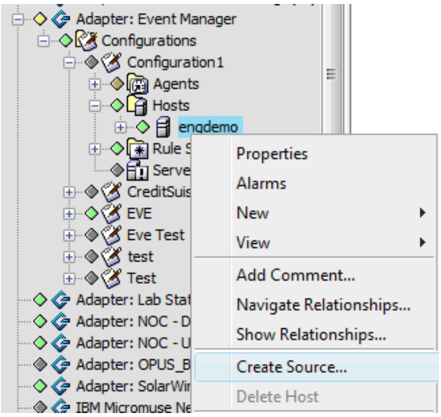
6.3 Creating Sources

Sources are access points for agents to receive data from a host. Therefore, sources are the communication channel by which agents can:

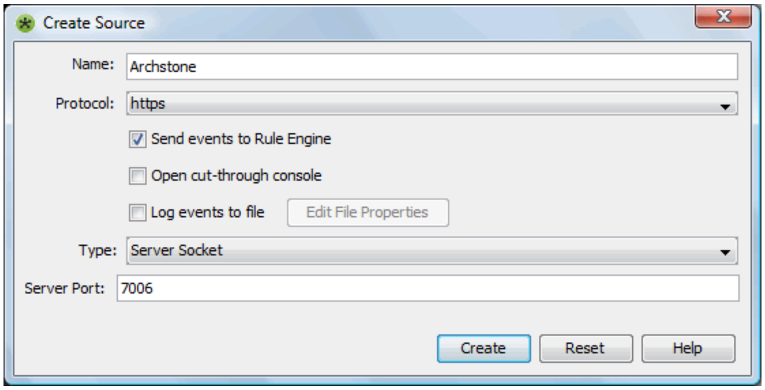
- Receive events from a log file
- Listen to accept text for the rules engine
- Receive the output from an external program and apply a ruleset
- Accept SNMP traps from SNMP agents
- Act as a proxy so that Operations Center users can connect to another system
- Connect a physical device such as a modem
- Accept T/EC Native feeds

To set up a source for a host:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a particular configuration > *Hosts*.



2 Right-click a host, then select *Create Source* to open the Create Source dialog box:



Create Source

Name: Archstone

Protocol: https

☑ Send events to Rule Engine

□ Open cut-through console

□ Log events to file

Type: Server Socket

Server Port: 7006

3 Complete the settings:

Name: The name of the source.

Protocol: Click the drop-down list, then select a protocol for the source:

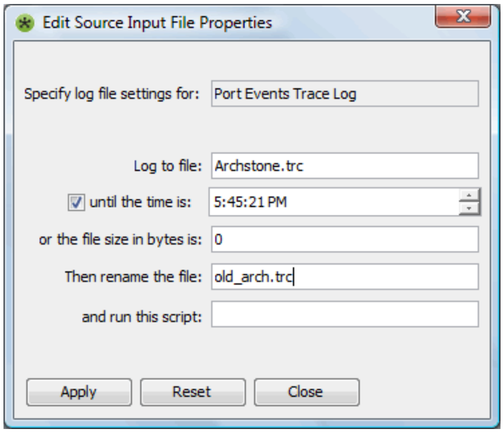
- **none:** establishes a raw socket transport without any protocol being used.
- **telnet:** establishes a Telnet session.
- **ftp:** establishes an FTP session.
- **http or https:** establishes an HTTP or HTTPS connection.

  When the agent queries the web site, if the `If-Modifed_Since` header property is greater than the last query, then the query will return data. Otherwise the query returns data every time.
- **smtp/pop3/nntp:** establishes an SMPT/POP3/NNTP connection.

Send events to rule engine: Select the check box to collect alarms from this source.

Open cut-through console: Select the check box to provide a console window for the user to access the source.

Log events to file: Select the check box to write the raw events to a file. Click *Log File Properties* to configure the destination in the Edit Source Input File Properties dialog box opens:



Edit Source Input File Properties

Specify log file settings for: Port Events Trace Log

Log to file: Archstone.trc

☑ until the time is: 5:45:21 PM

or the file size in bytes is: 0

Then rename the file: old_arch.trc

and run this script:

The following describes the *Log File* properties required for the *Log File Configuration* setup:

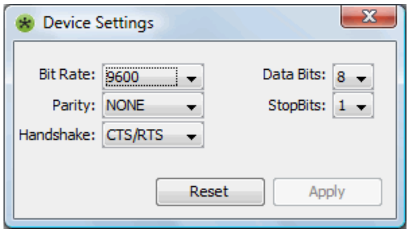
- **Log to file:** Specify the file name for storing the log information. Edit this entry to reflect the path to the Operations Center directory.
- **Until the time is:** Select the check box to set a cut-off time. Use the spinner buttons to select a cut-off time for collecting log data.
- **Or the file size in bytes is:** Enter the cut-off file size for collecting trace log data. The file size is used as a cut-off unless a cut-off time is selected.
- **Then rename the file:** When the trace log file reaches one of the cut-offs above, it renames the file to this entry, and start a new log file.
- **And run this script:** Any program can be run here, but the default is a file compression application, gzip.

Click *Apply* to save settings and close the dialog box when selections are complete.

Type: Click the drop-down list, then select a source type. The dialog box changes to show required options for the selected source type. Select from the following source types:

- **Server Socket:** Passively listens and waits to be connected to the port. Specify:
  - **Port:** The server port where the agent connects. Make sure the port selected does not conflict with the ports already in use for Operations Center. For more information on port usage in Operations Center, see the *Operations Center Server Configuration Guide*.
- **Client Socket:** Initiates a socket connection to the specified host and port, from which it receives lines of text to process. Specify:
  - **Host:** The name of the host to connect to.
  - **Port:** The port number for the host. Make sure the port selected does not conflict with the ports already in use for Operations Center. For more information on port usage in Operations Center, see the *Operations Center Server Configuration Guide*.
- **Device:** Defines a device where the agent assigned is connected. Specify:
  - **Device:** The device name.

    Click *Change Device Parameters* to customize the standard connection parameters, then click *Apply*.

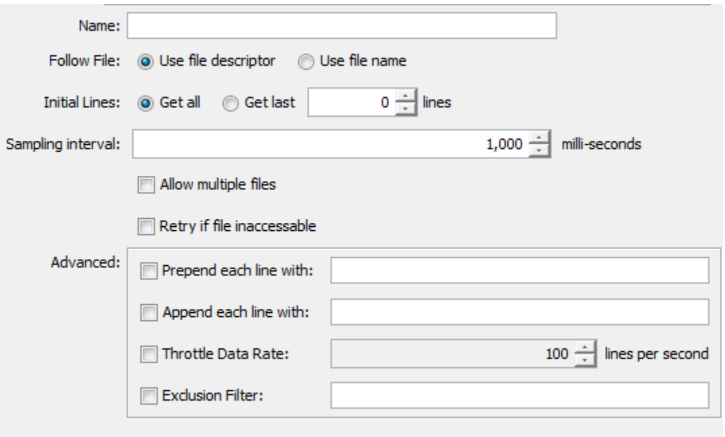
    Device Settings

    Bit Rate: 9600
    Parity: NONE
    Handshake: CTS/RTS
    Data Bits: 8
    StopBits: 1

- **Process:** Runs a specified command at the command line prompt and collects the output of that command. Specify:
  - **Process:** Enter a command to return output to the agent. To send all updates to the trace file (formula.trc) are sent to the agent, enter:

    ```
    tail -f d:/OperationsCenter_install_path/logs/formula.trc
    ```
- **SNMP Trap:** Defines a new SNMP trap port in the Event Manager. Specify:
  - **SNMP trap port:** the port number for the SNMP trap. The default value is 162.

- **File Tail:** Obtains information from a file:



Name:

Follow File: ● Use file descriptor ○ Use file name

Initial Lines: ● Get all ○ Get last 0 lines

Sampling interval: 1,000 milli-seconds

☐ Allow multiple files

☐ Retry if file inaccessable

Advanced:

☐ Prepend each line with:

☐ Append each line with:

☐ Throttle Data Rate: 100 lines per second

☐ Exclusion Filter:

Specify the following values:

- **Name:** A single tail file, a file that contains a list of files to follow, or a file expression (UNIX or WINTEL). Use commas as a delimiter if specifying more than one file.

WARNING: If specifying a tail file on a mapped or network drive, the Operations Center Service Account must have permissions to access the file. Without permissions, the source will be unable to access the file.

If using a file expression, the name can consist of a sequence of characters, path expressions, and date expressions as follows:

```
fileName{pathexp}{date}
```

where {pathexp} is a sequence of standard UNIX or WINTEL path expression syntax characters. For example:

```
my_file_???.txt matches my_file_0000.txt and my_file_172.txt and *.txt
```

Date expressions must be differentiated from regular expressions. Inject a special set of tags that follow the XML convention:

```
<date>datexp</date>
```

The `datexp` portion of the name is defined as:

-datexp: %YYYY, %yyyy – Year expressed as a four-digit numeral (such as 2008)

%yy – Year expressed as a two-digit numeral (such as 08)

%M, %m – Month

%D,%d – Day

For example:

```
my_files_*_<date>%m.%d.%yy</date>.txt
```

matches:

```
my_files_friday_10.22.07
```

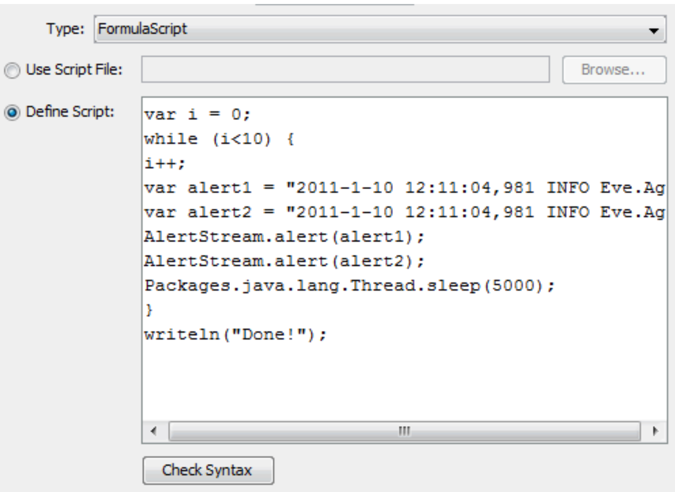
Using expression syntax means that more than one file can match. However, if the *Allow multiple files* option is not selected, only the first file is tailed.

    - **Follow File radio buttons:** Select one of the following to specify how the file is identified:
        - **Use file descriptor:** Uses the operating system descriptor of the file for identification. If the file name is changed, the process continues to use the original file regardless of the file name.
        - **Use file name:** Searches for the file based on the file name.
    - **Initial lines radio buttons:** Select one of the following ways to specify how many lines are returned to the source:
        - **Get all lines:** Returns the entire contents of the file.
        - **Get Last X Lines:** Use the spinner to select the number of lines to take from the end of the files.
    - **Sampling interval:** Use the spinner to set the time interval, in milliseconds, for checking the file for new data.
    - **Allow multiple files check box:** Select to allow more than one file to be tailed. If this is deselected and multiple files are matched, the first file found is tailed.
    - **Retry if file inaccessible check box:** Select to automatically attempt another connection if the file is not accessible.
    - **Prepend each line with check box:** Includes the specified text at the beginning of each line.
    - **Append each line with check box:** Includes the specified text at the end of each line.
    - **Throttle data rate check box:** Use the spinner to set the number of lines per second as the rate of data transmission.
    - **Exclusion filter check box:** Use a regular expression to exclude matching lines. Enter the regular expression in the field.
- **FormulaScript:** Runs a script using the `eventIntegrator` object and returns the results. Available methods include:
    - `eventIntegrator.postEvent(eventString)` - Sends an event string into the processing engine (similar to reading a line from a file tail.)
    - `eventIntegrator.getLog()` - returns the logger for the agent.
    - `eventIntegrator.getAgentHandle()` - provides access to agent configuration object, from which the script can see:
        - host()
        - name()
        - className()
        - maxQueuedAlarms()
        - dataType()
        - emulation()
        - encoding()
        - startOnStartup()
        - processRuleSetOnStart()
        - isInUse()
        - lastModified()
        - serverName()
        - traceLevel()

Select the *Use Script File* radio button to use a stored script file.

Specify the location or file name in the field or click *Browse* to find, then select a file.

Alternatively, select the *Define Script* radio button to enter (or cut and paste) a script into the script dialog box, as shown:


Type: FormulaScript

○ Use Script File:

● Define Script:

```
var i = 0;
while (i<10) {
i++;
var alert1 = "2011-1-10 12:11:04,981 INFO Eve.Ag
var alert2 = "2011-1-10 12:11:04,981 INFO Eve.Ag
AlertStream.alert(alert1);
AlertStream.alert(alert2);
Packages.java.lang.Thread.sleep(5000);
}
writeln("Done!");
```

Then, click *Check Syntax* to verify correct FormulaScript syntax.

- **URL:** Connects to a source using Internet protocols. Specify:
    - **Source URL:** Specify a URL address/location.

4 Click *Create* to save changes and complete the configuration.

6.4 Deleting Sources

To delete a source:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a particular configuration > *Hosts* > a host element.

2 Right-click a source, then select *Delete Source*.

The source disappears from the *Explorer* pane.

7 Working with Rulesets

The Event Manager processes alarms in accordance with rulesets. Rulesets provide the Event Manager with instructions on how to process raw event data. Rulesets contain individual rules that provide a set of instructions on parsing and extracting useful information from events.

Use the Event Manager Ruleset Editor to create and validate rulesets. This section provides information on creating, editing, and working with rulesets. Launch the Ruleset Editor through the Event Manager adapter.

7.1 Understanding Rulesets

A ruleset is a text file that describes how the Event Manager agents parse and extract meaningful information from raw text data.

Assign a ruleset to each agent in the network. The ruleset instructs the agent to process any raw data that it receives.

Event Manager rulesets are compatible with BMC Software MAX/Enterprise rulesets. Rulesets created using the MAX/Enterprise ruleset editor can be imported directly into the Event Manager.

Use rulesets to:

- Generate alarms using information such as the alarm description, severity, and priority
- Parse information from incoming events into attributes (standard or user-defined)
- Reformat or embellish terse or cryptic messages to produce more meaningful messages
- Escalate the severity or priority of a message based on the number of messages received, the period of time in which a message was received, or if an operator did not acknowledge the message
- Remove messages that are invalidated by subsequent messages
- Determine a course of action through simple IF/THEN logic
- Identify matches between incoming events and parent and child level rules
- Determine whether an incoming event displays as an alarm or is discarded
- Parse information from an incoming event into variables (system or user-defined)
- Define derived alarm information such as the alarm description, severity, and priority

  Use a component level to identify a failed component or affected resource. Alarms display in the Operations Center console.

- Discard irrelevant messages
- Assign severity to messages
- Delete redundant messages or events

7.2 Importing Rulesets from File or Clipboard

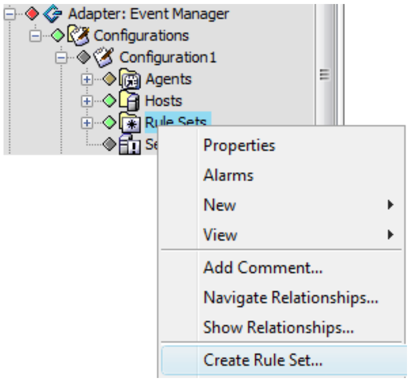
It is possible to import pre-existing ruleset definitions created in the MAX/Enterprise ruleset editor or the Operations Center Event Manager Ruleset Editor.

- Section 7.2.1, “Importing a Ruleset into the Event Manager,” on page 44
- Section 7.2.2, “Importing a Ruleset from a File,” on page 45
- Section 7.2.3, “Importing a Ruleset from the Clipboard,” on page 45
- Section 7.2.4, “Viewing or Editing the Imported Ruleset in the Ruleset Editor,” on page 45

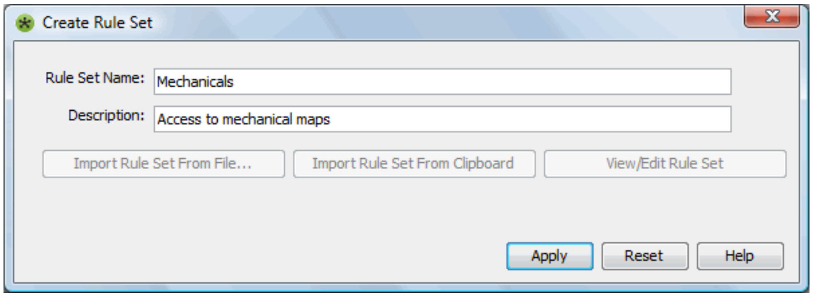
7.2.1 Importing a Ruleset into the Event Manager

To import a ruleset:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a particular configuration.



2 Right-click *Rule Sets*, then select *Create Rule Set* to open the Create Rule Set dialog box:



Rule Set Name: Mechanicals

Description: Access to mechanical maps

3 Specify a name in the *Rule Set Name* field and a description in the *Description* field (optional).

4 Click *Apply*, which activates the ruleset option buttons.

7.2.2 Importing a Ruleset from a File

To import a ruleset from a file:

1. Click *Import Rule Set from File* to open the Please Choose Rule Set Import File dialog box.
2. Browse the directories, then select a ruleset file.
3. Click Open to import the file.

7.2.3 Importing a Ruleset from the Clipboard

To import a ruleset from the clipboard:

1. Click *Import Rule Set From Clipboard*.

   The imported ruleset displays under *Rule Sets* in the *Explorer* pane.

7.2.4 Viewing or Editing the Imported Ruleset in the Ruleset Editor

To view or edit imported rulesets:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a particular configuration > *Rule Sets*.
2. Right-click a ruleset, then select *View/Edit Rule Set* to open the Ruleset Editor.

7.3 Creating and Editing Rulesets

When setting up and using the Event Manager configuration, create and define the necessary rulesets. Access the Ruleset Editor directly through the Operations Center console to create each ruleset.

For information on using the Ruleset Editor, see Section 7.4.1, “Understanding the Ruleset Editor,” on page 47.

IMPORTANT: When logging into the Operations Center console through a Web browser, use the Java Web Start technology to launch Operations Center and the Ruleset Editor. It does not work using a Java plug-in.

The following instructions describe the general process of creating a ruleset:

- Section 7.3.1, “Creating a Ruleset and Launching the Ruleset Editor,” on page 46
- Section 7.3.2, “Editing a Ruleset and Launching the Ruleset Editor,” on page 46

7.3.1 Creating a Ruleset and Launching the Ruleset Editor

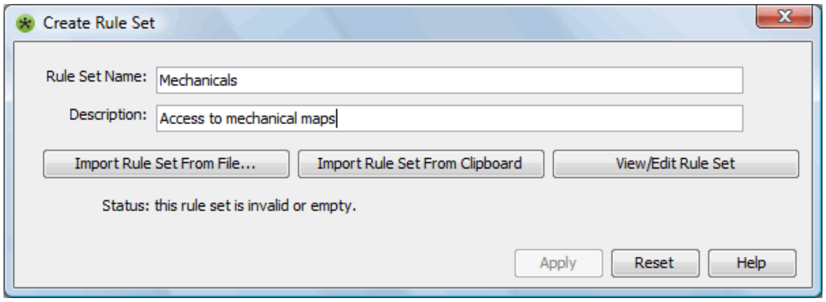
To create a ruleset using the Ruleset Editor:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a particular configuration.

2 Right-click *Rule Sets*, then select *Create Rule Set* to open the Create Rule Set dialog box.

3 Specify the ruleset name in the *Rule Set name* field and a description in the *Description* field.

4 Click *Apply*, which activates the ruleset option buttons.



Rule Set Name: Mechanicals

Description: Access to mechanical maps

Status: this rule set is invalid or empty.

5 Click *View/Edit Rule Set* to create a new ruleset.

The Event Manager Ruleset Editor opens. For more information on using the Ruleset Editor, see Section 7.4.1, “Understanding the Ruleset Editor,” on page 47.

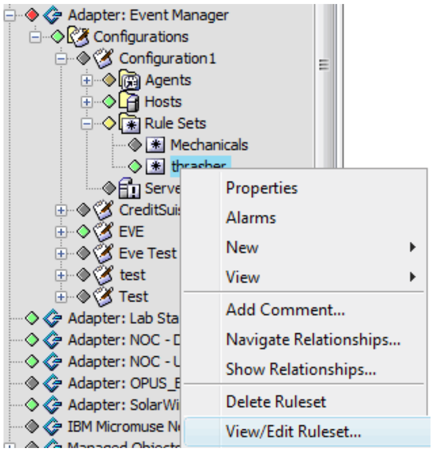
7.3.2 Editing a Ruleset and Launching the Ruleset Editor

To edit a ruleset using the Ruleset Editor:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a particular configuration > *Rule Sets*.

2 Right-click a ruleset, then select *View/Edit Ruleset*.

The Ruleset Editor opens. For information on using the Ruleset Editor, see Section 7.4.1, “Understanding the Ruleset Editor,” on page 47.



The colored diamonds next to the rulesets in the *Explorer* pane identify the condition of the rules within the ruleset:

- Green indicates all rules are valid
- Yellow indicates some rules are invalid
- Gray indicates all rules are invalid

7.4 Defining and Editing Rulesets

Use the Operations Center Event Manager Ruleset Editor to create, edit and manage rulesets. Ruleset files are contained within Operations Center files and can only be accessed through the Event Manager.

Rulesets do not interact with the data source nor do they provide any connectivity or integration points with the data source. Rulesets do provide a customizable approach to handling highly variable raw data streams and the delivery of event management with the Event Manager.

TIP: View instructions for setting up rulesets and how to use the Event Manager Ruleset Editor by selecting the *Help* menu option.

- Section 7.4.1, “Understanding the Ruleset Editor,” on page 47
- Section 7.4.2, “Creating Rules within a Ruleset,” on page 49
- Section 7.4.3, “Creating and Managing Rules,” on page 50
- Section 7.4.4, “Defining and Editing Variables,” on page 56
- Section 7.4.5, “Loading Sample Data,” on page 59
- Section 7.4.6, “Editing the Rule Matching Pane,” on page 61
- Section 7.4.7, “Editing the Rule Parsing Pane,” on page 64
- Section 7.4.8, “Editing the Rule Logic Pane,” on page 66
- Section 7.4.9, “Configuring Alarms,” on page 70
- Section 7.4.10, “Testing Rulesets Using Sample Data,” on page 76
- Section 7.4.11, “Clearing the Ruleset Editor to Create a New Ruleset Definition,” on page 77
- Section 7.4.12, “Exiting the Ruleset Editor,” on page 77

7.4.1 Understanding the Ruleset Editor

The Ruleset Editor directly supports building rulesets and processing raw text.

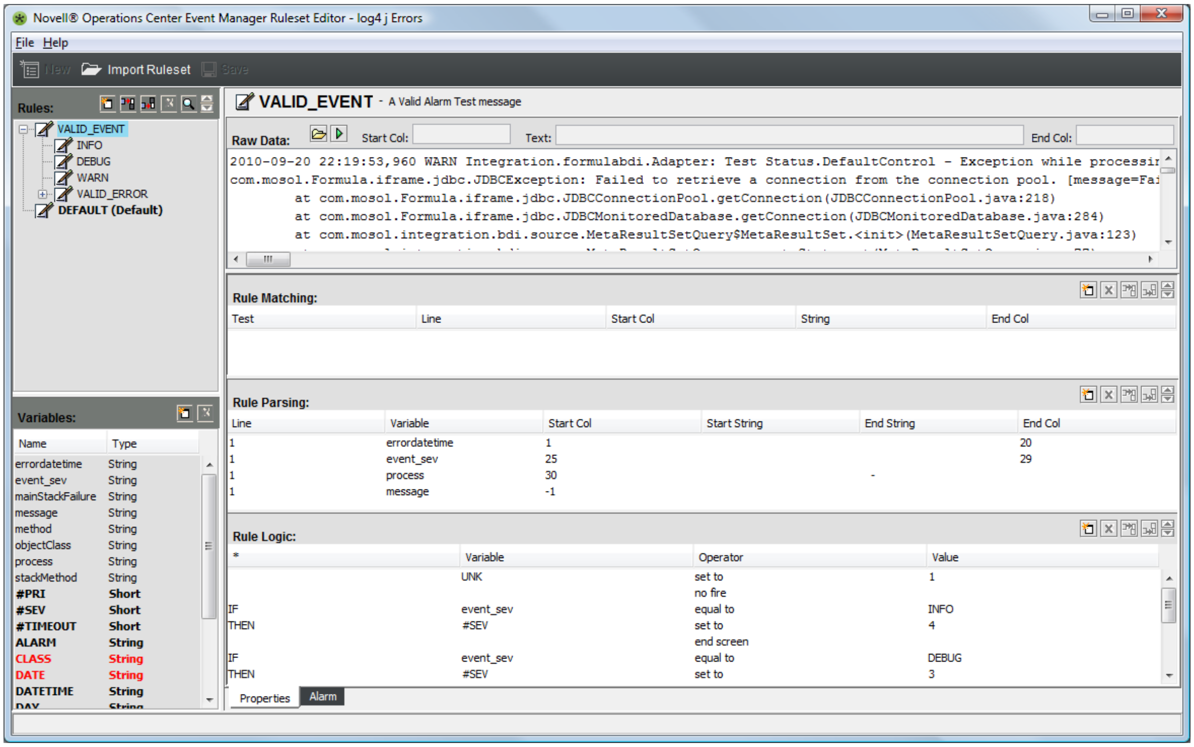
The following topics provide an overview of using the Ruelset Editor tool:

- “Understanding the Ruleset Editor’s Views” on page 48
- “Understanding How the Ruleset Editor Processes Incoming Text” on page 49

Understanding the Ruleset Editor’s Views

The Ruleset Editor consists of a left pane and two tabular views: *Properties* and *Alarm*.

Figure 7-1 *Event Manager Ruleset Editor*



```
2010-09-20 22:19:53,960 WARN Integration.formulabdi.Adapter: Test Status.DefaultControl - Exception while processi
com.mosol.Formula.iframe.jdbc.JDBCException: Failed to retrieve a connection from the connection pool. [message=Fai
        at com.mosol.Formula.iframe.jdbc.JDBCConnectionPool.getConnection(JDBCConnectionPool.java:218)
        at com.mosol.Formula.iframe.jdbc.JDBCMonitoredDatabase.getConnection(JDBCMonitoredDatabase.java:284)
        at com.mosol.integration.bdi.source.MetaResultSetQuery$MetaResultSet.<init>(MetaResultSetQuery.java:123)
```

Rule Matching:

Test	Line	Start Col	String	End Col

Rule Parsing:

Line	Variable	Start Col	Start String	End String	End Col
1	errordatetime	1			20
1	event_sev	25			29
1	process	30		-	
1	message	-1			

Rule Logic:

*	Variable	Operator	Value
	UNK	set to	1
		no fire	
IF	event_sev	equal to	INFO
THEN	#SEV	set to	4
		end screen	
IF	event_sev	equal to	DEBUG
THEN	#SEV	set to	3

Variables:

Name	Type
errordatetime	String
event_sev	String
mainStackFailure	String
message	String
method	String
objectClass	String
process	String
stackMethod	String
#PRI	**Short**
#SEV	**Short**
#TIMEOUT	**Short**
ALARM	**String**
CLASS	**String**
DATE	**String**
DATETIME	**String**
DAY	**String**

The following lists the Ruleset Editor panes:

- **Rules Hierarchy:** A hierarchy tree displays parent and child rules defined for the current ruleset. Select a rule. The data in panes to the right update to reflect the properties for the currently selected rule. This pane displays when either the *Properties* or *Alarm* tab displays.
- **Variables:** A list of reserved system variables and user-defined variables used for parsing and filtering incoming events. System variables display in bold typeface. This pane displays when either the *Properties* or *Alarm* tab displays.
- **Raw Data:** Displays the contents of a selected imported text file. This pane is part of the *Properties* tab.
- **Rule Matching:** Statements that identify specific text strings to match in the incoming data. Incoming lines that contain matching text strings are then processed by statements in the *Rule Parsing* pane. This pane is part of the *Properties* tab.
- **Rule Parsing:** Statements that specify the rules for parsing and storing text from incoming event data in variables defined for the ruleset. This pane is part of the *Properties* tab.
- **Rule Logic:** Statements that evaluate variable values for the incoming events and define actions to perform based on these values. This pane is part of the *Properties* tab.

Understanding How the Ruleset Editor Processes Incoming Text

In the simplest scenario, the following actions occur when the Ruleset Editor processes incoming event data:

1. A selected rule applies to an event message received by the Event Manager.
2. If the message contains text that matches the statements in the *Rule Matching* pane, it is parsed into variables specified in the *Rule Parsing* pane.
3. Statements in the *Rule Logic* pane process the parsed variables.
4. Alarm properties specified in the *Alarm* tab of the Ruleset Editor apply to the event.

   Alarms are sent to the Alarm Server and subsequently to the Operations Center Event Manager adapter.

7.4.2 Creating Rules within a Ruleset

The following steps explain the general process of defining new rules within a ruleset. Subsequent sections explain the details.

The general steps for defining new rules within a ruleset are:

1. In the *Rules Hierarchy* pane, identify the location of the new rule in the hierarchy, then add the rule.

   For more information, see "Understanding Rule Inheritance and Event Processing" on page 50.
2. In the *Rules Hierarchy* pane, define the rule name and description.

   The name can contain spaces, periods, underscores and dashes.

   For more information, see "Adding Rules" on page 51.
3. In the *Variables* pane, define variables that will store some of the parsed incoming raw text.

   For more information, see Section 7.4.4, "Defining and Editing Variables," on page 56.
4. Load sample event data to facilitate the creation and testing of rules.

   For more information, see Section 7.4.5, "Loading Sample Data," on page 59.
5. In the *Rule Matching* pane, identify the text strings to look for in the incoming lines of raw text. Lines with matching text strings are selected for further processing by statements in the *Rule Parsing* pane.

   For more information, see Section 7.4.6, "Editing the Rule Matching Pane," on page 61.
6. In the *Rule Parsing* pane, define statements that parse the incoming event data into variable values.

   For more information, see Section 7.4.7, "Editing the Rule Parsing Pane," on page 64.
7. Define statements in the *Rule Logic* pane. Define statements that evaluate the variable values and perform actions based on these values.

   For more information, see Section 7.4.8, "Editing the Rule Logic Pane," on page 66.
8. In the *Alarm* tab, define alarm properties for events that match all conditions of the selected rule in the *Rules Hierarchy* pane.

   The *Alarm* tab defines the alarms that display in the Operations Center console.

   For more information, see Section 7.4.9, "Configuring Alarms," on page 70.

9 Test rules using sample data.

After defining a new rule, use the *Raw Data* pane to test the rule and make adjustments before putting it into production.

For more information, see Section 7.4.10, “Testing Rulesets Using Sample Data,” on page 76.

7.4.3 Creating and Managing Rules

The rule hierarchy is designed to process events efficiently. The following sections cover aspects of rule inheritance and event processing, as well as outline steps for adding rules, deleting rules, moving rules, and setting a default rule.

- “Understanding Rule Inheritance and Event Processing” on page 50
- “Adding Rules” on page 51
- “Adding Child Rules” on page 51
- “Adding Rules at the Same Level” on page 52
- “Copy, Pasting and Renaming Rules” on page 52
- “Editing a Rule Properties” on page 53
- “Deleting Rules” on page 53
- “Moving Rules” on page 53
- “Defining and Applying a Default Rule” on page 54
- “Changing a Default Rule” on page 55
- “Searching for a Rule” on page 55

Understanding Rule Inheritance and Event Processing

Typically, multiple parents and child level rules process an incoming event. The processing occurs through a branch of the rule tree structure.

If an event successfully matches a parent rule, then all rules that are children of the parent rule process the event.

Each rule can contain one or more statements in the *Rule Matching* pane. If an incoming event matches all the statements in the *Rule Matching* pane, additional processing occurs:

- The *Rule Parsing* pane extracts specific characters in the raw text as named variables

  See Section 7.4.7, “Editing the Rule Parsing Pane,” on page 64.
- Statements in the *Rule Logic* pane evaluate the variable values and perform actions based on these values
- An alarm is generated, unless a rule in the *Rule Logic* pane specifies a *No Fire* action

If an event fails to match a parent rule, parsing and screening do not occur and none of the child rules apply.

Processing from the top-level parent through the lowest-level child stops when one of the following conditions is met:

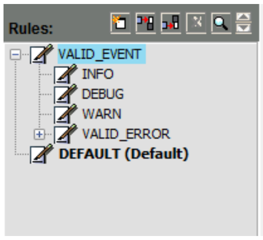
- Rule processing reaches the lowest level in the rule branch
- The incoming data fails to match a statement the *Rule Matching* pane
- A rule in the *Rule Logic* pane specifies not to convert an event to an alarm (a *No Fire* action)

Adding Rules

Define parent and child rules using the tree structure in the *Rules Hierarchy* pane. Child rules display indented beneath their parents.

Figure 7-2 illustrates parent and child rules in the hierarchy tree:

Figure 7-2 *Ruleset Editor*



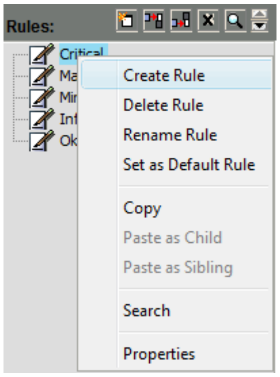
Adding Child Rules

To add a child rule to an existing rule:

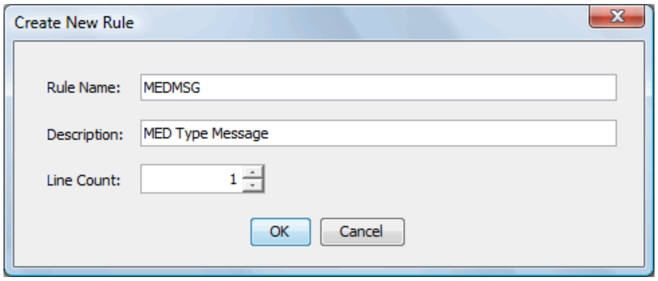
1 Select a rule in the *Rules Hierarchy* pane.

2 To open the Create New Rule dialog box, do one of the following:

- Click (*Add*).
- Right-click a rule, then select *Create Rule*.



3 In the Create New Rule dialog box, specify a name and a description for the new rule:


Create New Rule

Rule Name: MEDMSG

Description: MED Type Message

Line Count: 1

A rule name can consist of any combination of alphanumeric and underscore, space and dash characters, between 1 and 40 characters.

If a rule name that exceeds 37 characters is pasted, the rule name is truncated at 37 characters.

If this rule name is not unique, additional characters are appended until a unique rule name (40 characters or fewer) is created.

The default line count is 1, but can be a number between 1 and 999. The line count is the number of lines in an incoming event.

4. Click *OK*.

   The new rule displays as a child of the currently selected rule. It displays beneath all other child rules in the branch.

   It is possible to move the rule (see “Moving Rules” on page 53) elsewhere within the same branch.

Adding Rules at the Same Level

To add rules at the same level:

1. Select a rule in the *Rules Hierarchy* pane.
2. Click ▣ (*Insert Before*) or ▣ (*Insert After*) to open the Create New Rule dialog box.
3. Specify the Rule Name, Description and Line Count.
4. Click *OK*.

   The new rule displays before or after the currently selected rule, at the same level.

Copy, Pasting and Renaming Rules

It is possible to create new rules from existing rules. Copy and paste an existing rule, then modify it using the *Properties* and *Alarm* tabs.

- “Copying and Pasting a Rule” on page 52
- “Pasting at the Same Level of a Rule” on page 52
- “Renaming a Rule” on page 53

Copying and Pasting a Rule

To copy and paste a rule in the Ruleset Editor:

1. Right-click a rule in the *Rules Hierarchy* pane, then select *Copy*.
2. To paste the rule as a child of another rule, right-click a rule, then select *Paste as Child*.

   A copy of the original rule displays as a child of the selected rule.

Pasting at the Same Level of a Rule

To paste a rule at the same level as another rule in the Ruleset Editor:

1. Right-click a rule, then select *Paste as Sibling*.

   A copy of the original rule displays as a sibling of the selected rule.

Renaming a Rule

To rename a rule in the Ruleset Editor:

1. Right-click the rule, then select *Rename Rule*.
2. Specify the new name.

Editing a Rule Properties

To edit a rule’s description and line count:

1. Right-click a rule, then select *Properties* to open the Edit Rule Properties dialog box.

   Edit the description and line count.
2. Click *OK* to save changes.

Deleting Rules

To delete a rule in the Ruleset Editor:

1. Do one of the following:
   - Select a rule in the *Rules Hierarchy* pane, then click ☒ (*Delete*).
   - Right-click a rule, then select *Delete Rule*.

     This option works only for rules with no children.

Moving Rules

It is possible to change the order that rules display within a branch in the *Rules Hierarchy* pane.

- “Understanding Moving Rules” on page 53
- “Moving a Rule” on page 54

Understanding Moving Rules

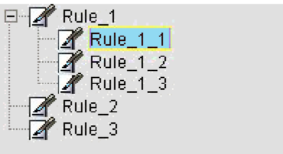
A rule can move only within its current branch. At the top level, a parent rule (and all its children) can move above or below other rules at the same level.

In the following example, Rule_1_1, Rule_1_2 and Rule_1_3 can move within the branch. For example, Rule_1_2 can move above Rule_1_1 or below Rule_1_3. However, none of the rules can move beyond its parent, Rule_1.

At the top level of this example, only Rule_2 and Rule_3 can move. For example, Rule_2 can move above Rule_1 or move below Rule_3. Although Rule_1 cannot move, changing the order of Rule_2 and Rule_3 could cause this to happen inadvertently.

Figure 7-3 illustrates reordering rules within a branch:

Figure 7-3 *Ruleset Editor*



Moving a Rule

To move a rule in the Ruleset Editor:

1 Select a rule, then click ⬍ (*Up* or *Down*) to move the rule.

Only rules with no children can move.

Defining and Applying a Default Rule

Use the default rule to handle unexpected events. Apply it to an event after all the other rules in a ruleset fail to identify a match.

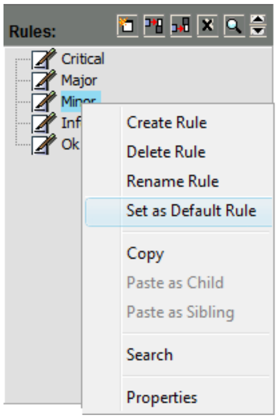
- "Understanding Default Rules" on page 54
- "Defining a Default Rule" on page 55

Understanding Default Rules

The default rule must be at the top level of the rule hierarchy; it has no parent and no children.

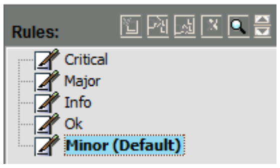
A greyed out option means the rule cannot be the default rule. The rule has children or is not at the top level of the rule hierarchy.

***Figure 7-4** Ruleset Editor: Rule Right-Click Menu*



When selected, the rule name changes to include the text: (Default). The rule moves to the bottom of the rule hierarchy. It is not possible to add new rules after it, or to move existing rules move beneath it.

***Figure 7-5** Ruleset Editor: The default rule is identified.*



Defining a Default Rule

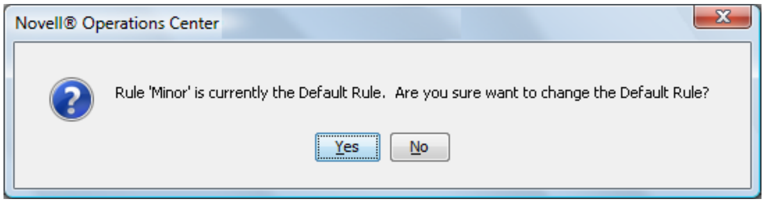
To define a default rule:

1 Right-click a rule, then select *Set as Default Rule*.

Changing a Default Rule

To change the default rule:

1 Right-click a rule, then select *Set as Default Rule* to open the following dialog box:



Rule 'Minor' is currently the Default Rule. Are you sure want to change the Default Rule?

2 Click *Yes* to confirm the change.

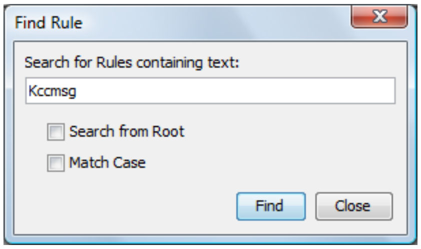
Searching for a Rule

When many rules display in the *Rules Hierarchy* pane, use the Search feature to locate a rule quickly.

To search for a rule:

1 Click 🔍 (*Search*) to open the Find Rule dialog box.

2 Enter search criteria for finding a rule in the *Rules Hierarchy* pane. In the following dialog box, enter the search string:



Search for Rules containing text: Kccmsg

□ Search from Root

□ Match Case

Do the following in this dialog box as necessary:

- To search the entire hierarchy from the top, select the *Search from Root* check box.

  To search the current branch starting from the selected rule, deselect the check box.

  The search includes the current level and lower levels for the current branch only.

- To conduct a case-sensitive search, select the *Match Case* check box.

  To search using any combination of uppercase and lowercase text strings, deselect the check box.

3 Click *Find* to begin the search.

The first rule containing a matching string is selected. If necessary, the search automatically expands the rule hierarchy tree to locate a matching rule.

4 Continue clicking *Find* to locate additional matches.

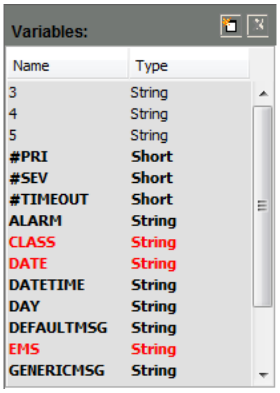
A message displays when there are no more matches.

5 Click *Close* to end the search.

7.4.4 Defining and Editing Variables

The *Variables* pane contains a list of reserved system variables and user-defined variables used to parse and screen incoming events. Variables can consist of text or numbers. System variables display in bold typeface. Variables display in alphabetical order; user-defined variables display first, followed by system variables.

Figure 7-6 *Variables Pane*



Variables:

Name	Type
3	String
4	String
5	String
#PRI	**Short**
#SEV	**Short**
#TIMEOUT	**Short**
ALARM	**String**
CLASS	**String**
DATE	**String**
DATETIME	**String**
DAY	**String**
DEFAULTMSG	**String**
EMS	**String**
GENERICMSG	**String**

The following topics describe how to add and maintain variables:

- "Understanding the System Variables for the Ruleset Editor" on page 56
- "Adding Variables" on page 58
- "Editing Variables" on page 59
- "Deleting Variables" on page 59

Understanding the System Variables for the Ruleset Editor

Table 7-1 lists all system variables currently defined in the Ruleset Editor:

Table 7-1 *Variables*

Variable	Definition	Values
#PRI	Priority of the alarm.	1–99; 1 is the highest priority (Default = 50)
#SEV	Severity of the alarm.	1 = Critical 2 = Major 3 = Minor 4 = Informational (Default) 5 = OK
#TIMEOUT	The time interval (number of minutes) after which an alarm closes automatically.	0–32767 minutes

Variable	Definition	Values
CLASS	The class assigned to the agent from which the event was received.	N/A
DATE	The date that the event was received.	Format is: mm/dd/yyyy, Where: mm (month) is between 01 and 12 dd (day) is between 01 and 31 yyyy (year) is the current year
DATETIME	The date and time that the event was received. When intending to use the Alarm data to set event date/time, be sure that the `usedatetime` custom properties are set correctly. See Section 3.4.3, “Custom Properties Related to Alarm Server Functions,” on page 23.	Format is: yyyy-mm-dd hh:MM:ss Where: yyyy is the current year mm (month) is between 01 and 12 dd (day) is between 01 and 31 hh (hour) is between 00 and 23 MM (minute) is between 00 and 59 ss (second) is between 00 and 59
DAY	The day of the week that the event was received.	Format is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday
EMS	The agent from which the event was received.	N/A
TOD	The time of day that the event message was received.	Format is: hh:mm Where: hh (hour) can be between 00 and 23 mm (minute)can be between 00 and 59

Reserved Words

The following are reserved words and cannot be used when defining variables:

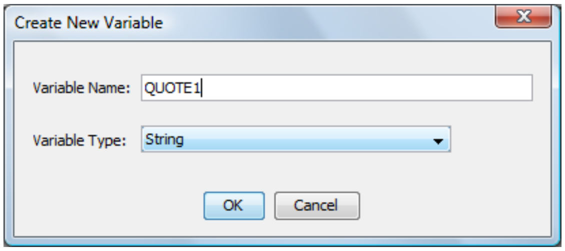
- id
- severity
- date
- accum
- is_assigned
- escalated_up
- escalated_down
- class
- can_escalate
- can_delay
- can_threshold

- can_accumulate
- can_discard
- can_timeout
- ems
- ems_class
- initdate
- assignedto
- enrouteto
- text
- priority
- rule
- group
- circuit
- segment
- object
- hrlt3
- hrlt4
- hrlt5

Adding Variables

To add a variable in the Ruleset Editor:

1 Click (*Add*) in the *Variables* pane to open the Create New Variable dialog box:



Variable Name: QUOTE1

Variable Type: String

2 Specify a name for the new variable.

Variable names must consist of alphanumeric characters (no `spaces) between 1 and 40 characters in length.

3 Click the *Variable Type* drop-down list, then select a variable type: *String*, *Long*, *Short*, or *Float*.

4 Click *OK*.

The new variable displays in the pane in alphabetical order.

Editing Variables

The name of a user-defined variable cannot change. Instead, delete the variable and add a new one. It is also not possible to edit the name or type of a system-defined variable. However, it is possible to change the type of a user-defined variable.

To change the type of a user-defined variable:

In the *Variables* pane, click the *Type* drop-down list next to the variable name, then select one of the following variable types:

String: Any text string.

Long: Any signed 32-bit decimal (-2147483647 to +2147483647).

Short: Any signed 16-bit decimal (-32767 to +32767).

Float: Any valid IEEE 754 32-bit floating point number (3.40282347e+38f to 1.40239846e-45f).

Deleting Variables

It is not possible to delete some system variables. The *Delete* button is dimmed after selecting these variables.

To delete a variable:

1. In the *Variables* pane, select the variable, then click ☒ (*Delete*).

   A dialog box opens to confirm the deletion.
2. Click *Yes* to delete the variable.

7.4.5 Loading Sample Data

Load sample event data to facilitate the creation and testing of rules. When defining rules, select text and identify start and stop columns using the sample event data.

The ▶ (*Test*) button located in the *Raw Data* pane tests the current ruleset using the sample event data. Both of these features are explained later in Section 7.4.10, “Testing Rulesets Using Sample Data,” on page 76.

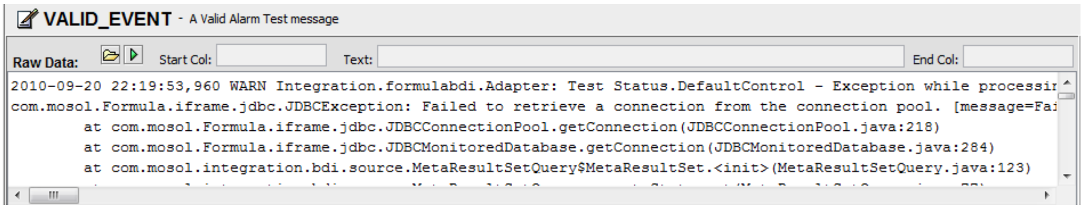
- “Loading a Text File Containing Sample Data” on page 60
- “Copying Raw Data to Other Panes” on page 60

Loading a Text File Containing Sample Data

To load a text file that contains sample data:

1. In the *Raw Data* pane, click 📂 (*Open*).
2. Browse and select a data file.

   The file content displays in the *Raw Data* pane:



```
2010-09-20 22:19:53,960 WARN Integration.formulabdi.Adapter: Test Status.DefaultControl - Exception while processir
com.mosol.Formula.iframe.jdbc.JDBCException: Failed to retrieve a connection from the connection pool. [message=Fai
        at com.mosol.Formula.iframe.jdbc.JDBCConnectionPool.getConnection(JDBCConnectionPool.java:218)
        at com.mosol.Formula.iframe.jdbc.JDBCMonitoredDatabase.getConnection(JDBCMonitoredDatabase.java:284)
        at com.mosol.integration.bdi.source.MetaResultSetQuery$MetaResultSet.<init>(MetaResultSetQuery.java:123)
```

   This text is read-only.

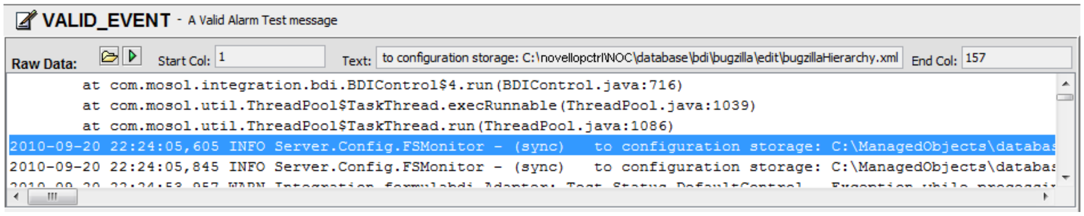
3. Do any of the following:
   - Use the vertical scroll bar to view additional rows of sample data.
   - Use the horizontal scroll bar to view additional data on a line.

Copying Raw Data to Other Panes

To minimize data entry errors, copy text strings and the start and end column numbers from the sample raw data to fill in cells in the *Rule Matching*, *Rule Parsing*, and *Rule Logic* panes.

To copy the raw data:

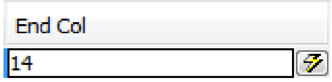
1. Click and drag to select information in the *Raw Data* pane.
2. Confirm the selection by checking the status bar of the *Raw Data* pane, which displays the selected start, text, and end columns:



Start Col: 1 Text: to configuration storage: C:\novellopctrl\NOC\database\bdi\bugzilla\edit\bugzillaHierarchy.xml End Col: 157

```
        at com.mosol.integration.bdi.BDIControl$4.run(BDIControl.java:716)
        at com.mosol.util.ThreadPool$TaskThread.execRunnable(ThreadPool.java:1039)
        at com.mosol.util.ThreadPool$TaskThread.run(ThreadPool.java:1086)
2010-09-20 22:24:05,605 INFO Server.Config.FSMonitor - (sync)   to configuration storage: C:\ManagedObjects\databas
2010-09-20 22:24:05,845 INFO Server.Config.FSMonitor - (sync)   to configuration storage: C:\ManagedObjects\databas
```

3. In the *Rule Matching*, *Rule Parsing*, or *Rule Logic* pane, select the cell to paste the information.
4. Click the ⚡ (lightning bolt icon) next to the cell to paste the information.



End Col: 14

7.4.6 Editing the Rule Matching Pane

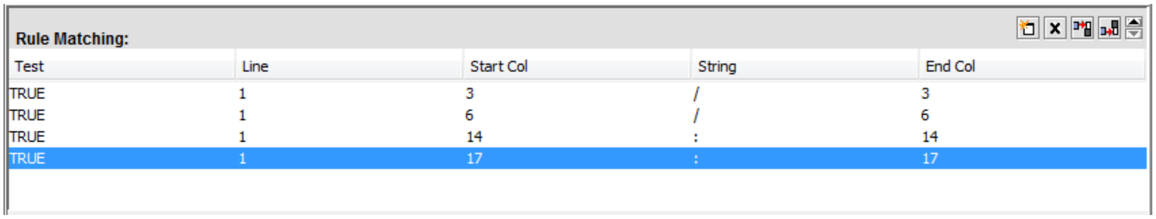
Statements in the *Rule Matching* pane evaluate specific sections of the incoming data for string matches. String matches are based on user-defined text strings and the start and end columns of the incoming data. Incoming data with string matches that meet the True or False criteria specified by the Rule Matching statements are further processed by statements in the *Rule Parsing* pane.

- “Understanding the Rule Matching Pane” on page 61
- “Adding Statements” on page 62
- “Moving Statements” on page 62
- “Editing Rule Matching Columns” on page 63
- “Copying and Pasting Statements” on page 63
- “Deleting Statements” on page 64

Understanding the Rule Matching Pane

In Figure 7-7, each statement searches for a single character.

Figure 7-7 *Ruleset Editor: Rule Matching Pane*

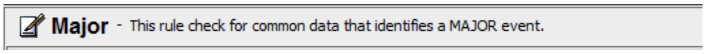


Rule Matching:

Test	Line	Start Col	String	End Col
TRUE	1	3	/	3
TRUE	1	6	/	6
TRUE	1	14	:	14
TRUE	1	17	:	17

Before editing the *Rule Matching* pane, select the appropriate rule in the *Rules Hierarchy* pane. The title bar displays the currently selected rule name and description:

Figure 7-8 *Ruleset Editor - The Title Bar Identifies the Current Rule.*



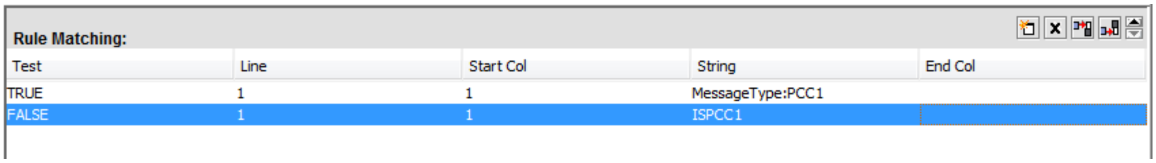
Major - This rule check for common data that identifies a MAJOR event.

The *Rule Matching* pane can contain one or more rows automatically joined by the AND operator. Multiple statements mean incoming events must match all the specified criteria.

Specifying a *Start and End Column* value is not required. A blank in these columns instructs the search to start at the beginning of a line and finish at the end of a line.

In the following example, the matching events must contain the string MessageType:PCC1, but must not contain the string ISPCC1. There is no *End Column* value, so the search ends at the last column of the line.

Figure 7-9 *Ruleset Editor: Rule Matching pane with both True and False search strings*



Rule Matching:

Test	Line	Start Col	String	End Col
TRUE	1	1	MessageType:PCC1	
FALSE	1	1	ISPCC1	

Adding Statements

- "Adding a Statement at the Bottom of the Rule Matching Pane" on page 62
- "Adding a Statement Beneath the Currently Selected Statement" on page 62
- "Adding a Statement Above the Currently Selected Statement" on page 62

Adding a Statement at the Bottom of the Rule Matching Pane

To add a statement at the bottom of the Rule Matching Pane:

1 Click (*Add*) in the *Rule Matching* pane.

A new row displays.

2 Specify the match statement in the new row.

Adding a Statement Beneath the Currently Selected Statement

To add a statement beneath the currently selected statement:

1 Click (*Insert After*).

A new row displays beneath the current row.

TIP: Be aware that clicking a cell in a row can automatically place it in an edit mode.

Adding a Statement Above the Currently Selected Statement

To add a statement above the currently selected statement:

1 Click (*Insert Before*).

A new row displays above the current row.

Moving Statements

To move a statement within the pane:

1 Select a statement.

2 Click (*Up* or *Down*) to move the statement.

Editing Rule Matching Columns

Table 7-2 provides a description of each column in the *Rule Matching* pane:

Table 7-2 *Rule Matching Columns*

Column	Value	Description
Test	True (Default)	Rule fires if the event message contains the text specified between the start and end columns.
	False	Rule fires if the event message does not contain the text specified between the start and end columns.
Line	1–999	The target line to search for a match in the event data. The default is 1. If the line count for the associated rule is greater than 1, select a different number from the drop-down list. If the line count for the rule equals 1, do not change this value.
Start Column	1–999	The position in the specified line where the string search begins. If this column is blank, the search begins at the first column of the line.
String	Any characters	The exact text found (True) or not found (False) in the event message. Trailing spaces are not trimmed and are represented using the space character (““).
End Column	1–999	The position in the specified line where the string search ends. If this column is blank, the search ends at the last column of the line.

Copying and Pasting Statements

- “Copying a Statement” on page 64
- “Pasting a Statement Above or Below an Existing Statement” on page 64
- “Pasting the Statement at the End of the Pane” on page 64

Copying a Statement

To copy a statement:

1. Right-click a statement, then select *Copy*.

Pasting a Statement Above or Below an Existing Statement

To paste a statement:

1. Right-click any location in the row, then select *Paste Before* or *Paste After*.

Pasting the Statement at the End of the Pane

To paste a statement at the end of the pane:

1. Right-click any location in the bottom section of the pane that is not part of a row, then select *Paste*.

Deleting Statements

To delete a statement:

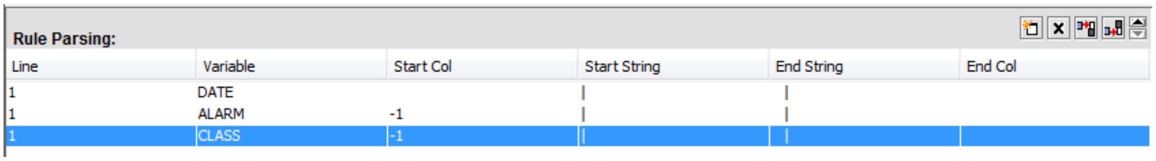
1. Select the row, then click ☒ (*Delete*) to open a dialog box where you can confirm the deletion.
2. Click *Yes* to delete the statement.

7.4.7 Editing the Rule Parsing Pane

The *Rule Parsing* pane specifies how to parse and store the incoming event data in variables defined for the ruleset. Be sure to define variables in the *Variables* pane before editing the *Rule Parsing* pane.

In Figure 7-10, the Ruleset Editor parses the string "|"into the variables named DATE, ALARM, and CLASS.

Figure 7-10 *Ruleset Editor: Parse strings using relative start columns.*



Rule Parsing:

Line	Variable	Start Col	Start String	End String	End Col
1	DATE		|	|	
1	ALARM	-1	|	|	
1	CLASS	-1	|	|	

It searches the entire incoming line for the string because no start or end column is specified.

Subsequent parsing depends on the location of the first parsed variable by defining a *Start Column* value of `-1` which specifies that the search begins after the last parsed column.

- "Adding Statements" on page 65
- "Moving Statements" on page 65
- "Editing the Rule Parsing Pane" on page 65
- "Copying and Pasting Rule Parsing Statements" on page 65
- "Deleting Statements" on page 66

Adding Statements

See “Adding Statements” on page 62.

Moving Statements

See “Moving Statements” on page 62.

Editing the Rule Parsing Pane

Table 7-3 provides a description of each column in the *Rule Parsing* pane:

Table 7-3 *Rule Parsing Columns*

Column	Value	Description
Line	1–999	The target line to search for a match in the event data. The default is 1. If the line count for the associated rule is greater than 1, select a different number from the drop-down list. If the line count for the rule equals 1, do not change this value.
Variable	Select from a drop-down list	The variable in which to store the parsed value specified by the start/ end strings and columns. Select a variable from the drop-down list. The variables are defined using the *Variable* pane on the left side of the Ruleset Editor.
Start Column	1–999; -1	The position in the specified line where the string search begins. If this column is blank, the search begins at the first column of the line. –1 indicates the search starts in the position after the last parsed column.
Start String	Any characters	The exact text found in the event message beginning with at the start column. Trailing spaces are not trimmed and are represented using the space character (““).
End Column	1–999; -1	The position in the specified line where the string search ends. If this column is blank, the search ends at the last column of the line. –1 indicates the search ends in the position after the last parsed column.
End String	Any characters	The exact text found in the event message, starting at the specified end column. Trailing spaces are not trimmed and are represented using the space character (““).

To minimize data entry errors, copy text strings and the start and end column numbers from sample event data to fill in cells in the *Rule Parsing* pane.

For more information, see “Copying Raw Data to Other Panes” on page 60.

Copying and Pasting Rule Parsing Statements

See “Copying and Pasting Statements” on page 63 for details.

Deleting Statements

To delete a statement in the *Rule Parsing* pane:

1. Select the statement, then click ☒ (*Delete*) to open a dialog box where you can confirm the deletion.
2. Click *Yes* to delete the statement.

7.4.8 Editing the Rule Logic Pane

Statements in the *Rule Logic* pane apply logic to incoming events that match the statements in the *Rule Matching* pane. IF/THEN comparison statements can screen incoming events based on variable values and perform actions such as not firing an alarm, assigning variable values or resetting variable values.

- “Adding Statements” on page 66
- “Moving Statements” on page 66
- “Editing Rule Logic Column” on page 66
- “Copying and Pasting Rule Logic Rows” on page 67
- “Using Set To and Un-set Operators” on page 67
- “Constructing Comparison Statements” on page 69
- “Using No Fire and End Screen Statements” on page 70

Adding Statements

See “Adding Statements” on page 62.

Moving Statements

See “Moving Statements” on page 62.

Editing Rule Logic Column

Table 7-4 provides a description of each column in the *Rule Logic* pane:

***Table 7-4** Rule Logic Columns*

Column	Value	Description
*	Filled in automatically, depending on contents of other columns	A read-only column used to show the logic flow represented by the rows in the pane. This column is automatically filled in as rows are added and removed from the pane. The possible values are: ◆ **Blank:** When the Set To, No Fire, End Screen, or Un-set operator is used and the previous row is not a comparison. ◆ **IF:** The first row in a series of comparison rows. ◆ **AND:** All subsequent comparison rows. ◆ **THEN:** All assignments (Set to, No Fire, End Screen, or Un-set) following an IF/AND statement.

Column	Value	Description
Variable	Select from a drop-down list	The variable to change or test using an operator. Select a variable from the drop-down list. The variables are defined using the Variables pane.
Operator	Select from a drop-down list	Comparison operators that require an operand: ◆ Equal to ◆ Not equal to ◆ Less than ◆ Less than or Equal to ◆ Greater than ◆ Greater than or Equal to ◆ Contains Action operators: ◆ No Fire ◆ End Screen ◆ Set-to ◆ Un-set
Value	Alphanumeric characters	The variable value to test using a comparison operator.

To minimize data entry errors:

1. Copy text strings and the start and end column numbers from sample event data to fill in cells in the *Rule Parsing* pane.

   For more information, see "Copying Raw Data to Other Panes" on page 60.

Copying and Pasting Rule Logic Rows

It is possible to copy and paste rows in the *Rule Logic* pane. For more information, see "Copying and Pasting Statements" on page 63.

Using Set To and Un-set Operators

The Set To operator assigns variable values, do the following:

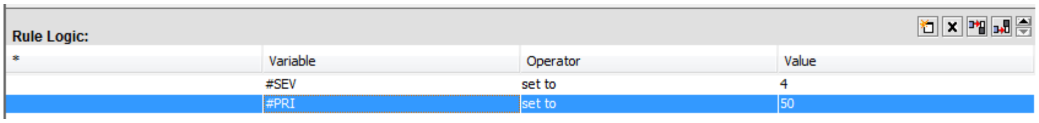
- "Assigning the Set To Operator" on page 68
- "Using the Un-Set Operator" on page 68
- "Using an Alternative Method of Applying the Set To or Un-Set Operator" on page 68

Assigning the Set To Operator

To assign the Set To operator to a variable:

1. Select a variable in the *Variable* column.
2. Select *Set To* in the *Operator* column.
3. Enter the new value for the variable in the *Value* column.

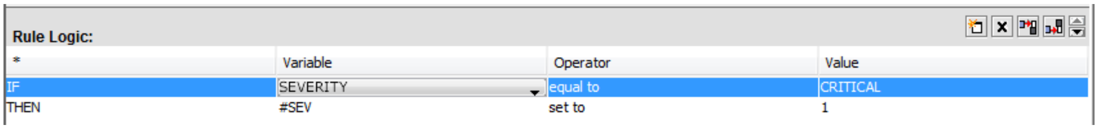
   The following example sets the severity and priority numerical values for events that match the statements in the *Rule Matching* pane:



Rule Logic:

*	Variable	Operator	Value
	#SEV	set to	4
	#PRI	set to	50

If one variable value depends on another variable value, use the *Set To* operator in conjunction with an IF/THEN comparison statement. In the following example, the #SEV value is set to 1 if the *Severity* code equals CRITICAL:



Rule Logic:

*	Variable	Operator	Value
IF	SEVERITY	equal to	CRITICAL
THEN	#SEV	set to	1

Using the Un-Set Operator

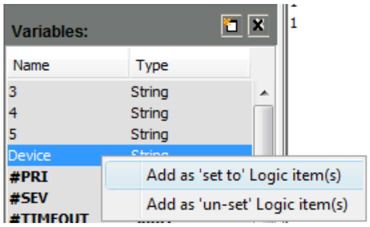
To assign the Un-Set operator to a variable:

1. Select a variable in the *Variable* column.
2. Select *Un-set* in the *Operator* column.

Using an Alternative Method of Applying the Set To or Un-Set Operator

To assign the set to or the Un-Set operator to a variable using an alternative method:

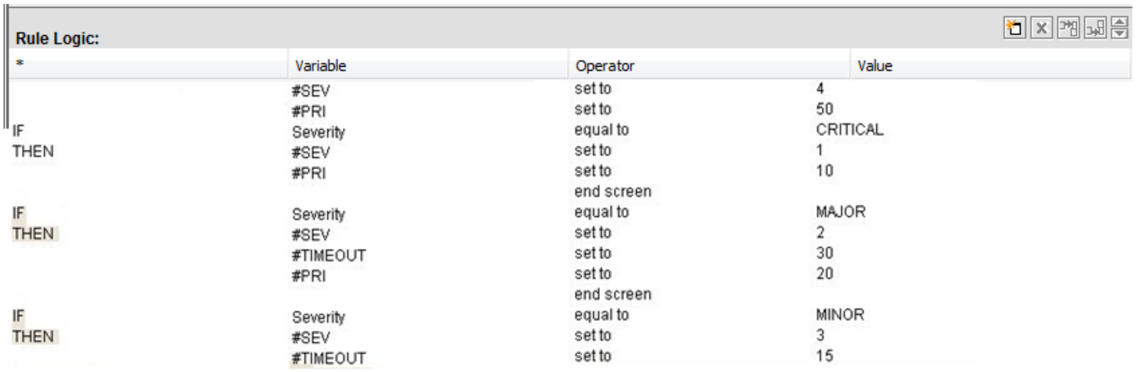
1. Right-click a variable in the *Variables* pane.
2. Select *Add As Set to Logic Items* or *Add As Un-set Logic Items*:



Variables:

Name	Type
3	String
4	String
5	String
Device	String
#PRI	
#SEV	
#TIMEOUT	

3 Select *Add as Un-set Logic items* and the new statement displays in the *Rule Logic* pane:

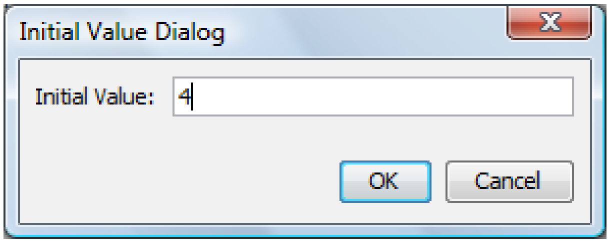


Rule Logic:

*	Variable	Operator	Value
	#SEV	set to	4
	#PRI	set to	50
IF	Severity	equal to	CRITICAL
THEN	#SEV	set to	1
	#PRI	set to	10
		end screen	
IF	Severity	equal to	MAJOR
THEN	#SEV	set to	2
	#TIMEOUT	set to	30
	#PRI	set to	20
		end screen	
IF	Severity	equal to	MINOR
THEN	#SEV	set to	3
	#TIMEOUT	set to	15

4 Select *Add as 'set to' Logic items* and the following dialog box prompts for an initial value to use as the variable, specify the value to assign to that variable, then click *OK*.

This assignment displays in a new row in the *Rule Logic* pane:



Initial Value Dialog

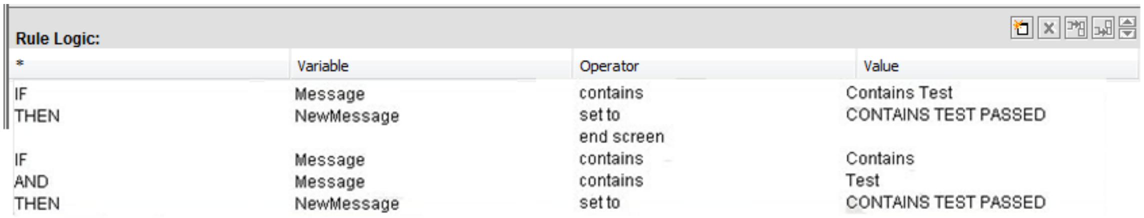
Initial Value: 4

Constructing Comparison Statements

Use IF/THEN comparison statements to test the values of particular variables of incoming events. The actions can consist of assigning values to specific variables or not firing an alarm for an event (No Fire). Use the End Screen operator (explained in the next section) to separate IF/THEN comparison statements.

In Figure 7-11, multiple IF/THEN statements assign #SEV and #PRI values based on the severity code value.

Figure 7-11 *Ruleset Editor: IF/THEN statements assign variable values.*



Rule Logic:

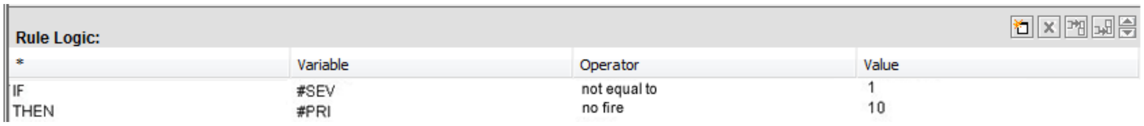
*	Variable	Operator	Value
IF	Message	contains	Contains Test
THEN	NewMessage	set to	CONTAINS TEST PASSED
		end screen	
IF	Message	contains	Contains
AND	Message	contains	Test
THEN	NewMessage	set to	CONTAINS TEST PASSED

Using No Fire and End Screen Statements

Ruleset hierarchy is designed to process events efficiently. If a parent rule does not identify an event or instructs a No Fire action through screening logic in the *Rule Logic* pane, then none of its child rules are used. In some situations, it is desirable to perform a No Fire action (do not fire the alarm) to exclude peripheral or unwanted events.

The statements in Figure 7-12 specify that if the value of the #SEV variable is not equal to 1, then do not fire an alarm for the event.

Figure 7-12 *Ruleset Editor: No alarm is fired for events whose #SEV value does not equal 1.*



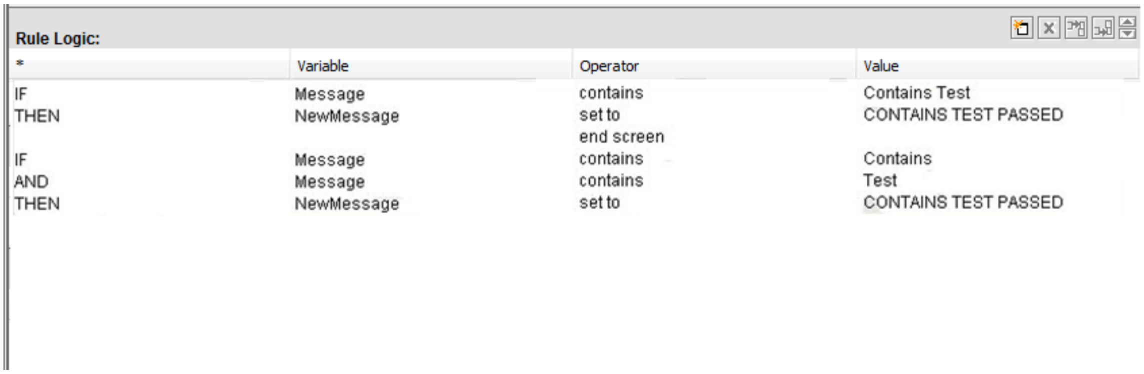
Rule Logic:

*	Variable	Operator	Value
IF	#SEV	not equal to	1
THEN	#PRI	no fire	10

Use the End Screen operator by itself, with no values in the *Variable* or *Value* column. End Screen separates multiple IF/THEN comparison statements. In most situations, when an event tests True for an IF statement, a THEN action occurs and nothing else should happen. Place End Screen after the THEN statement to prevent further processing of the event by subsequent IF/THEN comparison statements.

In Figure 7-13, the first comparison statement checks for the string "Contains Test." If it exists, the THEN statement sets the NewMessage variable to "CONTAINS TEST PASSED". The End Screen operator halts further processing of the event if it tests True; the second comparison statement does not apply.

Figure 7-13 *Ruleset Editor: The End Screen operator is used to separate condition statements.*



Rule Logic:

*	Variable	Operator	Value
IF	Message	contains	Contains Test
THEN	NewMessage	set to	CONTAINS TEST PASSED
		end screen	
IF	Message	contains	Contains
AND	Message	contains	Test
THEN	NewMessage	set to	CONTAINS TEST PASSED

After completing the *Rule Logic* pane, the next step is to set up the rules for generating alarms in the *Alarm* tab. Refer to next section for details.

7.4.9 Configuring Alarms

In the *Alarm* tab, define alarm properties for events that match all conditions of the selected rule in the *Rules Hierarchy* pane. The *Alarm* tab defines the alarms that display in the Operations Center console.

- "Configuring the Alarms Generated by Incoming Events" on page 71
- "Editing the Generated Alarm Text Strings" on page 71

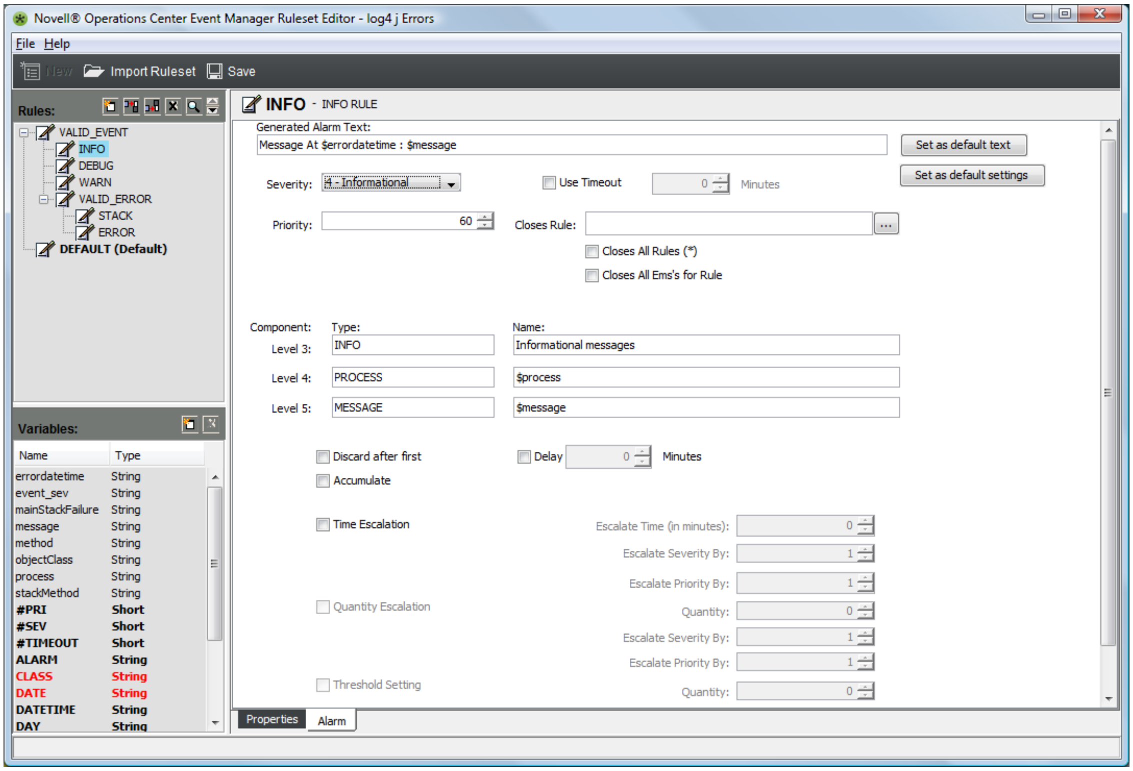
- “Editing the Component Level Section” on page 74
- “Editing Alarm Display Options” on page 74

Configuring the Alarms Generated by Incoming Events

To configure the alarms generated by incoming events that meet the criteria specified in the *Rule Matching* pane:

1 Select a rule in the *Rules Hierarchy* pane.

2 Click the *Alarm* tab in the Ruleset Editor to display the *Alarm* tab:



Generated Alarm Text: Message At $errordatetime : $message

Severity: 4 - Informational

☐ Use Timeout 0 Minutes

Priority: 60

Closes Rule:

☐ Closes All Rules (*)

☐ Closes All Ems's for Rule

Component:	Type:	Name:
Level 3:	INFO	Informational messages
Level 4:	PROCESS	$process
Level 5:	MESSAGE	$message

☐ Discard after first

☐ Delay 0 Minutes

☐ Accumulate

☐ Time Escalation

Escalate Time (in minutes): 0

Escalate Severity By: 1

Escalate Priority By: 1

☐ Quantity Escalation

Quantity: 0

Escalate Severity By: 1

Escalate Priority By: 1

☐ Threshold Setting

Quantity: 0

Name	Type
errordatetime	String
event_sev	String
mainStackFailure	String
message	String
method	String
objectClass	String
process	String
stackMethod	String
#PRI	**Short**
#SEV	**Short**
#TIMEOUT	**Short**
ALARM	**String**
CLASS	**String**
DATE	**String**
DATETIME	**String**
DAY	**String**

The remaining subsections explain these settings.

Editing the Generated Alarm Text Strings

The *Generated Alarm Text* field specifies the alarm description that displays for the generated alarms in the Operations Center console.

TIP: To exit the *Variables* drop-down list without selecting a variable, press the Esc key or the spacebar.

- “Specifying the Text for Alarms” on page 72
- “Adding a Ruleset Variable” on page 72
- “Displaying the Current Generated Alarm Text” on page 72
- “Saving the Current Alarm Settings as the Default for All New Rules” on page 72

Specifying the Text for Alarms

To specify the text for alarms generated for events that match the selected rule:

In the *Generated Alarm Text* field, enter a text string or enter one or more ruleset variables.

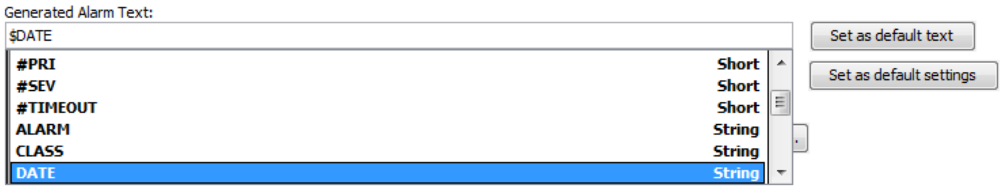
Adding a Ruleset Variable

To add a ruleset variable:

1. Enter the prefix $, followed by the variable name.

   For example, enter $DATE to display the DATE string.

   After typing $, a drop-down list of variables displays, to save time and minimize typing errors.



Generated Alarm Text: $DATE

#PRI	Short
#SEV	Short
#TIMEOUT	Short
ALARM	String
CLASS	String
DATE	String

2. Select a variable by double-clicking it, then press the Tab or Enter key.

Displaying the Current Generated Alarm Text

To display the text currently displayed in the *Generated Alarm Text* field as the default text for all future new rules:

1. Click *Set as Default Text*.

   A dialog box asks to confirm setting the text as the default for all future rules.

2. Click *Yes* to confirm.

   It is possible to override the default text by editing the *Generated Alarm Text* field subsequent rules.

Saving the Current Alarm Settings as the Default for All New Rules

To save the current alarm settings as default settings for all new rules:

1. Click *Set as Default Settings*.
2. Define the following options under *Generated Alarm Text*:

   Severity: Defines the severity level of the alarm, which can range from 1 (highest severity) to 5 (lowest severity).

   Priority: Defines the criticality and functional responsibility level of the alarm. The priority assignment can range from 1 (highest) to 99 (lowest).

   Use Timeout: Select this check box to automatically close the alarm after the specified number of minutes. If the check box is deselected, the active alarm never times out. If the check box is selected and set to 0, then all alarms, active or delayed, are closed, provided they meet any *Closes Rule* parameters. A new alarm is not created nor is any other alarm processing performed.

   - For nondelayed alarms, the timeout time is the initial event time + x minutes.
   - For delayed alarms and threshold alarms, the timeout is the time the alarm became active + x minutes.

- For active accumulated alarms, the timeout is reset to the time of the latest accumulating event + x minutes.
- For discarded alarms, the active alarm timeout time is not updated when matching events are discarded.

Closes Rule: One rule might close another, thereby closing all alarms triggered by the second rule. For example, RULE A closes RULE B, thereby closing all alarms triggered by RULE B.

The *Closes Rule* drop-down list is read-only. Click the "…" button to the right to select a rule from the *Rules Hierarchy* pane. In addition, the following options are available:

- **Closes All Rules(*):** Select this check box and the rule closes all alarms, active or delayed, fired by any other rule that has a matching EMS, HRL3, HRL4, and HRL5, regardless of rule name. (It ignores the rule name. HRL represents Hierarchy Resource List.)

  TIP:

  EMS = Event Manager Agents
  HRL3 = host
  HRL4 = source
  HRL5 = sub_source

- **Closes All EMSs for Rule:** Select this check box and the rule closes all alarms, active or delayed, fired by the rule under any EMS that has the same HRLs, except for HRLT2 and HRLN2.

If both the *Closes All Rules(*)* and the *Closes All EMSs for Rule* check boxes are selected, the rule closes all alarms fired by anything that has matching HRL3, HRL4, and HRL5 values. Both the rule name and HRL2 are ignored.

Currently there is an issue with the $EMS parameter setting in the Event Manager Agent that does not allow setting the $EMS globally. To work around this issue, the EMS class defined when the agent is created is used (instead of $EMS) for this function.

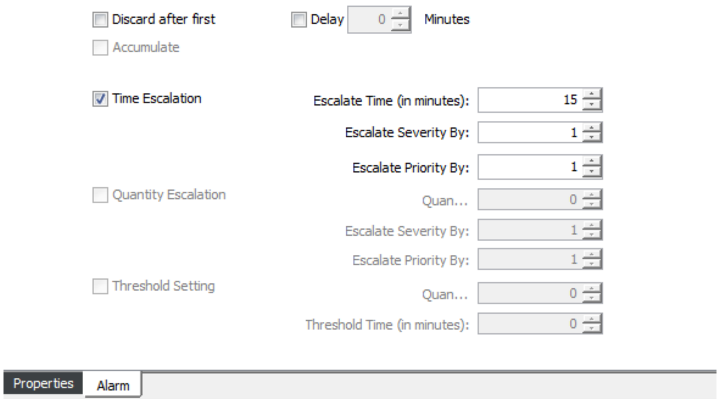
Editing the Component Level Section

The *Component Level* section of the *Alarm* tab identifies the resource or component that generated the event. The *Type* field defines the category of the component. The Name is the specific component.

To enter a variable name in the *Type* or *Name* field, Enter $ and select from a list of variables.

Editing Alarm Display Options

The following options in the *Alarm* tab define the details of alarm display:



☐ Discard after first

☐ Delay 0 Minutes

☐ Accumulate

☑ Time Escalation

Escalate Time (in minutes): 15

Escalate Severity By: 1

Escalate Priority By: 1

☐ Quantity Escalation

Quan... 0

Escalate Severity By: 1

Escalate Priority By: 1

☐ Threshold Setting

Quan... 0

Threshold Time (in minutes): 0

Ruleset Editor: Escalate alarm severity and priority using time, quantity, and thresholds factors.

The following describes the Alarm display options on the *Alarm* tab:

- **Discard after first:** When selected, discards duplicate alarms. No other alarm processing is performed. Selecting this check box disables the *Quality* and *Threshold Setting* fields. Discard and Accumulate cannot both be True. If Discard is True, then Accumulate is evaluated as False.
- **Delay:** When selected, postpones the creation of an alarm for x minutes. Alarms do not display in the Alarms view until the specified time interval (in minutes) elapses. A delayed alarm can be closed by another event before it becomes active. The time interval is the time the alarm became active + x minutes. and is independent of all other fields in the *Alarm* tab. After the alarm is created, normal event processing applies as for all other alarms.
- **Accumulate:** When selected, duplicate alarms do not display as new alarms in the Alarms view. An active alarm is updated every time an event with a matching rule name and HRL is processed. Discard must be False in order for Accumulate to be evaluated.

  An accumulation counter is updated by N + 1 each time an alarm is accumulated. The timeout time is reset to the time of the latest accumulating event + x minutes. The alarm’s initial date and time is set to the date and time that the first alarm was created and its most recent date and time is set to the date and time that the alarm was last accumulated. The alarm’s date and time in Operations Center is the most recent date and time. Selecting this check box activates the *Time*, *Quantity* and *Threshold Setting* check boxes.

  Accumulated alarms that have escalated/de-escalated will not have their severity or priority properties updated.

- **Time Escalation:** If an alarm has been active for the specified number of minutes since the initial date and time, then increase or decrease the severity and/or priority by a rule-determined threshold amount until the upper or lower limit is reached. This is done for each multiple (nx) of the threshold time. Accumulating alarms that have time escalated/de-escalated no longer have their severity or priority properties updated.

  Selecting the *Time Escalation* check box enables the following spinners to the right of the check box:

  Escalate Time (in minutes)
  Escalate Severity By
  Escalate Priority By

  Use the *Escalate Time* spinner to select the interval in which the severity and priority levels escalate.

  For example, specify 5 minutes for Time Escalation, 1 for Severity Interval and 1 for Priority Escalation. Assume an event creates a MINOR active alarm with the counter set to 1 and a priority of 50. When the alarm has been active for 5 (x) minutes, the alarm severity increases to MAJOR and the priority increases to 49. (Note that a lower priority number is actually a higher priority.)

  When the alarm has been active for 10 minutes (2x), the alarm severity increases to CRITICAL and the priority increases to 48. The same behavior occurs for each nx increment, except that the severity remains CRITICAL because it cannot go any higher. Severities can go no higher than CRITICAL nor lower than INFO via escalation.

  The valid range of values for Escalate Severity is: 0–3; -1, -2, -3. Select a negative number to decrease severity.

  The valid range of values for Escalate Priority is: 0–99; -1 to -99. Select a negative number to decrease priority.

- **Quantity Escalation:** The alarm severity and priority escalate depending on the number of alarm occurrences. Select the *Accumulate* check box to enable Quantity Escalation.

  Selecting the *Quantity Escalation* check box enables the following spinners:

  Quantity
  Escalate Severity By
  Escalate Priority By

  Use the Quantity spinner to select the number of alarm occurrences that trigger the severity and/or priority escalation. The valid range of values is: 0 – 9,999.

  The definitions and valid values for Escalate Severity and Escalate Priority are the same as for Time Escalation.

  For example, set Quantity Escalation equal to 5, Escalate Severity By to 1, and Escalate Priority By to 1. Assume an event creates a MINOR active alarm with the accumulation counter set to 1 and a priority of 50. With subsequent alarms and the accumulation counter between 1 and 4, no change occurs to alarm severity or priority.

  When the accumulation counter increments to 5 (x), the alarm severity increases to MAJOR and the priority is increased to 49. (Lower priority number is actually a higher priority.)

  With subsequent alarms and the accumulation counter less than 10, no change occurs to alarm severity or priority. When the accumulation counter increments to 10 (2x), the alarm severity increases to CRITICAL and the priority increases to 48. The same behavior occurs for the next increment of 5 alarms, except that the severity remains CRITICAL because it cannot go any higher.

  Severities can go no higher than CRITICAL nor lower than INFO via escalation. Priorities can go no higher than 1 nor lower than 99 with escalation.

- **Threshold Setting:** If the *Accumulate* check box is selected, the alarm count does not advance until the alarm fires a specific number of times (*Quantity*) within a specific number of minutes (*Threshold Time*). Select the *Threshold Setting* check box, then use the *Quantity* and *Threshold Time* spinners.

  If the Alarm server receives an event with the threshold set and there is a matching active alarm, normal event processing related to an active alarm takes place. If there is no matching active alarm, events are kept in a pending state and evaluated on a sliding time scale each time a new event arrives. An alarm is created if the number of events matches the quantity threshold within the past threshold time (in minutes). The alarm accumulation count is set to the quantity threshold setting.

  Note that *Delay* and *Threshold Setting* are mutually exclusive, with *Threshold* taking precedence if both are set.

  Threshold events are evaluated when the Alarm server receives them and older pending events falling outside the time threshold are discarded.

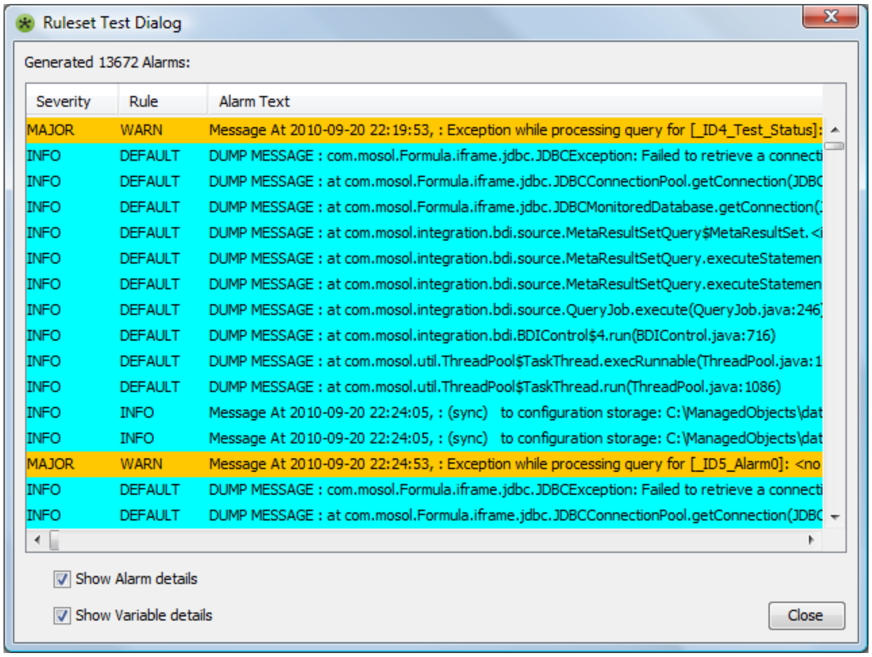
  The alarm's initial date and time is set to the date and time when the oldest threshold event and its most recent date and time is set to the date and time when the alarm became active.

  For example, set *Quantity* to 5 and *Threshold Time* to 2. In order to create an alarm, there must be five events in the past two minutes evaluated at the time of the most recent event. All five events are accumulated as a single alarm with an alarm count of 5. Events older than two minutes are discarded. Subsequent events increment the alarm counter as normal accumulated alarms.

7.4.10 Testing Rulesets Using Sample Data

During the process of defining rules, click ▷ (*Test*) in the *Raw Data* pane to apply the current selections/definitions to the sample data. The results display in a separate dialog box, as shown in Figure 7-14:

Figure 7-14 *Ruleset Test Dialog Box: Use the Scroll Bar to View Additional Columns.*



Ruleset Test Dialog

Generated 13672 Alarms:

Severity	Rule	Alarm Text
MAJOR	WARN	Message At 2010-09-20 22:19:53, : Exception while processing query for [_ID4_Test_Status]:
INFO	DEFAULT	DUMP MESSAGE : com.mosol.Formula.iframe.jdbc.JDBCException: Failed to retrieve a connecti
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.Formula.iframe.jdbc.JDBCConnectionPool.getConnection(JDBC
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.Formula.iframe.jdbc.JDBCMonitoredDatabase.getConnection(
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.integration.bdi.source.MetaResultSetQuery$MetaResultSet.<i
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.integration.bdi.source.MetaResultSetQuery.executeStatemen
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.integration.bdi.source.MetaResultSetQuery.executeStatemen
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.integration.bdi.source.QueryJob.execute(QueryJob.java:246
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.integration.bdi.BDIControl$4.run(BDIControl.java:716)
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.util.ThreadPool$TaskThread.execRunnable(ThreadPool.java:1
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.util.ThreadPool$TaskThread.run(ThreadPool.java:1086)
INFO	INFO	Message At 2010-09-20 22:24:05, : (sync) to configuration storage: C:\ManagedObjects\dat
INFO	INFO	Message At 2010-09-20 22:24:05, : (sync) to configuration storage: C:\ManagedObjects\dat
MAJOR	WARN	Message At 2010-09-20 22:24:53, : Exception while processing query for [_ID5_Alarm0]: <no
INFO	DEFAULT	DUMP MESSAGE : com.mosol.Formula.iframe.jdbc.JDBCException: Failed to retrieve a connecti
INFO	DEFAULT	DUMP MESSAGE : at com.mosol.Formula.iframe.jdbc.JDBCConnectionPool.getConnection(JDBC

☑ Show Alarm details

☑ Show Variable details

By default, all alarm details and variable details display in the Ruleset Test dialog box.

- "Viewing Additional Information in the Dialog" on page 77
- "Suppressing the Alarm or Variables Details" on page 77

Viewing Additional Information in the Dialog

To view additional information in the Ruleset Test dialog:

1. Use the scroll bar on the bottom to view columns to the right.

Suppressing the Alarm or Variables Details

To hide the alarm or variable details in the Ruleset Test dialog:

1. Deselect the *Show Alarm Details* and *Show Variable Details* check boxes.

   The alarm's *Severity*, *Rule*, and *Alarm Text* always display.
2. Use the output in the Ruleset Test dialog box to verify that the correct parsing and processing occurred.

   The *Rule* column identifies the rule used to generate each alarm.

7.4.11 Clearing the Ruleset Editor to Create a New Ruleset Definition

To clear the Ruleset Editor to create a new ruleset:

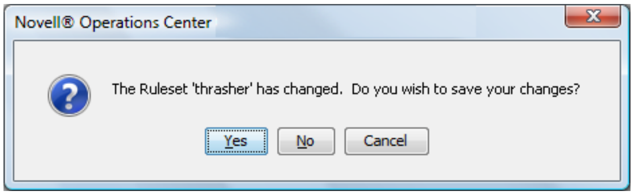
1. Do one of the following:
   - Click New (*New*) on the tool bar.
   - Click *File* > *New Ruleset*.

7.4.12 Exiting the Ruleset Editor

To close the Ruleset Editor:

1. Do one of the following:
   - Click *Close* in the upper right corner of the Ruleset Editor dialog box.
   - Click *File* > *Exit*.
2. When asked to confirm exiting the Ruleset Editor, click *Yes*.

   The following prompt asks you to save changes to the current ruleset:



Novell® Operations Center

The Ruleset 'thrasher' has changed. Do you wish to save your changes?

3. Click *Yes* or *No*.

7.5 Exporting Rulesets

After creating a ruleset, export it to the `.exp` (export) file format.

To export a ruleset:

1. Click *File* > *Save As*.
2. Specify a file name with an `.exp` extension.

7.6 Validating Rulesets

Rule validation automatically occurs upon importing or adding rules to the Event Manager. It is also possible to validate a ruleset using a manual process.

- Section 7.6.1, “Validating a Ruleset Manually for Correct Syntax,” on page 78
- Section 7.6.2, “Sending Input to the Ruleset,” on page 78

7.6.1 Validating a Ruleset Manually for Correct Syntax

To validate if the ruleset has correct syntax:

1. Execute the following command:

   ```
   mosjava com.mosol.Eve.Rule.RuleSet -import test.rs test.exp
   ```

   This example validates an exported ruleset named test.exp. If successfully validated, it creates the compiled ruleset named test.rs:
2. After compiling the ruleset, send input (raw text) to the ruleset and examine the result to see if the ruleset performs as expected.

7.6.2 Sending Input to the Ruleset

To send input tot he ruleset, execute the following command:

```
mosjava com.mosol.Eve.Rule.RuleSet -test test.rs test.dat
```

In this example, the input is contained in the `test.dat` file.

This input consists of a file containing event data that the test.rs ruleset can process. For example, this event data could be the raw log of events from a device.

7.7 Deleting Rulesets

To delete a ruleset:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a specific configuration > *Rule Sets*.
2. Right-click a ruleset, then select *Delete* to open a confirmation dialog box.
3. Click *Yes* to delete the ruleset.

8 Creating and Defining Agents

After defining the hosts, ports, and rulesets, the next step is to create and define the agents. The agents for the Event Manager collect alarms from a variety of sources.

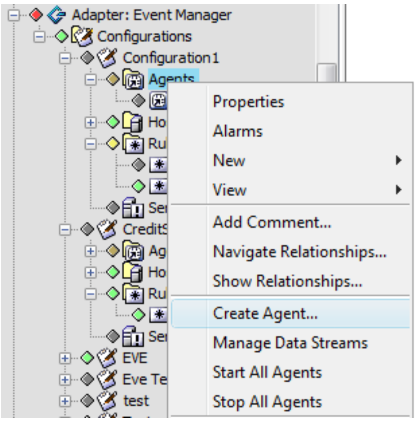
8.1 Creating and Configuring an Event Manager Agent

IMPORTANT: You should have the agent software for the Event Manager installed on each machine where the agents reside. For more information, see Section 3.1, “Installing the Event Manager Agent on a Remote Host,” on page 15.

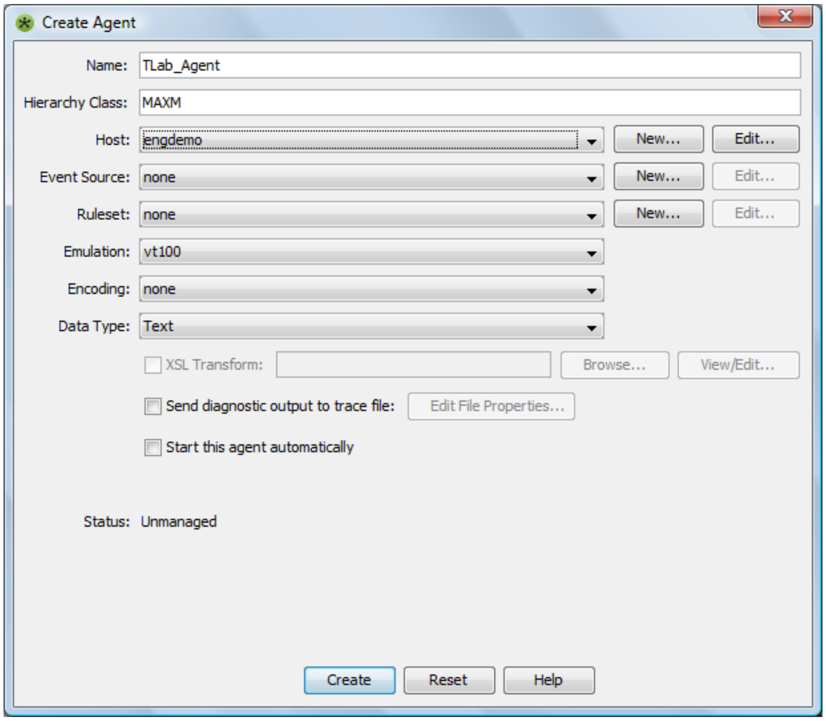
Use caution in configuring more than six agents, as some server hardware could have limitations on the number agents that can be handled, particularly machines with slower processors.

To create and configure an Event Manager agent:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter.



2 Right-click *Agents*, then select *Create Agent* to open the Create Agent dialog box:



Name: TLab_Agent

Hierarchy Class: MAXM

Host: engdemo

Event Source: none

Ruleset: none

Emulation: vt100

Encoding: none

Data Type: Text

□ XSL Transform:

□ Send diagnostic output to trace file:

□ Start this agent automatically

Status: Unmanaged

3 In the *Name* field, enter a name for the agent.

4 In the *Hierarchy Class* field, enter the class name of objects to associate with the agent. If a special icon is defined for the object class, the agent displays using that icon.

5 From the *Host* drop-down list, select a host where the agent resides.

If a specific host is not listed, click *New* to create a new host. For more information regarding creating host definitions, see Section 6.1, “Creating Hosts,” on page 35.

Click *Edit* to edit the selected host definition.

6 From the *Event Source* drop-down list, select a source from the list of all sources available on the selected host .

If the agent is to process events via a ruleset and more than one port is listed, select the port to use for the ruleset.

Agents that are used as a cut through need only select a port from the list.

If a particular source is not listed, click *New* to create the source. For more information regarding creating source definitions, see Section 6.3, “Creating Sources,” on page 36.

If necessary, click *Edit* to edit the selected source definition.

7 From the *Ruleset* drop-down list, select a ruleset to apply to the data collected by the agent. Select from a list of available rulesets on the selected host.

If necessary, click *New* to create a ruleset.

If necessary, click *Edit* to edit the selected ruleset.

8 From the *Emulation* drop-down list, select the type of emulation that this agent uses. Options are `vt100`, `vt220`, or `vt320`.

9. From the *Encoding* drop-down list, select a character encoding type. Options are:

   - **None:** The default. No encoding type is used.
   - **US-ASCII:** Seven-bit ASCII, a.k.a. ISO646-US, a.k.a. the Basic Latin block of the Unicode character set.
   - **ISO-8859-1:** ISO Latin Alphabet No. 1, a.k.a. ISO-LATIN-1.
   - **UTF-8:** Eight-bit Unicode Transformation Format.

   For information on various Unicode Transformation Formats, see the Frequently Asked Question section on the Unicode Standard Web site.

10. From the *Data Type* drop-down list, select the type of data expected. Options are `Text`, `TEC`, or `XML`.

    - If *XML* is selected, the Event Manager Agent requires that either the XML already be in normalized format, or that you attach the XLST file to translate it into the normalized format, which conforms to the following tag structure:

      ```
      <events>
         <event class="event_class">
            name=value,
            name2=value2,
               ...
            nameN=valueN
        </event>
        <event...
        </event>
      </events>
      ```

      For XML that does not originally conform to the Operations Center Normalized Event Format, select the *XSL Transform* check box and specify an XSL file used to transform the data received.

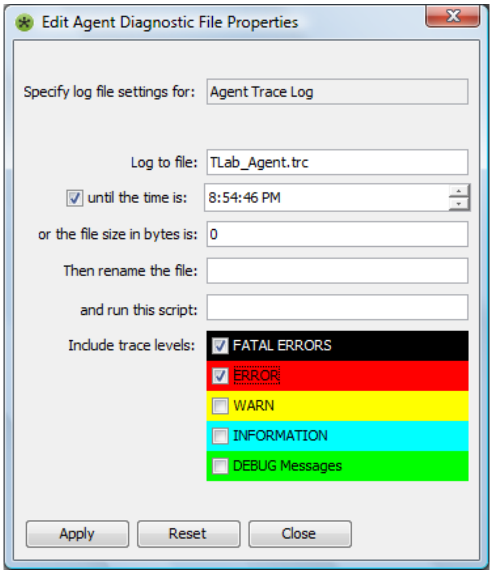
      Enter the XSL file name in the *XSL Transform* field or click *Browse* to locate and select the file.

      Note that you can only browse to files located on the local file system where the Operations Center client runs. To specify a file where the agent or the Operations Center server is running (or any other location), enter the file’s path and pathname based on that.

      Click *View/Edit* to view or edit the XSL file code.

11. Select the *Send diagnostic output to trace file* check box to maintain a log file to track agent activity.

    Identify the path to that file by clicking *Edit File Properties*. The Edit Agent Diagnostic File Properties dialog box opens:



Edit Agent Diagnostic File Properties

Specify log file settings for: Agent Trace Log

Log to file: TLab_Agent.trc

☑ until the time is: 8:54:46 PM

or the file size in bytes is: 0

Then rename the file:

and run this script:

Include trace levels:

☑ FATAL ERRORS

☑ ERROR

☐ WARN

☐ INFORMATION

☐ DEBUG Messages

The following defines the agent trace log properties that are required for the trace file setup:

- **Log to file:** Specify the file name for storing log information. Edit this entry to reflect the path to the Operations Center directory.
- **Until the time is:** Use the spinner buttons to select a cut-off time for storing log data. The time format is HH:MM:SS AM/PM. For example, specify 12:00:00 PM for noon or 09:30:00 PM for 9:30 PM.
- **Until the file's size is:** Enter the cut-off file size for collecting trace log data.
- **Then rename the file:** When the trace log file reaches one of the cut-offs above, it renames the file to this entry, and starts a new log file.
- **And run this script:** Any program can be run here, but the default is a file compression application, gzip.
- **Include trace Levels:** Mark the levels of output messages to include in the trace file.

Click *Close* when selections are complete.

12. Select the *Start this agent automatically* check box to start this agent automatically when the Agent Container starts up.

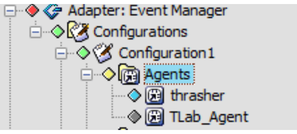
    If you do not select this check box, the agent must be manually started.

13. Click *Create* to create the agent definition.
14. To set up a T/EC Server Socket connection, create a source for a server socket connection, then select *TEC* as the Data Type for the agent.

8.2 Checking the Agent Status

Agent status updates automatically. The colored diamonds next to the agents in the *Explorer* pane indicate the status:

Figure 8-1 Explorer Pane: Color-coded condition indicators identify the status of the selected agent.



- OK (default is green) indicates all agents have started.
- MINOR (default is yellow) indicates some agents have started.
- MAJOR (default is orange) indicates the agent has been terminated. Check Operations Center and agent trace logs for any error messages.
- CRITICAL (default is red) indicates the agent has failed with an exception. Check Operations Center and agent trace logs for error messages.
- UNKNOWN (default is gray) indicates no agents have started.

8.3 Stopping and Starting Agents

IMPORTANT: Before an agent can start, the Operations Center daemon (`mosdaemon`) must be start started on every host (or machine) where an agent is installed.

If the Event Manager agents are configured to start automatically (see Section 8.1, “Creating and Configuring an Event Manager Agent,” on page 79), skip this section. To verify that agents are running or stopped, or to manually start or stop agents, follow one of these procedures:

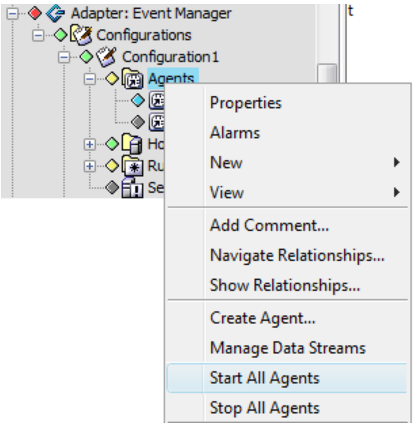
- Section 8.3.1, “Starting All Agents,” on page 84
- Section 8.3.2, “Starting a Single Agent,” on page 84
- Section 8.3.3, “Stopping All Agents,” on page 84
- Section 8.3.4, “Stopping a Single Agent,” on page 84

8.3.1 Starting All Agents

To start all defined agents, regardless of the automatic start setting:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter.

2 Right-click *Agents*, then select *Start All Agents*:



8.3.2 Starting a Single Agent

To start an individual agent, regardless of the automatic start setting:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter > *Agents*.

2 Right-click an agent, then select *Start Agent*.

8.3.3 Stopping All Agents

To stop all agents:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter.

2 Right-click *Agents*, then select *Stop All Agents*.

8.3.4 Stopping a Single Agent

To stop an individual agent:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter > *Agents*.

2 Right-click an agent, then select *Stop Agent*.

8.4 Deleting Agents

To delete an agent:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter > *Agents*.
2. Right-click an agent, then select *Delete*.

   The agent disappears from the *Explorer* pane.

8.5 Configuring the Agent Container

As stated in Section 2.2, "Agents and the Agent Container," on page 13, agents use a common virtual machine called an Agent Container to save system resources. The Agent Container is a container that works behind the scenes to house all the agents on a single machine. An Agent Container can hold up to 4,000 alarms in its outbound queue. After reaching this limit, it discards the oldest alarms. For example, if the Alarm server is unavailable and cannot forward alarms, it discards the oldest alarms.

The `/`*`OperationsCenter_install_path`*`/config/eve.properties` file contains properties used to configure the Agent Container.

To configure the Agent Container:

1. Open the `/`*`OperationsCenter_install_path`*`/config/eve.custom.properties` file in a text editor. (or create one it if it doesn't already exist).

   Using the `eve.custom.properties` file ensures that customizations are not overwritten during product reinstallations, upgrades, or when settings are changed using Configuration Manager.

   If the `eve.custom.properties` file doesn't already exist, create it. For more information about custom properties files, see Section 3.4.1, "Creating a Custom Properties File," on page 22.
2. Add and configure the following settings:
   - **com.mosol.Eve.Agent.alarmQueueSize:** The maximum size of the alarm queue within the agents. Default is `4000`.
   - **com.mosol.Eve.Agent.blockMode:** When set to `BLOCKED` and the *com.mosol.Eve.Agent.alarmQueueSize* value is reached, this property blocks additional alarms, but does not discard any previous alarms. If set to `NON-BLOCKED`, agents discard the oldest alarms after surpassing the specified *com.mosol.Eve.Agent.alarmQueueSize* property.
   - **com.mosol.Eve.Agent.AutoCloseKeepAliveValue:** The length of time, in minutes or milliseconds based on the *com.mosol.Eve.Agent.AutoCloseStrategy* property setting, to keep an agent socket connection alive.
   - **com.mosol.Eve.Agent.AutoCloseStrategy:** Works in conjunction with the *com.mosol.Eve.Agent.AutoCloseKeepAliveValue* for configuring and monitoring an agent socket connection. Set to one of the following:
     - `NONE`: Do not monitor the socket connection. Best starting option if you are getting out of memory exceptions.
     - `MOS_SO_TIMEOUT`: Times out the socket connection after a length of time, in milliseconds, as based on the *com.mosol.Eve.Agent.AutoCloseKeepAliveValue* setting.

- `SO_KEEPALIVE`: Keep alive flag on the socket connection regardless of the *com.mosol.Eve.Agent.AutoCloseKeepAliveValue* setting. The socket might stay alive for a long time if not closed.
- `MOS_KEEPALIVE`: Default behavior. Monitors the socket connection for a length of time, in minutes, as based on the *com.mosol.Eve.Agent.AutoCloseKeepAliveValue* setting.

3 Restart all Event Manager processes.

8.6 Setting Up Distributed Agent Support

The Agent Container is the CORBA component that manages individual agents within a single host machine and is the source of the actual preprocessed alarm stream.

The Agent Container can send data streams of preprocessed alarms to more than one alarm server process within the Event Manager, to provide configurations that are fault tolerant and increase scalability.

- Section 8.6.1, "Fulfilling the Prerequisites," on page 86
- Section 8.6.2, "Setting Up the Distributed Agent Support Feature," on page 86

8.6.1 Fulfilling the Prerequisites

Before using the distributed agent support feature:

1 Define the hosts where servers (other than the default or primary alarm server) are running.

2 Make sure that all affected alarm servers are up and running.

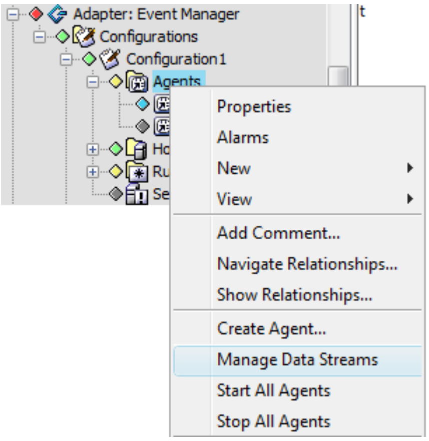
The data stream management feature is supported on all Event Manager alarm servers.

8.6.2 Setting Up the Distributed Agent Support Feature

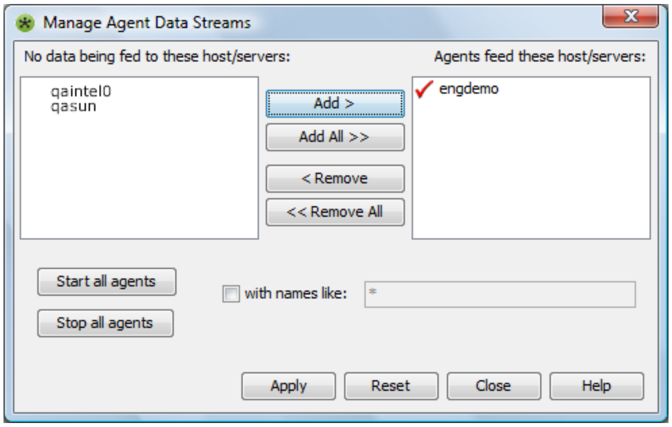
To set up distributed agent support:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter.

2 Right-click *Agents*, then select *Manage Data Streams* to open the Manage Agent Data Streams dialog box:



In the Manage Agent Data Streams dialog box, the primary host displays in the *Agents feed these hosts/servers* list.



No data being fed to these host/servers:

qaintel0
qasun

Agents feed these host/servers:

✓ engdemo

☐ with names like: *

The default or primary alarm server is under the *Configurations* element and usually runs on the same machine as the Event Manager and the Operations Center server.

Other hosts display in the *No data being fed to these hosts/servers* list.

IMPORTANT: The security setting must be the same on the sending server and the receiving server.

3. Do any of the following:
   - To select a host, click a host in the *No data being fed to these hosts/servers* list, then click *Add*.

     The selected host displays in the *Agents feed these hosts/servers* list.

     If no hosts display in the *Agents feed these hosts/servers* list, then no data goes to any host or server.
   - To select all hosts, click *Add All*.

     All hosts display in the *Agents feed these hosts/servers* list.
   - To remove a host, in the *Agents feed these hosts/servers* list, select a host, then click *Remove*.

     The hostname displays in the *No data being fed to these hosts/servers* list.

     Select any combination of hosts, including the primary host from receiving data.
4. Do any of the following:
   - To start all agents, click *Start All Agents*.
   - To start only specific agents as specified by a regular expression, select the *With Names Like* check box and enter the regular expression in the field, then click *Start All Agents*.

     Only the agents that meet the expression criteria start.
5. Do any of the following:
   - To stop all agents, click *Stop All Agents*.
   - To stop only specific agents as specified by a regular expression, select the *With Names Like* check box and enter the regular expression in the field, then click *Stop All Agents*.

     Only the agents that meet the expression criteria stop.

6 To send data to alarm servers on the selected hosts, click *Apply*.

The Agent Container attempts to send data to alarm servers on all hosts displayed in the *Agents feed these hosts/servers* list.

If an alarm server is unreachable, a warning message is stored in the `eve.trc` file and that particular host is ignored. The data is sent to all hosts/servers that are reachable within the set.

WARNING: As additional hosts are added to receive preprocessed alarms, significant slowing in performance can occur. Moving from a single alarm server to a server and a backup server doubles the amount of time required for a send operation. The Event Manager administrator sets the agent buffering to compensate for this in cases where large data bursts might occur.

9 Configuring the Alarm Server Database

All alarms generated by the Alarm server can reside in the database so that the current set of alarms persists across multiple runs of the Alarm server.

The Alarm server leverages a database definition defined in Operations Center for the Operations Center Event Store.

- Section 9.1, “Configuring the Alarm Server Database,” on page 89
- Section 9.2, “Checking the Alarm Server Status,” on page 93
- Section 9.3, “Using mosstatus to Check Alarm Server Status,” on page 94
- Section 9.4, “Starting and Stopping the Alarm Server,” on page 94
- Section 9.5, “Viewing Event Manager Alarm Properties,” on page 96
- Section 9.6, “Event Manager Alarm Server Dictionary,” on page 98

9.1 Configuring the Alarm Server Database

Use the steps in this section to configure the Alarm server database. For information about server processing functionality and features that can be customized, see Section 9.6, “Event Manager Alarm Server Dictionary,” on page 98.

- Section 9.1.1, “Configuring the Alarm Server Database,” on page 90
- Section 9.1.2, “Configuring the Alarm Server using Eve.Properties,” on page 92

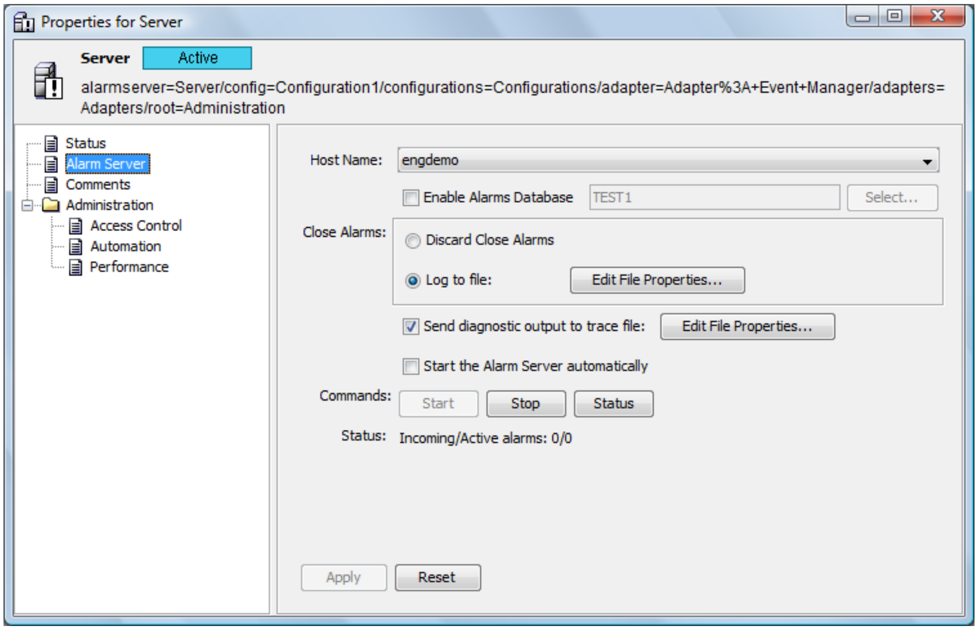
9.1.1 Configuring the Alarm Server Database

To configure the Alarm Server database:

1 In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter.

2 Right-click *Server*, then select *Properties* to open the Status property page.

3 In the left pane, click *Alarm Server* to open the Alarm Server property page:



Properties for Server

Server Active

alarmserver=Server/config=Configuration1/configurations=Configurations/adapter=Adapter%3A+Event+Manager/adapters=Adapters/root=Administration

Host Name: engdemo

□ Enable Alarms Database TEST1

Close Alarms:
○ Discard Close Alarms
● Log to file:

☑ Send diagnostic output to trace file:

□ Start the Alarm Server automatically

Status: Incoming/Active alarms: 0/0

4 Verify that the hostname is correct.

To select a different host, click the *Hostname* drop-down list.

5 To select the Alarm server database, select the *Enable Alarms Database* check box and verify the appropriate database displays in the adjacent field.

6 To define a new database definition, click *Select*. For more information about creating and initializing database definitions, see the *Operations Center Server Configuration Guide*.

After stopping and restarting the Alarm server, previously generated alarms redisplay. If the *Enable Alarms Database* check box is deselected, generated alarms are lost after stopping and restarting the Alarm server.

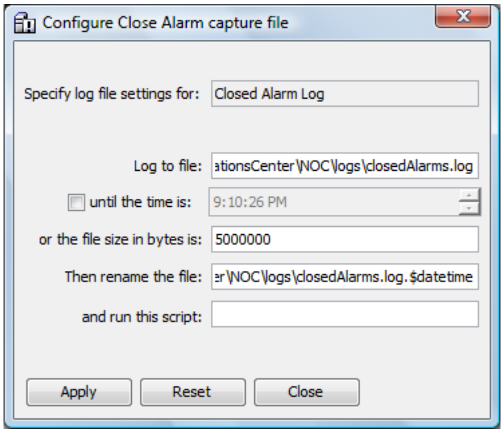
If creating a database definition on-the-fly solely for the Operations Center Event Data Store schema, it is necessary to initialize the database before use. If created in conjunction with the Service Warehouse schema selection, this is not necessary. For more information, see the *Operations Center Server Configuration Guide*.

For a list of the most current versions of supported databases, see the *Operations Center Getting Started Guide*.

7 To use the *Close Alarms* options to set policies for closed alarms, select one of the following radio buttons:

Discard Close Alarms: Discards all closed alarms (alarms that are closed by a user or are timed out according to the ruleset definition).

Log to file: Records closed alarms in a file. Click *Edit File Properties* to open the Edit Alarm Server Alarm Capture File Properties dialog box shown in the following figure:



Configure Close Alarm capture file

Specify log file settings for: Closed Alarm Log

Log to file: ationsCenter\NOC\logs\closedAlarms.log

□ until the time is: 9:10:26 PM

or the file size in bytes is: 5000000

Then rename the file: er\NOC\logs\closedAlarms.log.$datetime

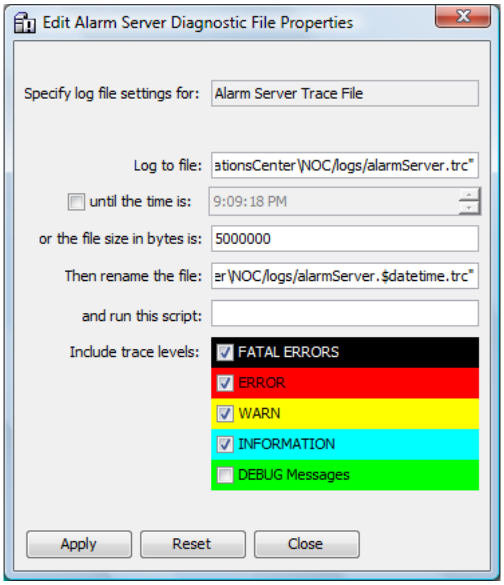
and run this script:

Complete the *Log File* properties required for the *Alarm Capture File* setup:

- **Log to file:** Specify the file name for storing log information. Edit this entry to include the path to the Operations Center directory.
- **Until the time is:** Use the spinner buttons to select a cut-off time for storing log data.
- **Until the file's size is:** Enter the cut-off file size for collecting trace log data.
- **Then rename the file:** When the trace log file reaches one of the cut-offs above, it renames the file to this entry, and starts a new log file.
- **And run this script:** Any program can run here, but the default is a file compression application, gzip.
- **Include trace levels:** Mark the trace levels to include in the log file.

Click *Close* when finished.

8 Select the *Send Diagnostic Output to Log File* check box to send diagnostic output (the Alarm server trace file) to a log file, click *Edit File Properties* to open the Edit Alarm Server Diagnostic File Properties dialog box, then specify the log file name and complete the parameters shown in Step 7.



Specify log file settings for: Alarm Server Trace File

Log to file: ationsCenter\NOC/logs/alarmServer.trc"

□ until the time is: 9:09:18 PM

or the file size in bytes is: 5000000

Then rename the file: er\NOC/logs/alarmServer.$datetime.trc"

and run this script:

Include trace levels:
☑ FATAL ERRORS
☑ ERROR
☑ WARN
☑ INFORMATION
□ DEBUG Messages

Complete the *Log File* properties required for the *Diagnostic File Properties* setup:

- **Log to file:** Specify the file name for storing log information. Edit this entry to include the path to the Operations Center directory.
- **Until the time is:** Use the spinner buttons to select a cut-off time for storing log data.
- **Until the file's size is:** Enter the cut-off file size for collecting trace log data.
- **Then rename the file:** When the trace log file reaches one of the cut-offs above, it renames the file to this entry, and starts a new log file.
- **And run this script:** Any program can run here, but the default is a file compression application, gzip.
- **Include trace levels:** Mark the trace levels to include in the log file.

9. Select the *Start the Alarm Server Automatically* check box to start the Alarm server automatically when the configuration starts.
10. Click *Apply* to save and use the Alarm server database settings.

9.1.2 Configuring the Alarm Server using Eve.Properties

A section of the `/`*`OperationsCenter_install_path`*`/config/eve.properties` file contains properties used to configure the Alarm server. Most of the properties are self-explanatory, but the following is a description of two standard properties.

- **com.mosol.Eve.AlarmServer.persistAlarmsWhenNoSession:** If set to True, and the Operations Center server shuts down, the send queues retain all processed alarms until the Operations Center server restarts. This saves all alarm open and close records and thereby enables execution of automation tasks.
- **com.mosol.Eve.AlarmServer.keepOriginatingAlarmTextOnAccum:** If set to False or if the property is not used, the description text for alarms updates as alarms accumulate. If set to True, the original (first to arrive) description text remains. Depending on the size of the text description, this can be more efficient.

You can also create a custom properties file to help manage data streams after losing Alarm server connectivity and to set Alarm server functions. For more information, see Section 3.4.2, "Properties Related to Alarm Server Connectivity," on page 22 and Section 3.4.3, "Custom Properties Related to

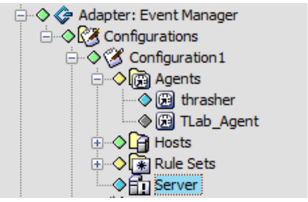
Alarm Server Functions,” on page 23.

NOTE: To store alarm history, the element properties created by the Event Manager adapter must meet the supported schema as specified in the Data Dictionary. For example, dnames cannot exceed 3,000 characters.

9.2 Checking the Alarm Server Status

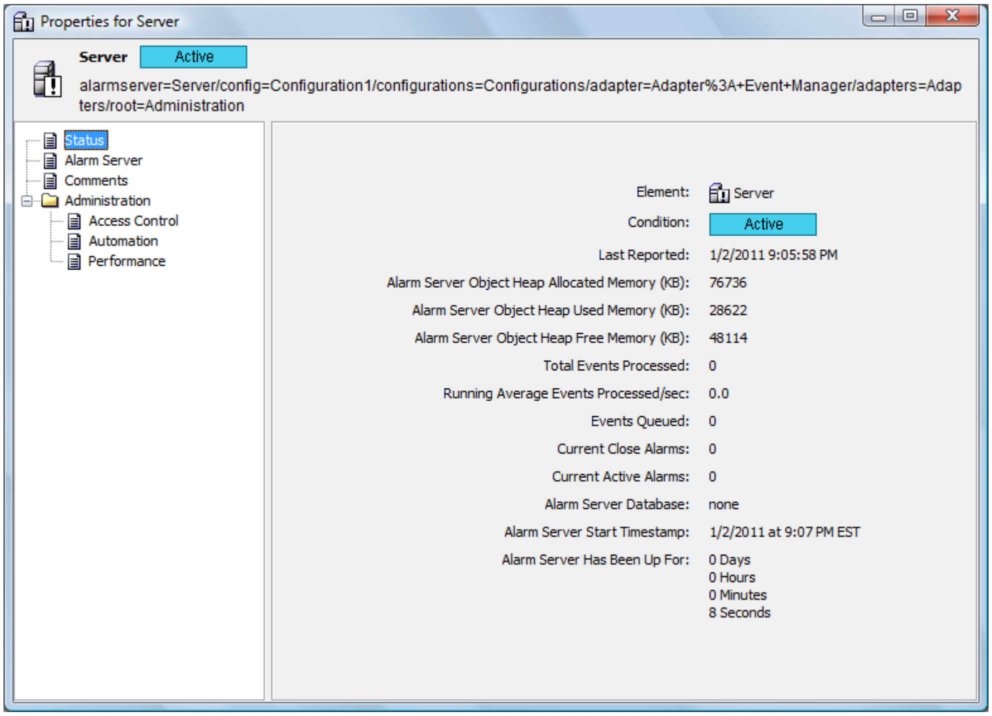
The Alarm server status updates automatically. The colored diamond next to the *Server* element in the *Explorer* pane identifies the server condition.

Figure 9-1 *Explorer Pane: The server condition indicators display.*



To view Alarm server state and status information:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter.
2. Right-click *Server*, then select *Properties* to open the Status property page:



Server: Active

alarmserver=Server/config=Configuration1/configurations=Configurations/adapter=Adapter%3A+Event+Manager/adapters=Adapters/root=Administration

Element:	Server
Condition:	Active
Last Reported:	1/2/2011 9:05:58 PM
Alarm Server Object Heap Allocated Memory (KB):	76736
Alarm Server Object Heap Used Memory (KB):	28622
Alarm Server Object Heap Free Memory (KB):	48114
Total Events Processed:	0
Running Average Events Processed/sec:	0.0
Events Queued:	0
Current Close Alarms:	0
Current Active Alarms:	0
Alarm Server Database:	none
Alarm Server Start Timestamp:	1/2/2011 at 9:07 PM EST
Alarm Server Has Been Up For:	0 Days 0 Hours 0 Minutes 8 Seconds

This page displays state and status information.

9.3 Using mosstatus to Check Alarm Server Status

To view the status of the Alarm server using the `mosstatus` command, do the following at the command prompt:

1 Go to the `/`*`OperationsCenter_install_path`*`/bin` directory, or go to the directory where the Event Manager is installed.

2 Enter:

```
mosstatus EveAlarmServer
```

The output is similar to the following message:

```
Server EveAlarmServer
Status: Incoming/Active alarms: 0/0
```

9.4 Starting and Stopping the Alarm Server

The Alarm server starts automatically when the Event Manager Configuration Server starts, but it is also possible to manually start and stop the server.

The Event Manager components are not necessarily interdependent. This means that stopping the Alarm server does not automatically stop the adapter, the Agent Container or the Configuration.

- Section 9.4.1, “Shutting Down Everything for the Event Manager,” on page 94
- Section 9.4.2, “Starting or Stopping the Alarm Server,” on page 95

9.4.1 Shutting Down Everything for the Event Manager

1 Stop the alarm server.

2 Stop the adapter.

3 Stop all agents.

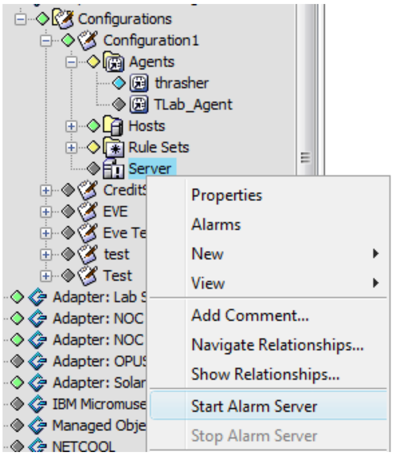
4 Stop the Configuration Server.

9.4.2 Starting or Stopping the Alarm Server

To start or stop the alarm server:

1. In the *Explorer* pane, expand the *Administration* root element > *Adapters* > the Event Manager adapter > *Configurations* > a configuration profile for the adapter.
2. Right-click *Server*, then select *Start Alarm Server* or *Stop Alarm Server*.

   If the Alarm server is running, the *Start Alarm Server* option is dimmed, and if the server is not running the *Stop Alarm Server* option is dimmed.



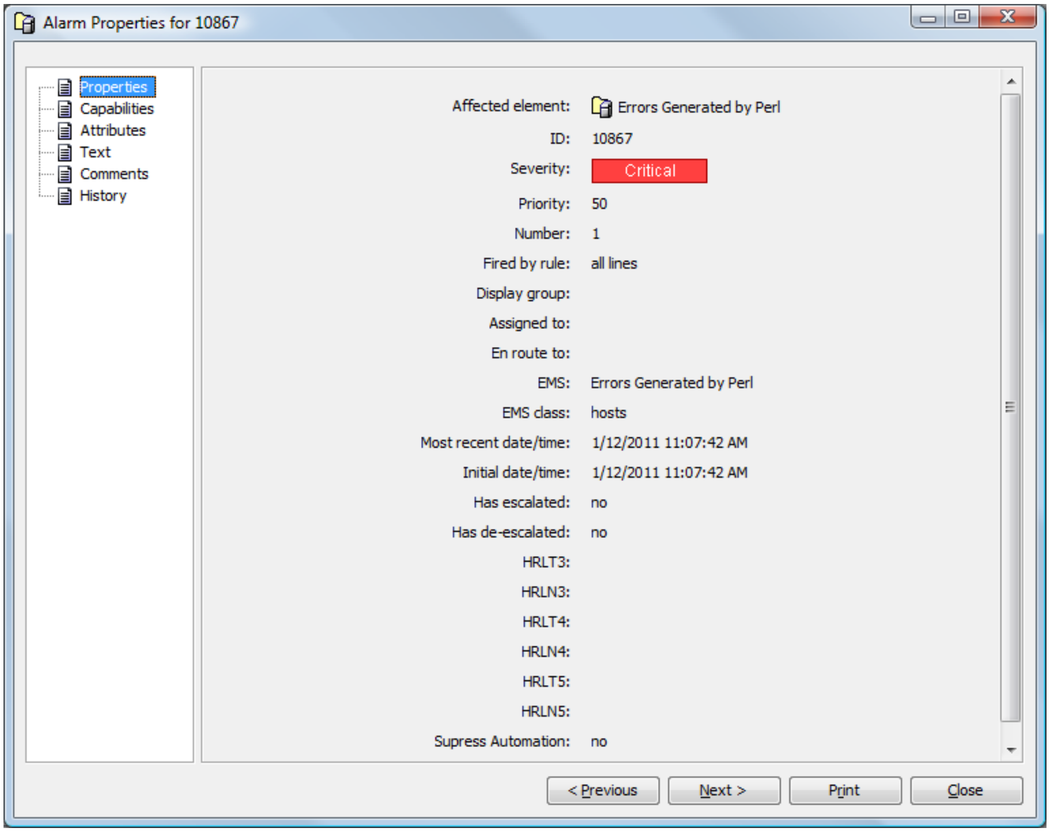
9.5 Viewing Event Manager Alarm Properties

The alarm properties for Event Manager events display different types of information related to the alarm.

To view the alarm properties:

1 In the *Alarms* view, double-click an alarm to open the Properties page.

Figure 9-2 *Properties Page of Alarm Properties*



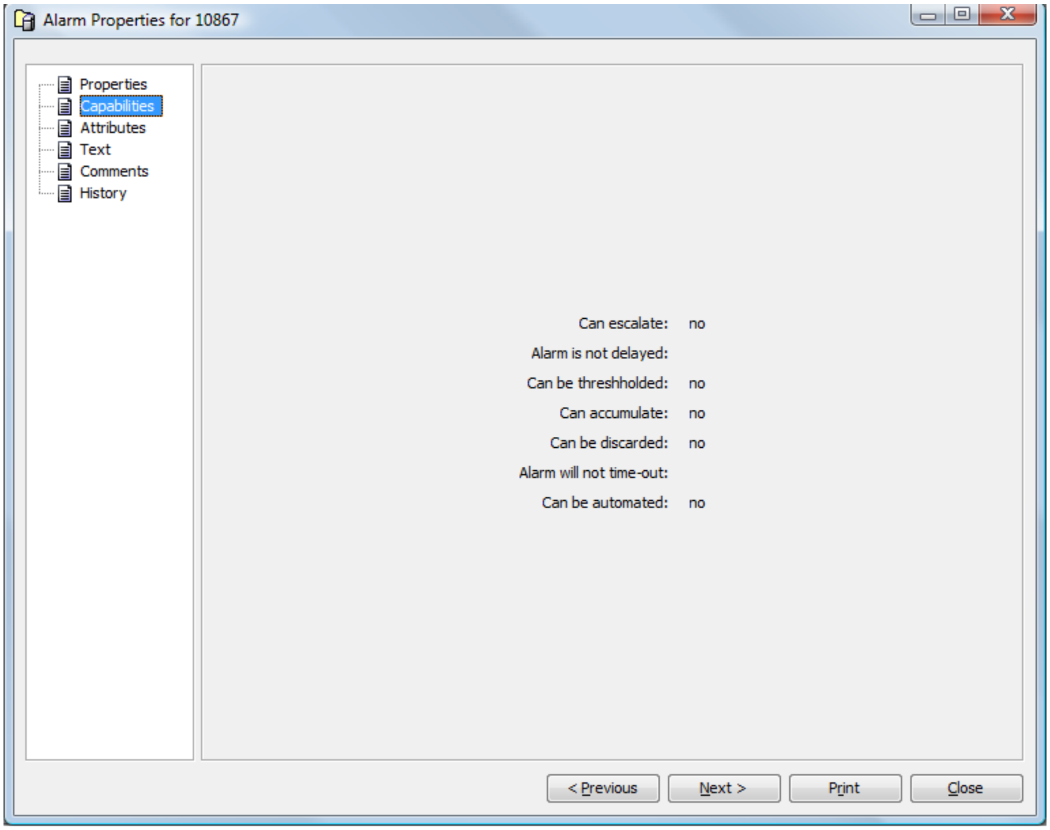
Affected element:	Errors Generated by Perl
ID:	10867
Severity:	Critical
Priority:	50
Number:	1
Fired by rule:	all lines
Display group:	
Assigned to:	
En route to:	
EMS:	Errors Generated by Perl
EMS class:	hosts
Most recent date/time:	1/12/2011 11:07:42 AM
Initial date/time:	1/12/2011 11:07:42 AM
Has escalated:	no
Has de-escalated:	no
HRLT3:	
HRLN3:	
HRLT4:	
HRLN4:	
HRLT5:	
HRLN5:	
Supress Automation:	no

The Properties page displays a summary of the alarm status, its priority, the rule that fired the alarm, and the assigned user (if any).

2 Click other property page names to view additional information:

- Click *Capabilities* to display:

Figure 9-3 *Capabilities Page of Alarm Properties*



Can escalate: no

Alarm is not delayed:

Can be threshholded: no

Can accumulate: no

Can be discarded: no

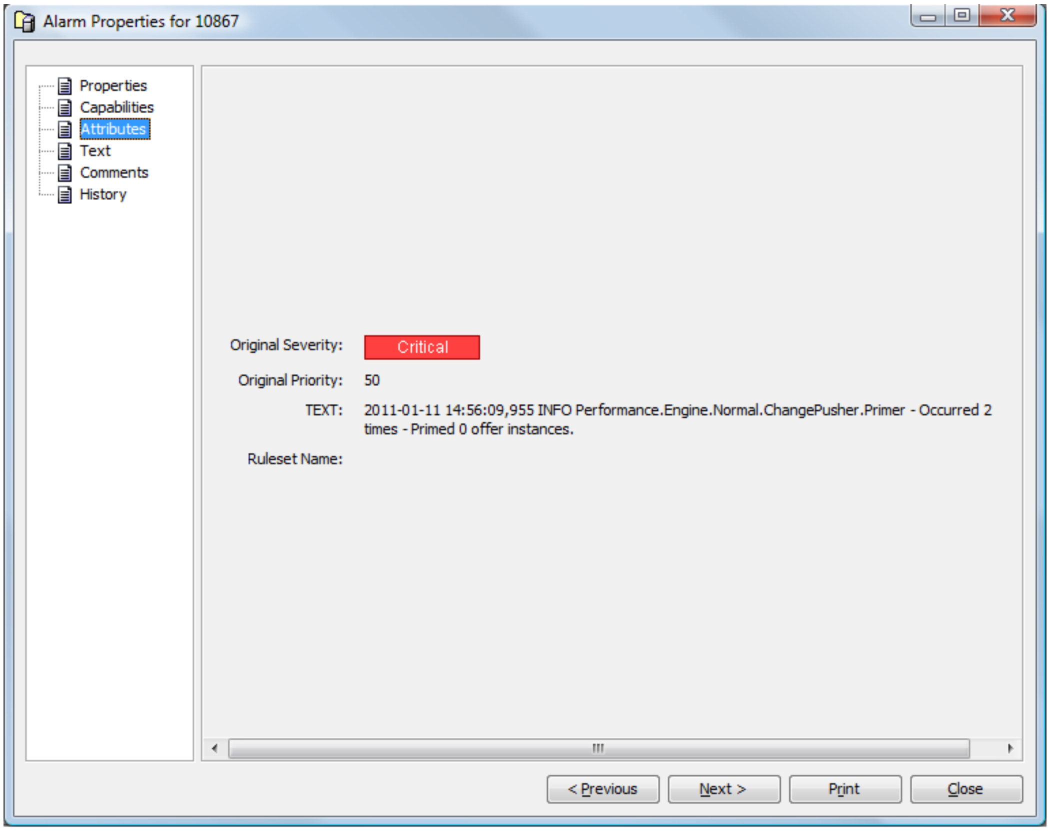
Alarm will not time-out:

Can be automated: no

The Capabilities page displays alarm features such as whether it can accumulate or be discarded, as well as the delay factor or time-out factor, if it exits.

- Click *Attributes* to display:

Figure 9-4 Attributes Page of Alarm Properties



Original Severity: Critical

Original Priority: 50

TEXT: 2011-01-11 14:56:09,955 INFO Performance.Engine.Normal.ChangePusher.Primer - Occurred 2 times - Primed 0 offer instances.

Ruleset Name:

The Attributes page displays information about the origin of the alarm, including the associated ruleset name and process.

- Click *Text* to display a description or message related to the alarm.
- Click *Comments* to enable you to enter text comments about the alarm and to view comment history.
- Click *History* to display the alarm history, including values recorded during previous alarm updates.

9.6 Event Manager Alarm Server Dictionary

The Alarm Server dictionary provides information about server processing functionality and features that can be customized. To learn more about editing the custom properties file, see Section 3.4, “Setting Custom Properties for Alarm Server Connectivity and Alarm Server Functions,” on page 22.

- Section 9.6.1, “Alarm Keys,” on page 99
- Section 9.6.2, “Custom Property Flags,” on page 100
- Section 9.6.3, “Accumulation Subrules,” on page 101

9.6.1 Alarm Keys

Alarm keys for the Event Manager custom properties are listed in the following:

- **HRL:** Hierarchy Resource List, a composite key.
- **HRLT(Type)1-5, HRLN(Name)1-5, and the rule name, provide a unique key for the alarm:**

  HRLT1==SP HRLN1 == $MAXM (Default: Eve)
  HRLT2=TP HRLN2 == $EMS (Default: Agent Name)
  HRLT3-5 == User defined
  HRLN3-5== User defined
- **Generated Alarm Text:** Any combination of rule set variables and free text display as alarm text.
- **Severity:**
  - **1:** CRITICAL
  - **2:** MAJOR
  - **3:** MINOR
  - **4:** INFORMATIONAL
  - **5:** OK

  Increase the severity level by decreasing the severity number. Alarms cannot de-escalate lower than OK or escalate higher than CRITICAL.
- **Priority:** Valid values: 1 – 99. Increase the priority by decreasing the priority number. Alarm priority cannot go lower than 99 or higher than 1.
- **Close Rule enhanced processing:** Remove all alarms, active or delayed, from the system if the rule name specified is the Close Rule and all HRL values match the HRL values of a rule being fired.

  Wildcards:
  - **Closes All Rules (*):** Close all alarms, active or delayed, with matching HRLs, regardless of rule name. (Ignore rule name).
  - **Close All EMSs for Rule:** Close all alarms, active or delayed, with matching HRLs, except for HRLT2 and HRLN2. (Ignore HRL2).

  When both wildcard flags are used, both the rule name and HRL2 are ignored.

  Currently, t the $EMS parameter setting in the Event Manager Agent does not allow setting the $EMS globally. The workaround is to use the EMS class that is defined when the agent is created instead of using $EMS.

  The custom property flag that controls this behavior:

  com.mosol.Eve.AlarmServer.useEMSClassToClose

  If True, alarms are closed across EMS_class using the hierarchy class defined in the agent.

  If False (the default), the EMS defined as the agent’s name is used.
- **Timeout:** Closes the active alarm after *x* minutes.
  - For nondelayed alarms, the timeout time is the initial event time + *x* minutes.
  - For delayed alarms and threshold alarms, the timeout time is the time the alarm became active + *x* minutes.
  - For active accumulated alarms, the timeout time is reset to the time of the latest accumulating event + *x* minutes.

  - For discard alarms, the active alarm timeout time is not updated when matching events are discarded.
  - If timeout is not selected, the active alarm never times out.
  - If timeout is selected and set to 0, closes all alarms, active or delayed, and adheres to all *Close Rule* parameters. However, it does not create a new alarm or perform any other alarm processing.

  The custom property flag that controls this behavior:

  com.mosol.Eve.AlarmServer.timeout.schedule

  This is the scheduled time (in milliseconds) to check for alarm timeouts. The default is 30000 (30 seconds).

- **Delay:** Postpones creating an alarm for *x* minutes. A delayed alarm can be closed by another event before it becomes active. The timeout time is the time the alarm became active + *x* minutes. After the alarm is created, normal event processing applies.

  Delay and Threshold are mutually exclusive. Threshold takes precedence if both are set.

9.6.2 Custom Property Flags

The following custom property flags modify the behavior of delayed alarms for the Alarm Server:

- **com.mosol.Eve.AlarmServer. delayedAlarmsPreCloseRules:** If True (the default), events that create a delayed alarm perform Close Rule functions as soon as the event arrives in the Alarm server.

  If False, Close Rule functions are not performed until the delayed alarm becomes active.

- **com.mosol.Eve.AlarmServer. resetDelayed AlarmsTime:** If True, a delayed alarm's initial date and time and its most recent date and time is set to the date and time that the alarm became active.

  If False (the default), a delayed alarm's initial date and time is set to the date and time the event arrives in the Alarm server and its most recent date and time is set to the date and time that the alarm became active. In both cases the alarm's date and time in Operations Center is the most recent date and time.

- **com.mosol.Eve.AlarmServer. delay.schedule:** The scheduled time (in milliseconds) to evaluate delayed events. The default is 30000 (30 seconds).
- **Discard (after first):** If an active alarm exists with the same rule name and HRL values, discard the incoming alarm. Only active alarms are evaluated for matches. No other alarm processing is performed. Discard and Accumulate cannot both be True. If Discard is True, Accumulate is evaluated as False.
- **Time Escalation:** If an alarm has been active for x minutes since the initial date and time, increase/decrease the severity and/or priority by a rule-determined threshold amount until the upper or lower limit is reached.

  This is performed for each multiple (nx) of the threshold time. Accumulating alarms that have time escalated/de-escalated no longer have their severity or priority properties updated.

  Example: Set Escalate Time to 5, Escalate Severity by 1, Escalate Priority by 1.

  An event creates a MINOR active alarm with the counter set to 1 and a priority of 50. When the alarm has been active for 5 (*x*) minutes, the alarm severity is increased to MAJOR and the priority is increased to 49. (Note that a lower priority number actually sets a HIGHER priority.)

  When the alarm has been active for 10 minutes (2x), the alarm severity increases to CRITICAL and the priority increases to 48.

The same behavior apples for each nx increment, except that the severity remains CRITICAL because it cannot go any higher. Severities can go no higher than CRITICAL nor lower than INFO using escalation. Priorities can go no higher than 1 nor lower than 99 with escalation.

The custom property flag that controls this behavior:

com.mosol.Eve.AlarmServer.escalation.schedule

This is the scheduled time (in milliseconds) to evaluate time escalated alarms. The default is 30000 (30 seconds).

- **Accumulate:** Updates an active alarm every time an event with a matching rule name and HRL is processed.

  Discard must be False for Accumulate to be evaluated.

  An accumulation counter is updated by N + 1 each time an alarm is accumulated. The timeout time is reset to the time of the latest accumulating event + x minutes. The alarm's initial date and time is set to the date and time when the first alarm was created and its most recent date and time is set to the date and time that the alarm was last accumulated. The alarm's date and time in Operations Center is the most recent date and time.

  The custom property flag that controls this behavior:

  com.mosol.Eve.AlarmServer.escalation.schedule

  If True (the default), updates all the alarm's properties on accumulation. This includes, but is not limited to, severity, priority and alarm text.

  If False, updates only the accumulation counter, the most recent date and time, and the alarm's timeout value.

  NOTES:

  - Accumulated alarms that have escalated/de-escalated will not have their severity or priority properties updated.
  - com.mosol.Eve.AlarmServer.updateTextOn Accumulation is obsolete and should be removed completely from the Alarm server.

9.6.3 Accumulation Subrules

The following are accumulation subrules for the Alarm Server Dictionary:

- **Quantity Escalation (Accumulate True):** Accumulate must be True for this function to be evaluated.

  If the alarm quantity count of an accumulated alarm exceeds a rule-determined value x, the severity and/or priority increases or decreases by a rule-determined threshold amount until the upper or lower limit is reached. This is performed for each multiple (nx) of the threshold quantity. Alarms that have quantity escalated/de-escalated no longer have their severity or priority properties updated.

  Example: Set Quantity to 5, Escalate Severity by: 1, Escalate Priority by: 1.

  An event creates a MINOR active alarm with the counter set to 1 and a priority of 50. If subsequent alarms have the accumulation counter set between 1 and 4, there is no change to alarm severity or priority.

  When the accumulation counter increments to 5(x), the alarm severity increases to MAJOR and the priority increases to 49. (A lower priority number is a HIGHER priority.)

  Subsequent alarms that have the accumulation counter set to less than 10 experience no change to alarm severity or priority.

When the accumulation counter increments to 10 (2x), the alarm severity increases to CRITICAL and the priority increases to 48.

The same behavior occurs for the next increment of 5 alarms, except that the severity remains CRITICAL because it can go no higher. Severities can go no higher than CRITICAL nor lower than INFO via escalation. Priorities can go no higher than 1 nor lower than 99 with escalation.

- **Threshold Setting (Accumulate True, Delay False):** *Accumulate* must be True and *Delay* must be False for this function to be evaluated.

  Delay and *Threshold* are mutually exclusive, with *Threshold* taking precedence if both are set.

  If the Alarm server receives an event with the threshold set and there is a matching active alarm, normal event processing related to an active alarm takes place.

  If there is no matching active alarm, events are kept in a pending state and evaluated on a sliding time scale each time a new event arrives. An alarm is created if the number of events matches the quantity threshold within the past threshold time in minutes. The alarm accumulation count is set to the quantity threshold setting.

  Threshold events are evaluated when the alarm server receives them and older pending events falling outside of the time threshold are discarded.

  The alarm’s initial date and time is set to the date and time the oldest threshold event and its most recent date and time is set to the date and time that the alarm became active.

  If the com.mosol.Eve.AlarmServer.updateAllFieldsOnAccumulation flag is True, the properties of the newest event are used to create the alarm. If the flag is False, the properties of the oldest event are used to create the alarm.

  Example: Set *Quantity* to 5 and *Threshold Time* to 2. To create an alarm, there must be five events in the past two minutes evaluated at the time of the most recent event. All five events are accumulated into a single alarm with an alarm count of 5. Events older than two minutes are discarded. Subsequent events increment the alarm counter as normal accumulated alarms.

10 Testing the Configuration

When you have a socket-based agent, the `testarc` command tests the Event Manager configuration by simulating a source that sends data to that Event Manager agent.

When an Event Manager agent is running and waiting for a socket to connect to it and send data, use the `testarc` command to simulate an incoming event stream.

- Section 10.1, “Running Testarc,” on page 103
- Section 10.2, “Running Testarc with a Command File,” on page 103
- Section 10.3, “Understanding the Testarc Command Parameters,” on page 104

10.1 Running Testarc

Running Testarc requires the creation of a file that contains data for the agent to process. For example, place alarm data in a file named `test.dat`. If the test is successful, the agent processes the alarms and displays them in the Operations Center console *Alarms* view.

To run testarc:

1 From the `/OperationsCenter_install_path/bin` directory, enter the following at the command line prompt:

```
testarc test.dat [-1|0|delay_value] hostname
[port|port_range] [-1|iterations] [-s] [socket_interval]
```

where *hostname* is the hostname being tested, and *port* is the port number where the agent is listening.

and where *test.dat* is the file with sample data to process.

For more information on the `testarc` command parameters, see Section 10.3, “Understanding the Testarc Command Parameters,” on page 104.

10.2 Running Testarc with a Command File

Running Testarc with a command file requires the creation of a command file and a file that contains data for the agent to process.

To run testarc:

1 From `the /OperationsCenter_install_path/bin` directory, enter the following at the command line prompt:

```
testarc [command_file] [socket_interval]
```

where *hostname* is the hostname being tested

where *command_file* is a file containing command lines and comments. All lines starting with \'#\' are considered comments. The command file must contain the command line to initiate connection to a listening agent's server socket, which is:

```
[test.dat] [threshold sec] [hostname] [port]|[port_range] [iterations]
[socket_interval] [-s]
```

where *hostname* is the hostname being tested, and *port* is the port number where the agent is listening.

and where *test.dat* is the file with sample data to process.

For more information on the `testarc` command parameters, see Section 10.3, “Understanding the Testarc Command Parameters,” on page 104.

10.3 Understanding the Testarc Command Parameters

Table 10-1 describes the command parameters.

Table 10-1 *Testarc Command Parameters*

Parameter	Description
test.dat	The name of the file that contains the data to send.
Threshold	The maximum time to wait between attempts to send data records. The possible values are: –1 (Uses a time delay, which simulates the actual rate the data was originally sent at.) 0 (No time delay.)
delay_value	The number of seconds to wait between each attempt to send data.
hostname	The host where the agent is running.
port | *port_range*	The ports where the agents listen. An example of the range of ports in this format: 7000–7100.
iterations	The number of times to send all data in the dump file. (-1 means loop continuously on a given file.)
-s	Do not overflow the alarm buffer.
socket_interval	The number of lines sent before the socket closes/opens. If the socket interval is not provided, a single socket opening is used.

11 Restricting Access to the Event Manager

By default, any host can connect to the Event Manager. It is possible to control the connections by restricting the host machines that access the Event Manager. Enabling the access restriction security option denies access to all hosts, except for those whose IP addresses are listed in the `eve.properties` file.

When enabling the security option, keep in mind that the restricted host machine cannot access any components of the Event Manager, including the Configuration Server, the Alarm server, and the Agent Container (and all agents housed by the Agent Container).

- Section 11.1, "Restricting Access to the Event Manager Configuration Server by Host Machines," on page 105
- Section 11.2, "Restricting Access to the Event Manager Alarm Server and the Event Manager Agent Container," on page 105

11.1 Restricting Access to the Event Manager Configuration Server by Host Machines

To restrict access to the Event Manager Configuration Server by host machines:

1. Open the `/`*`OperationsCenter_install_path`*`/config/eve.properties` file in any text editor.
2. Add the following command to specify hosts that can access the Configuration Server:

   ```
   CORBA.Allow=host IP address**
   ```

3. Stop and restart the Operations Center server.

11.2 Restricting Access to the Event Manager Alarm Server and the Event Manager Agent Container

To restrict access to the Event Manager Alarm Server and the Event Manager Agent Container (and all agents housed by the Agent Container):

1. Open the `/`*`OperationsCenter_install_path`*`/config/daemon.ini` file in any text editor.
2. Add the following command as an argument to the javaArgs property as follows:

   ```
   JavaArgs=-CORBA.Allow=any IP address** -Xmx256m
   Stop and restart the Operations Center server.
   ** IP address is for the host machines that should be allowed to access the
   Event Manager
   ```