This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") is for the end user’s informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the provisions of the license for the product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user’s responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

The use of any product referenced in the Documentation is governed by the end user’s applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Copyright © 2008 CA. All rights reserved.
Contents

Preface
Intended Audience ......................................................... v
What Is In This Guide .................................................... v
Text Conventions ......................................................... vi
Documentation Feedback ............................................... vi
Online Documentation ................................................... vii

Chapter 1: Introduction
Host System Resources Management Concepts .......................... 1
Monitoring Tasks Overview ................................................ 2
  About Creating Process and File System Monitoring Rules .......... 2
  About Using Rule Sets to Automate Monitoring Rule Creation ...... 4
  About Creating a Log File Monitor .................................... 4
Host Resources Monitoring and Service Level Agreements ................. 5
Host Resource Events and Alarms Reporting ............................ 5
Getting Started with Managing Host System Resources in OneClick ...... 5
  Access the Workspace for Creating and Managing Monitoring Rules 5
  Access the Workspace for Creating and Managing Rule Sets ...... 6
  View Monitoring Rule Information .................................... 6

Chapter 2: Process Monitoring
Create a Process Monitoring Rule ........................................ 7
Configure RFC 2790 Process Monitoring Rule Parameters ................. 9
  Process Identifier and Differentiator .................................. 9
  Alarm Conditions for RFC 2790 ....................................... 10
  Specify the Watch for New Processes Polling Interval ................ 10
NSM Agent Process Monitoring Rule Parameters .......................... 11
  Monitor Information ..................................................... 11
  Process Match Criteria ................................................ 12
  Threshold Configuration for NSM Agent ................................ 14
  Monitoring Options ..................................................... 17
  Advanced Options ..................................................... 18
  Specify the Agent Polling and Generating Alarms Options .......... 19
Edit a Process Monitoring Rule ........................................... 21
Delete a Process Monitoring Rule ......................................... 21

Chapter 3: File System Monitoring
Create a File System Monitoring Rule ..................................... 23
Edit a File System Monitoring Rule ....................................... 25
Delete a File System Monitoring Rule ..................................... 26
Chapter 4: Working with Monitoring Rule Sets

Create a Rule Set .......................................................... 27
Add a Monitoring Rule to a Rule Set ........................................... 29
Apply a Rule Set to a Global Collection ........................................ 30
Remove a Rule Set from a Global Collection ................................. 31
Edit a Rule in a Rule Set ....................................................... 32
   If You Edit a Rule Outside of the Rule Set ................................. 32
Delete a Rule from a Rule Set ................................................ 33
   If You Delete a Rule Outside of the Rule Set ............................... 33
Delete a Rule Set ............................................................ 33

Chapter 5: Log File Monitoring

About the Log File Monitoring Process ....................................... 35
Log File Syntax .................................................................. 37
Create Log File Monitors for iAgent or SystemEDGE Hosts ............ 38
Create Log File Monitors for NSM Agents .................................... 38
   Set Up a Log File Monitor for NSM Agents Using OneClick ........... 39
   Set Up a File Monitor for NSM Agents Using OneClick ................. 42
Specify a Log-to-Process Mapping ............................................. 43
   Managing Monitored Log and Process Log Mapping Settings ......... 44
Configuring SPECTRUM to Process Syslog File Matches ............... 44
   Trap Processing Overview .................................................. 45
   Processing Traps That Contain an IP Address, Host Name, or Model Handle .. 45
Creating ParseMap Files ...................................................... 45
   Enabling Event Forwarding for Agent Models ............................ 49

Chapter 6: Application Monitoring

SystemEDGE Application Insight Modules (AIMs) .......................... 51
   AIM for Apache .......................................................... 51
   AIM for Microsoft IIS .................................................... 52
   Insight AIM .............................................................. 52

Index
Preface

Intended Audience

This guide is intended for SPECTRUM administrators who want to use host system resources management tools in OneClick to complete the following tasks:

- Set up process and file system monitoring rules for hosts that support the RFC 2790 host resources MIB.
- Set up process monitoring rules on hosts that support NSM Agent.
- Set up log file monitoring on hosts that support it: iAgent, SystemEDGE, and NSM.

This guide assumes that users are familiar with SPECTRUM concepts, the OneClick user interface, and host system resource metrics.

What Is In This Guide

This guide is organized as follows:

- **Chapter 1: Introduction** provides an overview of host resources management concepts and tasks, describes the role host resources management plays in network service management, describes reporting options for host resources events and alarms, and describes how to access host resources management workspaces and views in OneClick.
- **Chapter 2: Process Monitoring** describes how to create and manage process monitoring rules for host models that support the RFC 2790 host resources MIB or NSM Agent.
- **Chapter 3: File System Monitoring** describes how to create and manage file system monitoring rules for host models that support the RFC 2790 MIB.
- **Chapter 4: Working with Monitoring Rule Sets** describes how to create rule sets, apply rule sets to Global Collection containers, and manage rule sets.
- **Chapter 5: Log File Monitoring** describes how to set up log file monitoring for iAgent, SystemEDGE, and NSM Agent host models.
Chapter 6: Application Monitoring describes the supported SystemEDGE Application Insight Modules (AIMs).

Text Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Element</th>
<th>Convention Used</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Variables</td>
<td><em>Code format and Italic in angle brackets (&lt;&gt;)</em></td>
<td>Type the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DISPLAY=&lt;workstation name&gt;:0.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>export display</td>
</tr>
<tr>
<td>The directory where you installed SPECTRUM</td>
<td><em>&lt;$SPECROOT&gt;</em></td>
<td>Navigate to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;$SPECROOT&gt;/app-defaults</td>
</tr>
<tr>
<td>Linux, Solaris, and Windows directory paths</td>
<td><em>Unless otherwise noted, directory paths are common to all operating systems, with the exception that slashes (/) should be used in Linux and Solaris paths, and backslashes () should be used in Windows paths.</em></td>
<td>&lt;$SPECROOT&gt;/app-defaults on Linux and Solaris is equivalent to &lt;$SPECROOT&gt;/app-defaults on Windows.</td>
</tr>
<tr>
<td>On-screen text</td>
<td><em>Code format</em></td>
<td>The following line displays:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>path=&quot;/audit&quot;</td>
</tr>
<tr>
<td>User-typed text</td>
<td><em>Bold format</em></td>
<td>Type the following path name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>C:\ABC\lib\db</strong></td>
</tr>
</tbody>
</table>

Documentation Feedback

To send feedback regarding SPECTRUM documentation, access the following web address:

http://supportconnectw.ca.com/public/ca_common_docs/docserver_email.asp

Thank you for helping us improve our documentation.
Online Documentation

SPECTRUM documentation is available online at the following address:

http://ca.com/support

Check this site for the latest updates and additions.
SPECTRUM OneClick provides management support for the following host system resource monitoring agents:

- CA SystemEDGE Agent
- CA Unicenter NSM System Agent
- Dell OpenManage
- HP Systems Insight Manager
- iAgent
- IBM Director
- Net-SNMP (UC Davis)
- Sun Management Center

This lets you view and evaluate relevant, up-to-date information about the status of resources on host systems in the network.

**Host System Resources Management Concepts**

The following is a list of terms and concepts that are key to understanding and working with host system resources management.

**Alarm Condition**

An *alarm condition* refers to process thresholds you specify in a RFC 2790 monitoring rule.

**Configuration Threshold**

A *configuration threshold* refers to process thresholds you specify in an NSM Agent monitoring rule.

**File System**

A *file system* is any data storage system on a host.
Monitoring Tasks Overview

Host

A host is any computer system capable of communicating with other systems in the network. In this guide, a host refers to any device modeled in SPECTRUM that supports the RFC 2790 host resources MIB, NSM Agent proprietary MIBs, or log file monitoring.

Host Resources

Host resources are the processes, file systems, processors, memory, and other host elements that can be monitored.

Host Resources Monitoring

Host resources monitoring is a mechanism that defines host resource conditions and thresholds that when met or violated result in SPECTRUM event and alarm generation. The goal of resource monitoring is to alert network administrators about significant resource events that could impact host performance and service level agreements.

Log File

A log file is any file that includes status information about a host or a host application.

Monitor Rule

A monitor rule is a configuration (a model) you create in OneClick that associates SPECTRUM alarms to resource state changes and resource activity thresholds.

Process

A process is any application that runs on a host.

Monitoring Tasks Overview

This guide provides instructions for completing the following tasks in OneClick:

- Create and manage process monitoring rules
- Create and manage file system monitoring rules
- Create process and file system monitoring rule sets that are applied to SPECTRUM Global Collection containers to automate monitoring rule creation
- Create a log file monitor

About Creating Process and File System Monitoring Rules

When you create a process or file system monitoring rule for a host model, you specify conditions that, when met, cause SPECTRUM to generate alarms. You can specify any number of available conditions when you create a monitoring rule, and you can specify whether you want SPECTRUM to generate alarms for the monitoring rule model or the host model. For more information about creating monitoring rules, see Create a Process Monitoring Rule on page 7.
RFC 2790 Host Resources MIB Monitoring Rule Alarm Conditions and Thresholds

A process monitoring rule for a host that supports the RFC 2790 host resources MIB includes the following alarm conditions:

- Process start
- Process stop
- Process instance count exceeds a certain number
- Process instance count falls below a certain number

A file system monitoring rule includes the following alarm conditions:

- File system utilization threshold is met
- File system goes offline

For more information about RFC 2790 host resources monitoring rules, see Configure RFC 2790 Process Monitoring Rule Parameters on page 9.

NSM Agent Monitoring Rule Thresholds

As indicated in the following table, the configuration thresholds you can specify for an NSM Agent process monitoring rule depend on both the host type (UNIX or Windows) for which you are creating the rule and the version (3.1 or r11) of the agent on the host.

For more information about NSM Agent monitoring rules, see NSM Agent Process Monitoring Rule Parameters on page 11.

<table>
<thead>
<tr>
<th>Configuration Thresholds</th>
<th>Platforms and NSM Agent Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UNIX r11</td>
</tr>
<tr>
<td>Children</td>
<td>X</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>X</td>
</tr>
<tr>
<td>CPU Usage Long-term</td>
<td>X</td>
</tr>
<tr>
<td>Handles</td>
<td></td>
</tr>
<tr>
<td>Instances</td>
<td>X</td>
</tr>
<tr>
<td>Restart</td>
<td>X</td>
</tr>
<tr>
<td>Runtime</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>X</td>
</tr>
<tr>
<td>Threads</td>
<td>X</td>
</tr>
</tbody>
</table>
About Using Rule Sets to Automate Monitoring Rule Creation

A rule set is a collection of monitoring rules. You can apply one or more rule sets to a Global Collections container to automate creation of monitoring rules for models in the container. When a model that supports the RFC 2790 MIB or the NSM Agent is added to the collection, monitoring rules are automatically configured on the model for any of its processes or file systems that are referenced by rules in the rule set.

For example, a rule set that includes a monitoring rule for the svchost.exe process is applied to a Global Collection. The collection is configured to add Windows hosts to it as the hosts are modeled in SPECTRUM. The monitoring rule for svchost.exe is configured on all host models added to the collection. Conversely, when the hosts are removed from the collection the monitoring rule is removed from the hosts.

Modifications you make to a rule in a rule set that is associated with a Global Collection apply to all instances of the rule. This type of rule is denoted as belonging to (or as being “owned” by) a rule set by the rule set name in the Rule Owner field in all monitored process tables and monitored file system tables in OneClick.

Continuing with the svchost.exe example, suppose you want to change an alarm condition for svchost.exe monitoring. If, for instance, the svchost.exe rule in the rule set has a maximum process count threshold of 10 and you want to change it to 12, you would change the value for the rule in the rule set. The change would apply to all svchost.exe monitoring rule instances in the collection.

For more information about setting up rule sets, see Create a Rule Set on page 27.

About Creating a Log File Monitor

Agents that support log file and syslog file monitoring use regular expressions to find log file text. Typically, you use log file monitoring to get information about system or application error conditions. Discovery of a text match results in SPECTRUM in generating an alarm on the device from which the log file entry originated.

For more information about creating log file monitors, see Chapter 5: Log File Monitoring.
**Host Resources Monitoring and Service Level Agreements**

Host resources monitoring enables you to monitor host resources that can have an impact on network services defined in a service level agreement (SLA). For example, a process monitoring rule can determine whether a virus protection process has stopped unexpectedly or whether a malicious process has started on a host. A file system monitoring rule can determine whether a disk drive or physical RAM on a host has reached or is nearing capacity. The viability of a business service may largely depend on which processes are running or not running on a host that supports the service or on whether the host provides adequate data storage capacity.

**Note:** See the *Service Manager User Guide (5155)* for details about setting up a service management system and SLAs in SPECTRUM.

**Host Resource Events and Alarms Reporting**

The SPECTRUM Report Manager application lets you generate reports on events and alarms for host models resulting from threshold violations for monitored processes and file systems and alarms generated from error messages parsed from log files. See the *Report Manager User Guide (5158)* for details about generating event and alarm reports.

**Getting Started with Managing Host System Resources in OneClick**

This section describes how to invoke workspaces where you configure monitoring rules and rule sets and views of monitored host resource information. See the *OneClick Console User Guide (5130)* for detailed information about working with OneClick Console interface elements.

**Access the Workspace for Creating and Managing Monitoring Rules**

You create and manage monitoring rules from the context of a host model that supports a monitoring agent.

**To invoke the workspace for rules**

1. Select the host for which you want to create a monitoring rule from the Contents panel.
2. Expand the System Resources option under the Information tab in the Component Detail panel.
   The Running and Monitored Processes section lets you create and manage process monitoring rules. See *Chapter 2: Process Monitoring* for details.

Access the Workspace for Creating and Managing Rule Sets

Unlike monitoring rules you create for a particular host, SPECTRUM creates rules that you specify in a rule set for any host included in a Global Collection to which the rule set has been applied. This automates the process of creating monitoring rules for multiple, different host types.

To invoke the workspace for rule sets

- Select Locater, System & Application Monitoring, All Monitoring Rules.

  The Contents panel lists any rule sets that have been created. There are no default rules sets. See Chapter 4: Working with Monitoring Rule Sets for details about creating and managing rule sets and applying them to Global Collections.

View Monitoring Rule Information

OneClick lets you view comprehensive information about monitored processes and file systems in the Component Detail panel.

To view information about a process monitoring rule

- Select Locater, System & Application Monitoring, Monitored Processes, All Monitored Processes.

To view information about a file system monitoring rule


  The view provides information about the selected host and the monitoring configuration on the host. The information provided by the view depends on the monitoring agent associated with the rule.
Chapter 2: Process Monitoring

The NSM log monitors probably won't be associated to process monitors (since we do not currently have any NSM agent process monitoring support).

A process monitoring rule specifies the criteria that, when met, causes SPECTRUM to generate alarms. This section describes how to set up process monitoring rules for host models with process monitoring agents. See Chapter 4: Working with Monitoring Rule Sets for information about setting up an automated method for creating process monitoring rules for models included in Global Collection containers.

Create a Process Monitoring Rule

You can create a process monitoring rule for a host model regardless of whether the process is currently running on the host. When you create a process monitoring rule, SPECTRUM creates a model for the rule.

To create a process monitoring rule

1. In the Contents panel, select the host model for which you want to create a monitoring rule.
2. In the Component Detail panel, in the Information tab, expand System Resources, Running and Monitored Processes.
3. Expand both Running Processes and Monitored Processes.
   
   **Note:** RFC 2790 indicates a host that supports the RFC 2790 host resources MIB.
   
   The Running Processes table lists running processes for the selected host model.
   
   The Monitored Processes table lists process monitoring rules that have been created for the selected host model.
4. Use one of the following methods to create a process monitoring rule for the selected host model:
   
   - If the process is running, right-click the process for which you want to create a process monitoring rule in the Running Processes table and select 'Monitor this process.'
Create a Process Monitoring Rule

If the process is not running and therefore not included in the Running Processes table, click Add above the Monitored Processes table. This lets you specify process monitoring rules for processes that run periodically but are not currently running that you want to know about when they start, virus scan and system maintenance processes for example.

**Note:** For NSM Agent monitoring, you must use this method when you want to create a monitoring rule that watches multiple, different processes specified by the match criteria. See [NSM Agent Process Monitoring Rule Parameters on page 11](page 11) for more information.

The Add Monitored Process dialog appears. You specify all process monitoring rule settings in the dialog. If you selected a process from the Running Processes table, the dialog includes the process name and other information. If you invoked the dialog using the Add option, you must explicitly provide all process information.

5. Configure process monitoring rule settings:

- For details, see [Configure RFC 2790 Process Monitoring Rule Parameters on page 9](page 9) if you are setting up process monitoring for agents that support the RFC 2790 host resources MIB.
- For details, see [NSM Agent Process Monitoring Rule Parameters on page 11](page 11) if you are setting up process monitoring for agents that support NSM Agent versions 3.1 or r11.

6. Click OK.

The process monitoring rule is added to the Monitored Processes table. The table columns represent predefined process identifier information specific to the monitoring agent type on the selected host. The rule applies to all identical instances of the process that satisfy the process match selection criteria.

**Note:** Local ownership in a monitoring rule indicates that the rule has been created explicitly for a particular host and is therefore not part of a rule set. For more information about rule sets, see [Chapter 4: Working with Monitoring Rule Sets](chapter 4: Working with Monitoring Rule Sets).

7. Select a destination for alarms resulting from rule violations from the Generate Alarm On drop-down list. You can specify that SPECTRUM create alarms on the process monitoring rule model or the host model.

8. Specify agent polling settings for the agent you are working with. See [Specify the Watch for New Processes Polling Interval on page 10](page 10) or [Specify the Agent Polling and Generating Alarms Options on page 19](page 19) for more information.
Configure RFC 2790 Process Monitoring Rule Parameters

**I wonder if this should just go into the procedure...it should really all be done when the rule is created, shouldn’t it? Can all this stuff be edited later? I think we may need two separate procedures in the previous section - one for RFC one for NSM where everything is described.**

You can specify the following parameters when you create process monitoring rules for hosts that support RFC 2790 monitoring:

- Process identifiers, including a process name and process differentiator
- Process start/stop and process count alarm conditions
- Polling of the Running Processes table for new instances of processes that have had monitoring rules created for them

**Process Identifier and Differentiator**

You can specify that SPECTRUM monitor all or one or more instances of a process using the following parameters:

**Process Name**

Identifies the process on the host model. You can differentiate a process instance with this setting only. You can also use it with the ‘Differentiate Processes by these Parameters’ setting to provide more precise process differentiation.

**Differentiate Processes by these Parameters**

Specifies one or more process parameters that differentiate identically named instances of the same process. You can add parameters and you can modify parameters included with a process before you save the configuration. You can differentiate a process instance with this setting only, or you can use it with the Process Name setting. See About Differentiating Processes on page 9 for more information.

**Descriptive Name**

Identifies a nickname for the process. You may want to provide a descriptive name that more clearly conveys the purpose or function of a process than its proper name, “java runtime” for the javaw.exe process for example. This setting does not serve as a process differentiator.

**About Differentiating Processes**

At any time a host can be running multiple instances of a particular process. The svchost.exe process on Windows hosts and the nfsd process on Linux and UNIX hosts are typical examples. Accordingly, you may want to consider creating a process monitoring rule that applies to all process instances, some process instances, or a single process instance. For example, if you decide to monitor all instances of svchost.exe, you would not differentiate them by parameters or names.
This means that SPECTRUM considers the alarm conditions and thresholds specified in the svchost.exe process monitoring rule applicable to all instances of the process. Assuming that the rule specifies an alarm for process starts and stops, SPECTRUM will generate an alarm for each start and stop occurrence for each instance. In other words, SPECTRUM applies the rule to each entry in the Running Processes table that matches an entry (by process name) in the Monitored Processes table.

You may, however, decide to create a rule for a particular instance or a group of identical instances of a process. In this case you would be required to differentiate the instance or group of instances from those you do not want to monitor. You could differentiate by using a unique name, parameters, or both. The differentiation options offer you the flexibility to make many different types of distinctions between process instances.

**Alarm Conditions for RFC 2790**

You can specify the following alarm conditions in an RFC 2790 monitoring rule:

**Alarm on Stop**

Specifies whether SPECTRUM generates an alarm whenever the process is stopped. SPECTRUM clears the process-stop alarm when the process starts.

**Alarm on Start**

Specifies whether SPECTRUM generates an alarm whenever the process is started. SPECTRUM clears the process-start alarm when the process stops.

**Alarm if Count is Less than**

Specifies whether SPECTRUM generates an alarm when a process instance count is less than a particular value. SPECTRUM clears the alarm when the process count is equal to or greater than the value.

**Alarm if Count is Greater than**

Specifies whether SPECTRUM generates an alarm when a process instance count is greater than a particular value. SPECTRUM clears the alarm when the process count is equal to or less than the value.

**Specify the Watch for New Processes Polling Interval**

The 'Watches for New Processes Every (seconds)' parameter lets you specify the frequency with which SPECTRUM inspects the Running Processes (RFC 2790) table for new instances of processes that are currently being watched by a monitoring rule. SPECTRUM updates the 'No. Running' parameter in the Monitored Processes (RFC 2790) table for a monitored process when it detects that a new instance of the process is running.
NSM Agent Process Monitoring Rule Parameters

Process monitoring rules are defined in the Add Monitored Process dialog, as described in Create a Process Monitoring Rule on page 7. When you create a process monitoring rule for a host that supports NSM Agent monitoring, you can specify the following parameters:

- Process monitoring rule identifiers
- Process match criteria
- Configuration threshold monitoring options
- Configuration threshold values
- Advanced options such as aggregate status evaluation policy, resource cluster group, and aggregate violation threshold

**Note:** Depending on the NSM Agent version and agent host platform you are working with, you may or may not have access to all of these settings or the options described in this section.

You can specify the agent polling interval and method for all NSM Agent versions on all platforms. For more information, see Specify the Agent Polling and Generating Alarms Options on page 19 for more information.

Monitor Information

Depending on the NSM Agent version and agent host platform you are working with, the Add Monitored Process dialog may include the following process monitoring rule identifiers:

**Monitor Name**
Identifies the name of the monitoring rule. SPECTRUM distinguishes identical monitoring rule configurations by the monitor name. This name must be unique.

**Descriptive Name**
Identifies a monitoring rule nickname or brief descriptive term.

The following table describes which attributes, or fields, uniquely identify the process monitor for each agent type.

<table>
<thead>
<tr>
<th>Version</th>
<th>Monitor Identification Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Win r11</td>
<td>Monitor Name*</td>
</tr>
<tr>
<td></td>
<td>Descriptive Name (optional)</td>
</tr>
<tr>
<td>UNIX r11</td>
<td>Monitor Name*</td>
</tr>
<tr>
<td></td>
<td>Descriptive Name (optional)</td>
</tr>
</tbody>
</table>
**Process Match Criteria**

Before you can implement a process monitoring rule on an NSM agent, you must identify the process or processes you want SPECTRUM to evaluate according to the threshold criteria. You can do this using regular expressions and string comparisons to identify processes.

**Important**! The r11 agent supports regex for match criteria, but the 3.1 agent supports wildcard (*) use only.

The following table describes which attributes, or fields, are used as process matching criteria for each type of NSM agent.

**Note:** For r11 NSM Agents, Match Type applies to the combination of all the other match criteria attributes. It defines how the combination of the other process match fields are evaluated.

<table>
<thead>
<tr>
<th>Version</th>
<th>Monitor Identification Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Win 3.1</td>
<td>Process Name* Path* User* Descriptive Name (optional)</td>
</tr>
<tr>
<td>UNIX 3.1</td>
<td>Process Name* Parameters * Path * User *</td>
</tr>
</tbody>
</table>

* Uniquely identifies the process monitor.
Depending on the NSM Agent version and agent host platform you are working with, the Add Monitored Process dialog may include the following fields and options:

**Process Name**
Identifies the process or processes text pattern to match. You can use literal string identifiers or regular expressions to specify a text search pattern.

**Match Type**
Lets you specify the process or processes that match or do not match the process match criteria.

*Note:* Process Name match criteria are case-insensitive.

Options include:

- **positive-regular-expression**
  The agent searches for processes that match the process name as a regular expression.

- **negative-regular-expression**
  The agent searches for processes that do not match the process name as a regular expression.

- **positive-string-compare**
  The agent searches for processes that match the process name as a string comparison.

- **negative-string-compare**
  The agent searches for processes that do not match the process name as a string comparison.

**Parameters**
Identifies the process arguments to match. You can specify parameters as a literal string or a regular expression depending on the version of NSM and the platform you are using.

**Path**
Identifies the path name of the process or processes to match. You can specify paths as a literal string or a regular expression.

**User**
Identifies the user name of the process account to match. You can specify user names as a literal string or a regular expression depending on the version of NSM and the platform you are using.

*Note:* All processes matching the name in the Process Name field are monitored if no other process match criteria is specified.
Threshold Configuration for NSM Agent

Threshold configuration defines what is watched by the monitor. You can specify any number of thresholds when you create a monitoring rule. For example, you may want the monitor to only watch how much CPU time a process consumes. Or you may want the monitor to watch CPU usage and process children, threads and handles, and also how often a process restarts.

SPECTRUM generates Major (Orange) alarms for violations of warning thresholds and Critical (Red) alarms for violations of critical thresholds. Whether SPECTRUM generates alarms depends on the overall status of the monitoring rule.

The thresholds you can specify depend on the host platform (Windows or UNIX) and the NSM Agent version (3.1 or r11) running on the host.

The following table describes what threshold and monitoring options are available for each NSM agent.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Monitoring Options Platform and Agent Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Win r11</td>
</tr>
<tr>
<td>Children</td>
<td>do-not-monitor</td>
</tr>
<tr>
<td>CPU Usage</td>
<td>do-not-monitor</td>
</tr>
<tr>
<td>CPU Usage Long-term</td>
<td>N/A</td>
</tr>
<tr>
<td>Handles</td>
<td>do-not-monitor</td>
</tr>
<tr>
<td>Instances</td>
<td>do-not-monitor</td>
</tr>
<tr>
<td>Restart</td>
<td>do-not-monitor</td>
</tr>
</tbody>
</table>
**NSM Agent Process Monitoring Rule Parameters**

**Note:** Specifying the value ‘-1’ for a particular minimum or maximum value threshold disables the threshold. It lets you selectively specify that you want the monitor to watch, for example, a minimum threshold but not a maximum threshold or vice versa.

**Size**

Specifies whether the monitor watches the amount of memory (in kilobytes) a process consumes.

**CPU Usage/CPU Shortterm Usage/CPU Longterm Usage**

Specifies whether the monitor watches the amount of CPU time a process consumes.

Some of the available options include:

**Warning Threshold**

This value can be between one (1) and ninety-nine (99) percent, but it must be less than the critical threshold percent value. If there is more than one process instance, the maximum of all instances is compared with this value.

**Critical Threshold**

This value can be between two (2) and one hundred (100) percent, but it must be greater than the warning threshold percent value. If there is more than one process instance, the maximum of all instances is compared with this value.

**CPU Interval**

This value defines the total value in seconds to use as the base for the calculation of the CPU value. In other words, the CPU usage of a process, in seconds, refers to this interval. You can set the value to any value greater than zero (0) or -1.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Monitoring Options</th>
<th>Platform and Agent Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Win r11</td>
</tr>
<tr>
<td>Runtime</td>
<td>do-not-monitor</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>down-warning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>down-critical</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>do-not-monitor</td>
<td>do-not-monitor</td>
</tr>
<tr>
<td></td>
<td>warning-only</td>
<td>down-warning</td>
</tr>
<tr>
<td></td>
<td>critical-only</td>
<td>down-critical</td>
</tr>
<tr>
<td></td>
<td>minimum-only</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>maximum-only</td>
<td></td>
</tr>
<tr>
<td>Threads</td>
<td>do-not-monitor</td>
<td>do-not-monitor</td>
</tr>
<tr>
<td></td>
<td>down-warning</td>
<td>down-warning</td>
</tr>
<tr>
<td></td>
<td>down-critical</td>
<td>down-critical</td>
</tr>
</tbody>
</table>
– If set to -1, the CPU value is calculated as the CPU usage, in seconds, used up to the current time since the start of the agent or the creation of the process monitoring rule.
– If the CPU interval is set to a value greater than the current agent polling interval and this time has not elapsed for the first time, the CPU value is extrapolated.
– If the CPU interval is set to a value smaller than the current agent polling interval, the CPU value is calculated as the appropriate fraction of the value for the last agent polling interval.
– If the CPU interval is set to a value greater than the current agent polling interval and this time has already elapsed, the CPU value is calculated as the sliding sum (the sum of the value for the current poll interval and the value calculated at the last poll) weighted according to its fraction of the CPU interval.
– If the interval is set to -1, any overloading (%) used for the thresholds are ignored.

Min/Max Units
The unit of measure, in seconds or as a percentage, used for CPU usage thresholds.

Children
Specifies whether the monitor watches the process children count.

Note: For version r11 on Windows, this option is in the Resources, Type drop-down list.

Instances
Specifies whether the monitor watches the process instance count.

Threads
Specifies whether the monitor watches the process thread count.

Note: For version r11 on Windows, this option is in the Resources, Type drop-down list.

Restart
Specifies whether the monitor watches the process restart count and determines which policy the agent uses to determine when it should set the status of the restart alarm condition to down for a threshold violation.

none-should-stop-or-start
Sets the status to down if any process stops or starts.

none-should-stop
Sets the status to down if any process stops.

none-should-start
Sets the status to down if any process starts.

some-should-continue
Sets the status to down if all processes stop.
Resources
Specifies whether the monitor watches one of the following resources:

**threads**
Specifies the process thread count.

**handles**
Specifies the total number of handles currently opened by each thread in the process.

**children**
Specifies the process children count.

**runtime**
Specifies the time, in seconds, the process has been running since it was created.

Monitoring Options

A monitoring option specifies whether the NSM Agent watches a particular configuration threshold and which threshold types (warning or critical, minimum or maximum values) to watch.

Monitor drop-down lists in the Add Monitored Process dialog contain the following options depending on the host platform (Windows or UNIX), the NSM Agent version (3.1 or r11), and the particular alarm condition you are configuring:

**do-not-monitor**
No alarm. The agent disregards threshold settings.

**monitor**
Critical alarm. The agent monitors minimum and maximum values for all thresholds.

**warning-only**
Major alarm. The agent evaluates only the warning thresholds (both minimum and maximum) to determine the status of the process.

**critical-only**
Critical alarm. The agent evaluates only the critical thresholds (both minimum and maximum) to determine the status of the process.

**minimum-only**
Major (warning) and Critical (critical) alarms. The agent evaluates only the minimum thresholds (both warning and critical) to determine the status of the process.

**maximum-only**
Major (warning) and Critical (critical) alarms. The agent evaluates only the maximum thresholds (both warning and critical) to determine the status of the process.
**NSM Agent Process Monitoring Rule Parameters**

- **all**
  Major (warning) and Critical (critical) alarms. The agent evaluates all thresholds.

- **down-warning**
  Major alarm. The agent uses a warning severity if the resource is in a bad condition. This lets you designate a threshold violation as less crucial than a down-critical violation.

- **down-critical**
  Critical alarm. The agent uses a critical severity if the resource is in bad condition. This lets you designate a threshold violation as more crucial than a down-critical violation.

- **both**
  Major (warning) and Critical (critical) alarms. The agent evaluates both warning and critical thresholds to determine the status of the process.

**Advanced Options**

Advanced options let you specify an evaluation policy for configuration threshold violations when the monitor watches two or more processes, a process resource cluster group, and an aggregate alarm condition violation threshold that when met degrades the status of a process and triggers SPECTRUM alarm generation.

**Note:** The advanced options available depend on which host platform (Windows or UNIX) and NSM Agent version (3.1 or r11) you are configuring.

**Evaluation Policy (r11 only)**

Specifies how the agent calculates values that it compares to alarm condition thresholds for a monitor that watches multiple, different processes. It also specifies which other processes are included in the threshold violation culprits list.

**Note:** NSM Agent version 3.1 compares the worst values (the individual policy) from all watched process instances to alarm condition thresholds to determine threshold compliance.

Evaluation Policy options include:

- **individual (default)**
  Specifies that the agent compares the worst values (lowest and/or highest) of all process instances to alarm condition threshold values. If a value violates a threshold condition, the culprits list includes all instances individually violating the most severe threshold.

- **min**
  Specifies that the agent compares the lowest values (minimum) of all process instances to alarm condition threshold values. If a value violates a threshold condition, the culprits list includes all instances with the same minimum value.
**max**

Specifies that the agent compares the highest values (maximum) of all process instances to alarm condition threshold values. If a value violates a threshold condition, the culprits list includes all instances with the same maximum value.

**sum**

Specifies that the agent compares the cumulative values (sum) of all process instances to alarm condition threshold values. If a value violates a threshold condition, the culprits list includes all instances.

**avg**

Specifies that the agent compares the average values of all process instances to alarm condition threshold values. If a value violates the threshold condition, the culprits list includes all instances individually violating the most severe threshold.

**Cluster Resource Group (r11 only)**

Identifies the cluster resource group.

**Aggregate Violation Threshold**

Specifies the consecutive number of agent polling cycles for which any threshold is required to be in a less-than-ok state before the aggregate status for the monitor changes. This value must be greater than 0. The Aggregate Violation Threshold field is not available for UNIX 3.1.

The Status field in the Monitored Processes table for the selected host model indicates the aggregate status condition.

---

**Specify the Agent Polling and Generating Alarms Options**

Use the following parameters, found above the Monitored Processes table, to specify alarm generation, agent polling interval, and agent polling method:

**Generate Alarm On**

Specifies a destination for alarms resulting from rule violations. You can specify that SPECTRUM create alarms on the process monitoring rule model or the host model.

**Agent Poll Interval (seconds)**

Specifies the frequency with which the agent collects process information from the host device. The minimum value is 30 seconds.

**Agent Poll Method**

Specifies how and when the agent collects process data:

**disabled**

The agent does not retrieve process information (neither by polling nor by get request), and it sets all status indications for alarm conditions to passive or ok.
**poll-interval-and-query**

The agent retrieves process information both by polling and by get request.

**poll-interval-only**

The agent retrieves process information by polling only.

**query-only**

The agent retrieves process information by get request only.

---

**If the NSM Agent Fails to Retrieve Process Information**

If the NSM Agent subagent responsible for retrieving process monitoring information goes down, SPECTRUM responds as follows:

- Generates an NSM PROCESS MONITORING AGENT LOST alarm on the host model
- Asserts a suppressed APPLICATION_LOST alarm condition on the process models

When the process monitoring subagent restarts, SPECTRUM clears the NSM PROCESS MONITORING AGENT LOST alarm on the host model and the APPLICATION_LOST alarms on the associated process models.

---

**Status Indications for NSM Agent Process Monitoring Rules**

The Status field in the Monitored Processes table for the selected host model indicates the aggregate status condition of the monitor. It represents the worst case aggregate for the status values of each threshold defined on the monitor. Whether the aggregate status is in a less-than-ok state is dependent on whether any threshold is in a violated state over a particular number of consecutive agent polling cycles. The Aggregate Violation Threshold field defines the number of consecutive times that any threshold is in a violated state before the aggregate status value changes. SPECTRUM does not generate alarms for violated thresholds until the aggregate status is in a less-than-ok state.
Edit a Process Monitoring Rule

You can edit local process monitoring rules and rules owned by rule sets in the context of a host model. In the latter case, the modification transforms the ownership of the rule from the rule set to the model (Rule Owner value converts to Local).

To edit a process monitoring rule

1. In the Contents panel, select the model with the process monitoring rule you want to edit.
2. In the Component Detail panel, in the Information tab, expand System Resources, Running and Monitored Processes, Monitored Processes.
   The Monitored Processes table lists process monitoring rules for the selected model.
3. Select the process monitoring rule you want to edit, and then click Edit.
   The Edit Monitored Processes dialog appears.
4. Modify the settings as required, and then click OK.
   Changes to the process monitoring rule for the selected model take effect immediately.

Delete a Process Monitoring Rule

You can delete local process monitoring rules and rules owned by rule sets for a host model. In the former case, monitoring stops for the process. In the latter case, the deletion also stops monitoring for the particular model by the rule from the rule set. However, the deletion of a rule set rule is temporary because process monitoring specified by the rule is re-established the next time the rule set is updated. See If You Delete a Rule Outside of the Rule Set on page 33 for more information.

When you delete a process monitoring rule, SPECTRUM and the process monitoring agent stop monitoring all identical (non-differentiated) instances of the process specified in the rule, and the monitoring rule is removed from the agent MIB.

To delete a process monitoring rule

1. In the Contents panel, select the model with the process monitoring rule you want to delete.
2. In the Component Detail panel, expand System Resources, Running and Monitored Processes.
3. Expand Monitored Processes.
   The Monitored Processes table lists process monitoring rules for the selected model.
4. Select the process monitoring rule you want to delete, and then click Delete. A confirmation message prompts you to proceed or dismiss the deletion.

5. Respond affirmatively to the confirmation message to delete the process monitoring rule.
   Process monitoring specified by the rule for the selected model stops immediately.
A file system monitoring rule (RFC 2790) specifies file system alarm conditions that cause SPECTRUM to generate alarms when the conditions occur on a host model for which the rule is created:

- File system utilization
- File system goes offline

This section describes how to set up file system monitoring for particular host models. See Chapter 4: Working with Monitoring Rule Sets for information about automating the creation of file system monitoring rules for models in Global Collection containers.

Create a File System Monitoring Rule

When you create a file system monitoring rule, you can specify any file system whether it is currently online or offline. When you create a file system monitoring rule, SPECTRUM creates a model for the rule.

When you create a file system monitoring rule, you define the alarm conditions that cause SPECTRUM to generate alarms. Examples of such alarm conditions may include system utilization thresholds or file system goes offline.

**To create a file system monitoring rule**

1. In the Contents panel, select the model with the file system you want to monitor.
2. In the Component Detail panel, expand System Resources, File Systems.
   - The File Systems (RFC 2790) table lists file systems for the selected model, and the Monitored File Systems (RFC 2790) table lists file system monitoring rules that have been created for the selected model.
4. Use one of the following methods to create a file system monitoring rule for the selected model:
If the file system you want to monitor is available, right-click the file system in the File Systems (RFC 2790) table and choose Monitor this File System.

If the file system is not available and therefore not included in the File Systems (RFC 2790) table, click Add on the Monitored File Systems (RFC 2790) table. This lets you specify, for example, a file system that is currently offline that you want to know about and monitor when it does come online.

The Add File System Monitor dialog appears. If you selected a file system from the File Systems (RFC 2790) table, the box includes the file system name.

5. Configure the settings as desired. Some of the settings are described here:

**File System Name**
- Specifies the file system. If you add a file system to monitoring that is not currently available, you must type the name. If you added an available file system, the name is entered automatically.

**Description**
- Specifies a nickname, or alias, for the file system.

**Threshold Type**
- Specifies whether to monitor file system utilization thresholds in terms of capacity percentage or unit of storage (Bytes, Kbytes, Mbytes, Gbytes, Tbytes).

**Utilization Thresholds**
- Specifies thresholds for events, minor alarms, major alarms, and critical alarms. SPECTRUM clears threshold alarms when thresholds are no longer exceeded.

**Alarm if Offline**
- Specifies whether SPECTRUM generates an alarm if the file system goes offline. SPECTRUM clears the alarm when the file system comes back online.

6. Click OK.

The file system monitoring rule is added to the Monitored File Systems (RFC 2790) table. SPECTRUM generates alarms in response to the alarm condition threshold violations specified in the rule.

**Note:** A value of “Local” in the Rule Owner field of a monitoring rule indicates that the rule has been created explicitly for a particular host and is therefore not part of a rule set. For more information about rule sets, see Chapter 4: Working with Monitoring Rule Sets.

7. Select a destination for alarms resulting from rule violations from the Generate Alarm On drop-down list. You can specify that SPECTRUM create alarms on the monitoring rule model or the host model.
Edit a File System Monitoring Rule

You can edit local file system monitoring rules and rules owned by rule sets for a host model. In the latter case, the modification transforms the ownership of the rule from the rule set to the model (Rule Owner value converts to Local). However, the edits and ownership conversion are temporary because the original rule specifications and ownership are re-established the next time the rule set is updated. See If You Edit a Rule Outside of the Rule Set on page 32 for more information.

To edit a file system monitoring rule

1. In the Contents panel, select the model with the file system monitoring rule you want to edit.
2. In the Component Detail panel, expand System Resources, File Systems.
4. Select the file system rule you want to edit, and then click Edit.
   The Edit File System Monitor dialog appears. Immutable settings are grayed out.
5. Modify settings as required, and then click OK.
   Changes to the file system monitoring rule for the selected model take effect immediately.
Delete a File System Monitoring Rule

You can delete local file system monitoring rules and rules owned by rule sets for a host model. In the former case, monitoring stops for the file system. In the latter case, the deletion also stops monitoring for the particular model by the rule from the rule set. However, deletion of a rule set rule is temporary because file system monitoring specified by the rule is re-established the next time the rule set is updated. See If You Delete a Rule Outside of the Rule Set on page 33 for more information.

To delete a file system monitoring rule

1. In the Contents panel, select the model with the file system monitoring rule you want to delete.
2. In the Component Detail panel, expand System Resources, File Systems.
4. Select the file system monitoring rule you want to delete, and then click Delete.
   A confirmation message prompts you to proceed or dismiss the deletion.
5. Respond affirmatively to the confirmation message to delete the file system monitoring rule.
   File system monitoring specified by the rule for the selected model stops immediately.
A rule set is a collection of monitoring rules for processes and file systems you can apply to a Global Collection. This automates the process of setting up and managing monitoring for hosts modeled in SPECTRUM. When you create a process or file system monitoring rule for a particular host model, that rule applies only to that host model. If you want to apply the same rule to other host models, you must create the same rule again and again for each host model. If you want to edit the rule for all models, you must modify each and every instance of the rule for each host model. This is obviously a tedious and inefficient way to manage host monitoring for numerous host models.

By applying rule sets to Global Collections, you leverage a more efficient method of managing IT infrastructure resources. When host models are added to a collection, SPECTRUM creates monitoring rules that reference the processes or file systems for those models. Furthermore, when monitoring rules in rule sets are modified, the modifications apply to all host models in the collection. When host models are removed from a collection, all monitoring rules for the models are removed as well.

Create a Rule Set

You can create rule sets that contain multiple monitoring rules for both host processes and file systems, or you can create rule sets that include one or the other. You can apply as many rule sets as you want to a Global Collection, and you can apply the same rule set to multiple collections.

Plan your rule set implementation carefully to avoid duplicating rules or implementing conflicting rules. Also, verify that the Global Collections to which you apply rule sets include the host models that are germane to the monitoring rules in the rule sets.
As you create rule sets, keep the following in the mind:

- Rule sets must have unique names.
- Rules included in rule sets do not override identically named local monitoring rules for host models included in Global Collections. If a local monitoring rule has been created for a particular host model and the model is included in a Global Collection that has a rule set applied to it which contains an identically named rule, the local rule is preserved and remains in effect for the model.

To create a rule set

1. Select Locator, System & Application Monitoring, All Monitoring Rules. The Contents panel lists any rule sets that have been created.
   
   **Note:** There are no default rule sets.

2. Click (Create a New Rule Set by Type) and then select one of the following options, depending on the agent you are working with:
   - RFC2790
   - NSM Agent:
     - r11 Windows
     - r11 UNIX
     - 3.1 Windows
     - 3.1 UNIX
   
   The 'New Rule Set' dialog appears.

3. Type a name for the rule set in the Rule Set Name field, and then click OK.
   
   The new rule set appears in the list of rule sets. You can now add process monitoring and file system monitoring configuration rules to the rule set and apply the rule set to a Global Collection container.
Add a Monitoring Rule to a Rule Set

You can add monitoring rules to a rule set before or after the rule set has been applied to a Global Collection.

To add a monitoring rule to a rule set

   The Contents panel lists rule sets.
   Note: If there are no rule sets listed, you must create a rule set for the rule you want to add as described in Create a Rule Set on page 27.
2. Select the rule set to which you want to add the monitoring rule.
   The Component Detail panel displays information about the rule set.
3. In the Component Detail panel, in the Information tab, specify the type of rule you want to add to the rule set:
   - To add a process monitoring rule, expand Process Monitoring Rules.
   - To add a file system monitoring rule, expand File System Monitoring Rules.
   Note: The NSM rule sets do not support file system monitoring rules.
   Each rules table lists rules that have been added to the rule set.
4. Click Add for the type of rule you want to add to the rule set.
   - If you click Add for Process Monitoring Rules, the Add Monitored Process dialog appears.
   - If you click Add for File System Monitoring Rules, the Add File System Monitor dialog appears.
5. Configure settings.
   - See Create a Process Monitoring Rule on page 7 for information about creating a process monitoring rule.
   - See Create a File System Monitoring Rule on page 23 for information about creating a file system monitoring rule.
6. Click OK.
   The rule is added to the rule set.
Apply a Rule Set to a Global Collection

Applying a rule set to a Global Collection automates the process of creating monitoring rules. SPECTRUM automatically creates monitoring rules for all models in the Global Collection.

As you apply rule sets to Global Collections, consider the following:

- If you remove models from the Global Collection, all monitoring rules specified by the rule set are removed from the models.
- If you edit a rule from a rule set for a particular model that is included in a Global Collection, the rule’s ownership changes to local ownership. This means the rule is no longer associated with the rule in the rule set and applies only to that particular model.
- If you delete a rule set that is associated with a Global Collection or vice versa, the rules specified by the rule set are removed from the models in the collection.

To apply a rule set to a Global Collection

   **Note:** If there are no rule sets listed, you must create a rule set as described in Create a Rule Set on page 27.

2. Right-click the rule set or sets you want to apply to a Global Collection and select Apply/Remove Global Collection(s).
   The ‘Apply and Remove Collection(s) to/from the Rule Set’ dialog appears.

   **Note:** You can also click in the Results tab toolbar to launch this dialog.

   All the Global Collections listed in the left side of the dialog are currently applied to the selected rule set. All the Global Collections listed on the right side of the panel have not been applied to the selected rule set.

3. In the Not Applied To list, double-click the Global Collection to which you want to apply the rule set.
   The selected Global Collection is moved to the Applied To list on the left side of the dialog.

   **Note:** This dialog only works for one selected rule set at a time. You cannot apply Global Collections to multiple rule sets at one time.

4. (Optional) Select the Reapply check box to have the Global Collection or Collections that were already applied to the rule set *reapplied* when you click OK in the ‘Apply and Remove Collection(s) to/from the Rule Set’ dialog.

5. Click OK to apply your changes.

   **Note:** Only the changes you made in the dialog are applied. A Global Collection that already appears in the Applied To list is not reapplied unless you have selected the Reapply check box.
The Applied Global Collections List section in the selected rule set’s Information tab shows the Global Collections to which it is applied.

Remove a Rule Set from a Global Collection

When you remove a rule set from a Global Collection, SPECTRUM removes monitoring rules in the rule set from all models in the Global Collection.

**To remove a rule set from a Global Collection**

2. Right-click the rule set or sets from which you want to remove a Global Collection and select Apply/Remove Global Collection(s). The ‘Apply and Remove Collection(s) to/from the Rule Set’ dialog appears.

**Note:** You can also click ![icon] in the Results tab toolbar to launch this dialog.

All the Global Collections listed in the left side of the dialog are currently applied to the selected rule set. All the Global Collections listed on the right side of the panel have not been applied to the selected rule set.

3. In the Applied To list, double-click the Global Collection that you want to remove from the rule set.

The selected Global Collection is moved to the Not Applied To list on the right side of the dialog.

**Note:** This dialog only works for one selected rule set at a time. You cannot remove Global Collections from multiple rule sets at one time.

4. (Optional) Select the Reapply check box to have the Global Collection or Collections that were already applied to the rule set reapplied when you click OK in the ‘Apply and Remove Collection(s) to/from the Rule Set’ dialog.

5. Click OK to apply your changes.

**Note:** Only the changes you made in the dialog are applied. A Global Collection that already appears in the Applied To list is not reapplied unless you have selected the Reapply check box.

The Applied Global Collections List section in the selected rule set’s Information tab is updated and no longer displays the Global Collection or Collections that you removed.
Edit a Rule in a Rule Set

When you edit a rule in a rule set that is applied to a Global Collection, the revised rule settings extend to all models in the Global Collection.

To edit a rule in a rule set

   The Contents panel lists rule sets.
2. Select the rule set with the rule you want to edit.
   The Component Detail panel displays information about the rule set.
3. In the Component Detail panel, specify the type of rule you want to edit:
   - To edit a process monitoring rule, expand Process Monitoring Rules.
   - To edit a file system monitoring rule, expand File System Monitoring Rules.
   Each rule type table lists rules that have been included in the rule set.
4. Select the rule you want to edit, and then click Edit.
   The Edit dialog for the rule you selected appears.
   **Note:** Some settings will be unavailable for edit.
5. Edit settings, and then click OK.
   The modified settings take effect immediately.

If You Edit a Rule Outside of the Rule Set

Under some circumstances you may want to edit a monitoring rule for a particular model in a Global Collection and that rule belongs to a rule set that has been applied to a Global Collection. Moreover, you do not want the modification to apply to the rule in the rule set and thus apply to all models in the Global Collection and, for various reasons, you also want to keep the model in the collection.

In this case you want to convert the rule to a local version for the model. You can modify this rule from the context of the particular model outside of the rule set to achieve this result.
Delete a Rule from a Rule Set

When you delete a rule from a rule set that is applied to a Global Collection, the rule is removed from all models in the Global Collection.

To delete a monitoring rule from a rule set

2. Select the rule set with the rule you want to delete. The Component Detail panel displays information about the rule set.
3. In the Component Detail panel, specify the type of rule you want to delete from the rule set:
   - To delete a process monitoring rule, expand Process Monitoring Rules.
   - To delete a file system monitoring rule, expand File System Monitoring Rules.
   Each rule table lists rules that have been included in the rule set.
4. Select the rule you want to delete, and then click Delete. The rule is removed from the rule set and from its rule table.

If You Delete a Rule Outside of the Rule Set

Under some circumstances you may want to delete a rule for a particular model in a Global Collection and that rule belongs to a rule set that is applied to a Global Collection. Moreover, you do not want to delete the rule in the rule set and thus delete it for all models in the Global Collection and, for various reasons, you also want to keep the model in the collection.

In this case you would delete this rule from the context of the particular model outside of the rule set to achieve the desired result. When the association between the rule set and the Global Collection is updated, however, the deleted rule is re-created for the model.

Delete a Rule Set

When you delete a rule set that is applied to a Global Collection, all rules in the rule set are removed from the models in the collection.

To delete a rule set

1. Select Locator, System & Application Monitoring, All Monitoring Rules. The Contents panel lists all available rule sets.
2. Select the rule set you want to delete, and then click Delete.
Delete a Rule Set
Chapter 5: Log File Monitoring

This chapter describes how to set up log file monitoring in OneClick for the following agents:

- iAgent
- CA SystemEDGE Agent
- CA Unicenter NSM Agent

It also describes how to configure iAgent syslog server monitoring and trap forwarding to SPECTRUM.

Setting up log file monitoring involves the following tasks:

- Specifying the criteria that initiates trap and event generation when the type of information you want to know about is detected in a log file.
- (Optional) Specifying an association between a log file and a monitored process model so that events generated in response to a log file entry pertaining to the process model are generated on the process model instead of on the process host model.

About the Log File Monitoring Process

You may have various devices on your network that send data to log files on an iAgent, SystemEDGE agent, or NSM server, or you may have applications on one of these servers that sends data to a log file. In either case, these agents can be configured to monitor these log files and generate SNMP traps based on the content found in a log file entry.

Log file monitoring involves setting up a text pattern matching system that detects and parses the type of information you want to know about from log files. Then, the monitoring agent sends a trap to SPECTRUM that contains data about the parsed text. This data is then mapped to a SPECTRUM event and an alarm is asserted on the agent model or the device or process to which it
About the Log File Monitoring Process

pertain. You can also configure SPECTRUM to create a more granular event, and optionally an alarm, from the “text match in log file” event using an event condition rule. See the Event Configuration User Guide (5188) for details. The result is that you receive notification about events that have occurred in your infrastructure that indicate potential or actual problems.

The log file that you are monitoring will have a syntax that is dependent on the type of log file and the data being sent to the log file. Because application log files are matched directly to the application you are monitoring, no special log file syntax is required. However, SPECTRUM processes log files that gather data from other devices differently. Therefore, these log file entries must follow certain syntax criteria. For more information, see Log File Syntax on page 37.

Regardless of the type of log file you want to monitor, whether a log file for a particular application or a syslog file containing log file entries for multiple applications from multiple devices, you must define a regular expression (regex) that identifies, or parses, the type of information you want to know about. The regex syntax must be compatible with the type of agent for which you are creating the monitoring configuration. When the regex discovers matching text, the monitoring agent sends a trap to SPECTRUM that contains the matching text. Then, SPECTRUM associates the trap to an event that is asserted on the host model.

Note: See the Event Configuration User Guide (5188) for more information about defining regular expressions.

The Configuring SPECTRUM to Process Syslog File Matches on page 44 section explains how to configure an agent to monitor log files for strings of information that will generate a trap.

Note: iAgent can only monitor log files that exist on the iAgent server. It cannot monitor log files on a mapped network drive.
Log File Syntax

You can monitor application logs or log files that receive data from other devices, such as Syslog files. No special syntax is required for log files that monitor application logs. However, for SPECTRUM to assert the trap information on the appropriate device model, log files that receive information from devices on the network must have the following format, which is generally based on the BSD Syslog and Cisco IOS format:

\[
\text{<MessagePrefix>}%\text{<MessageHeader>\text{<Additional_Information>}}
\]

Where:

\[
\text{<MessagePrefix>}
\]
contains the date and time of the message and the IP address or the host name of the source of the information contained in the entry. There can be other information interspersed within the prefix, but it must contain these two pieces of information.

Note: If a host name is used to identify the source, it can be of the form myhost.ca.com or myhost.

\[
\text{<MessageHeader>}
\]
must have the format \(\text{<A>-<B>-<C>}\)

Where:

\[
\text{<A>}
\]
contains any number of uppercase alpha characters, underscores, or the string "Aprisma."

\[
\text{<B>}
\]
contains any number of uppercase alpha characters, numeric characters, or underscores.

\[
\text{<C>}
\]
contains any number of uppercase alpha characters, underscores, or dashes.

\[
\text{<Additional_Information>}
\]
can contain any data.

In general, this syntax can be found in the following types of log files:

- Solaris syslog file entries from a Cisco or Riverstone device.
- Solaris syslog file entries from another type of device that uses the \(\text{<MessageHeader>}\) format described previously.
- Kiwi syslog file entries from a Cisco or Riverstone device.
- Kiwi syslog file entries from another type of device that uses the \(\text{<MessageHeader>}\) format described previously.
- CA log files, for example those generated by SPECTRUM Report Gateway.

Note: For information about configuring SPECTRUM to process iAgent traps, see Configuring SPECTRUM to Process Syslog File Matches on page 44.
Create Log File Monitors for iAgent or SystemEDGE Hosts

The following procedures describe how to set up log file monitoring for iAgent or SystemEDGE host agents. For information about setting up log file monitoring for CA Unicenter NSM Agents, see Create Log File Monitors for NSM Agents on page 38.

To set up a log file monitor for an iAgent or SystemEDGE host

1. In the Contents panel, select the model with the log file you want to monitor.
2. In the Component Detail panel, in the Information tab, expand System Resources, Monitored Logs and Process Logs, Monitored Logs.
   
   **Note:** Some list fields are agent-specific.

3. Click Add in the Monitored Logs list.
   The Add Log File Monitor dialog for the agent you are working with appears.

4. Configure log file monitor settings as needed, paying particular attention to the following mandatory and optional settings:

   - **Log File Name**
     Identifies the monitored log file.

   - **Regular Expression**
     Identifies the text patterns to parse in the log file.
     
     **Note:** For more information about defining regular expressions, see the Event Configuration User Guide (5188).

   - **Description**
     Any brief annotation you want to provide that indicates to other users the monitor’s purpose.

   - **Send Trap on Match/Send Trap**
     Specifies whether the agent sends a trap to SPECTRUM when the regular expression detects a matching text pattern.

5. Click OK.
   The monitoring configuration is added to the Monitored Logs list, and monitoring begins immediately.

Create Log File Monitors for NSM Agents

You can set up log file monitoring and file monitoring for NSM Agents in OneClick. The following describes how these two monitors are different:

**NSM Log File Monitor**

An NSM Log File Monitor watches to contents of a file for specific patterns.
**NSM File Monitor**

An NSM File Monitor simply watches for the existence or non-existence of a file.

Once you set up NSM Agent log file monitoring, you can perform the following tasks.

- Edit and view file monitors for NSM Agents
- Edit and view log monitors for NSM Agents
- View status changes for file and log monitors for NSM Agents

**Set Up a Log File Monitor for NSM Agents Using OneClick**

**To set up log file monitoring for NSM host agents**

1. In the Contents panel, select the model with the log file you want to monitor.
2. In the Component Detail panel, in the Information tab, expand System Resources, Monitored Logs and Files.
3. Expand Monitored Logs and then click Add in the Monitored Logs list. The Add Log File Monitor dialog appears.
4. Configure log file monitor settings as needed, including the following:

   **Monitor Name**
   - Identifies the name of this log file monitor.

   **File Name**
   - Identifies the full path and file name (or wildcarded file name) of the log file to monitor.

   **Positive Pattern**
   - If the specified regular expression is found in the file, the monitor transitions to a DOWN state.

   **Negative Pattern**
   - If the specified regular expression is *not* found in the file, the monitor transitions to a DOWN state.

   **Toggle Positive Pattern**
   - If the specified regular expression is found in the file, the monitor transitions to an UP state. This field is only available when the Status Policy is toggled or toggledEOF.

   **Toggle Negative Pattern**
   - If the specified regular expression is *not* found in the file, the monitor transitions to an UP state. This field is only available when the Status Policy is toggled or toggledEOF.

   **Start**
   - The starting character position.
End
The ending character position.

Status Policy
The Status Policy attribute defines how the monitor handles files. Options include:

poll
The monitor’s status is set to UP at the beginning of each poll. If a match is made the state changes to DOWN. The file is scanned from the last read location unless it is a new monitor, in which case the entire file is read.

historical
The monitor’s status is set to DOWN when a match occurs and will remain DOWN for the life of the log file, hence, the log file is recreated. The file is scanned from the last read location unless it is a new monitor, in which case the entire file is read.

startFromPreviousRead
The monitor’s status is set to DOWN when a match occurs and will remain DOWN until reset by the user. The file is scanned from the last read location.

toggled
The user specifies a DOWN pattern, as with historical, and also an UP pattern (formed with the toggle positive and negative pattern attributes) which is matched against for changing the state back to UP. The file is scanned from the last read location.

firstLineOnly
Only the first line of a file is read. The monitor’s status is set to UP at the beginning of each poll. If a match is made the state changes to DOWN.

pollEOF
The monitor’s status is set to UP at the beginning of each poll. If a match is made the state changes to DOWN. The file is scanned from the last read location unless it is a new monitor, in which case reading starts at the end of the file.

startFromPreviousReadEOF
The monitor’s status is set to DOWN when a match occurs and will remain DOWN until reset by the user. The file is scanned from the last read location unless it is a new monitor, in which case reading starts at the end of the file.

toggledEOF
The user specifies a down pattern, as with historical, and also an up pattern (formed with the toggle positive and negative pattern attributes) which is matched against for changing the state back to up. The file is scanned from the last read location unless it is a new monitor, in which case reading starts at the end of the file.

rescan
Rescan the file from the beginning if the file length has increased. If the file is greater than 10kB, set the monitor to unknown.

**Monitor Status**

This attribute allows you to disable the status side of the monitor, but not match trap sending. Options include:

- **downCritical**
  The state change works as configured and a critical alert is raised.

- **doNotMonitor**
  The log file is monitored but the state is always UP.

- **downWarning**
  The state change works as configured and a warning alert is raised.

**Trap Send Policy**

This attribute defines the policy to be applied to the monitor’s status traps. Options include:

- **never**
  The state change never causes traps to be sent.

- **once**
  The state change trap is sent only when the monitor’s state changes.

- **perPoll**
  The state change trap is sent every poll even if the state does not change but a match condition occurred since the last poll.

- **each**
  The state change trap is sent for each match made by the agent. For toggle, once the monitor goes down the next match that will be looked for is the toggle pattern, so subsequent down patterns will not be matched.

**Match Trap Policy**

This attribute defines the policy to be applied to the match traps. Options include:

- **send**
  Send a trap for each match found. For toggle, once the monitor goes down the next match that will be looked for is the toggle pattern, so subsequent down patterns will not be matched unless status monitoring is switched off.
doNotSend
  Do not send a trap for each match found.

History Policy
  This attribute defines whether trap details are stored in the history table.
  Options include:
    generateHistory
      The status traps are recorded in the history table.
    noGenerateHistory
      The status traps are not recorded in the history table.

5. Click OK.
  The monitoring configuration is added to the Monitored Logs list, and
  monitoring begins immediately.

Set Up a File Monitor for NSM Agents Using OneClick

To set up file monitoring for NSM host agents
1. In the Contents panel, select the model with the file you want to monitor.
2. In the Component Detail panel, in the Information tab, expand System
   Resources, Monitored Logs and Files.
3. Expand Monitored Files and then click Add in the Monitored Files list.
   The Add File Monitor dialog appears.
4. Configure file monitor settings as needed, paying particular attention to the
   following mandatory and optional settings:

  **Monitor Name**
  Identifies the name of the file monitor.

  **File Name**
  Identifies the name of the file this monitor will watch.

  **File Exists**
  Indicates whether the file should exist or not.

  **Trap Send Policy**
  Specifies the frequency with which traps are sent by the NSM Agent.
  Options include:
    never
      A trap is never sent.
    once
      A trap is sent only once the state has been changed.
perPoll
A status trap is sent at each poll if the state is DOWN.

History Policy
For details about History Policy settings, see Set Up a Log File Monitor for NSM Agents Using OneClick on page 39.

5. Click OK.
The monitoring configuration is added to the Monitored Files list, and monitoring begins immediately.

Specify a Log-to-Process Mapping

In some cases, you may want SPECTRUM to generate an event on the process referenced by a parsed log file entry rather than on the host model. In this case, the process must be referenced by a process monitoring rule for the host model and you must associate the process with the log file that includes the entry related to the process. See Chapter 2: Process Monitoring for more information about process monitoring rules.

Mapping for RFC 2790 Agents

To specify a mapping for RFC 2790 Agents

1. In the Contents panel, select the model with the log files you want to monitor.
2. In the Component Detail panel, expand System Resources, Monitored Logs and Process Logs.
   The Add Log to Process Mapping dialog appears.
5. Type the name of the log file and the name of the process, and then click OK. The process name you specify must match the name specified for the process in the process monitoring rule.
   The mapping is added to the Monitored Process Log File Mappings list. SPECTRUM generates events on the monitored process model whenever text about the process is parsed from a log file.
Mapping for NSM r11 Agents

The following procedure describes how to specify a mapping for NSM r11 Agents.

**Note:** It is not possible to create mappings for NSM 3.1 Agents.

**To specify a mapping for NSM r11 Agents**

1. In the Contents panel, select the model with the log files you want to monitor.
2. In the Component Detail panel, expand System Resources, Monitored Logs and Files.
   The Add Log to Process Mapping dialog appears.
5. Type the name of the log file and the name of the process monitor, and then click OK. The process monitor name you specify will likely differ from the name specified for the process in the process monitoring rule.

   The mapping is added to the Monitored Process Log File Mappings list. SPECTRUM generates events on the monitored process model whenever text about the process is parsed from a log file.

Managing Monitored Log and Process Log Mapping Settings

This section describes how to edit and delete monitored log and process/log file mapping settings.

- To edit monitored log and process/log file mapping settings, select a configuration entry you want to modify, click Edit on the configuration entry list, edit the entry, and then click OK.
- To delete monitored log and process/log file mapping settings, select a configuration entry you want to remove, click Delete on the configuration entry list, and then click OK.

Configuring SPECTRUM to Process Syslog File Matches

You can configure SPECTRUM to process syslog file matches from iAgent, SystemEDGE, and NSM Agents.
Configuring SPECTRUM to Process Syslog File Matches

Trap Processing Overview

Each trap that an agent generates based on the content of a log file entry will have an OID. This OID generates the SPECTRUM event 0x3e00009 based on the trap mapping in the agent’s AlertMap file. This event is asserted on the model.

The matched line of each log file entry (up to 255 characters) and the log file name that generated the trap is sent as part of the trap information. SPECTRUM parses the trap data to determine the original source of the log file entry. The source can be an IP Address, host name, SPECTRUM model handle, or application log file name.

Processing Traps That Contain an IP Address, Host Name, or Model Handle

If an IP address, host name, or a model handle has been extracted as the source of the log file entry, SPECTRUM can find the device model that matches the IP address, host name, or model handle and assert the event on this model. If the log file entry conforms to the syntax described in Log File Syntax on page 37, to make the event asserted on the device model meaningful, you can create a ParseMap file to customize the event and its contents.

Note: SPECTRUM contains many ParseMap files. You do not always need to create one.

If no ParseMap file is created, the event routed to the device model is the same event asserted on the agent’s model.

Creating ParseMap Files

ParseMap files specify the event associated with the information in the incoming trap. In addition, ParseMap files allow you to specify that portions of the log file entry text be used as event variables. If desired, these variables can be used in conjunction with an Event Rule to process the event. For information about event processing and Event Rules, see the Event Configuration User Guide (5188).

As described in Log File Syntax on page 37, a log file entry contains the following components:

<MessagePrefix>%<MessageHeader><Additional_Information>

SPECTRUM identifies the ParseMap file that will process the trap by finding the ParseMap file whose name matches the text of the <MessageHeader> from the log file entry. The following is an example of a log file entry:

%SNMP-I-SENT_TRAP, Sending notification linkUp to 192.168.32.44

The <MessageHeader> portion of the entry is SNMP-I-SENT_TRAP, so SPECTRUM looks for a ParseMap file named SNMP-I-SENT_TRAP. As such, you must create a ParseMap file for each log entry with a unique <MessageHeader> that you configure to generate a trap.
Note: There are many ParseMap files available for use in SPECTRUM. You can find them in the following directory: <$SPECROOT>/SS/CsVendor/ParseMaps.

To create a ParseMap file

1. Create a new text file using any text editor.

2. In the first line of the text file, type the new event file name for the event that you want to generate. The event file name must begin with Eventffff and end with xxxx where x is be any valid hexadecimal number.
   For example, Eventffff1A2F and Eventffff1234 are valid event file names. Event012za8b is not.

3. Create a new line in the text file by pressing the Enter key on your keyboard.

4. This line contains the <Additional Information> portion of the log file entry. You can specify portions of this text as event variables, which can be used to process the event with an Event Rule.
   Specify variables using a data type and an integer. Valid data types are STRING, STRINGNOWS, INTEGER, and IPADDRESS. See STRING Data Type Usage Guidelines on page 47 for important information.
   The following image shows a valid ParseMap file for the log entry shown in the previous section. The variable 1 stores Uplink as a String. The Variable 2 stores 192.168.32.44 as an IP Address.

5. Save the text file in the <$SPECROOT>/SS/CsVendor/ParseMaps directory. The name of this text file must match the <MessageHeader> portion of the log file entry. In this case the file name would be SNMP-I-SENT_TRAP. Do not include a file extension in the file name.
   Note: Only the first two lines of the ParseMap file are processed. You can put whatever you want on subsequent lines but they are not processed and are informational only.
ParseMap File Example

The following is an example of a ParseMap file that provided with SPECTRUM named SYS-0-MOD_TEMPMAJORFAIL. It can be found in the following directory: <$SPECROOT>/SS/CsVendor/ParseMaps.

Event04bd1522
Module {STRING 1} major temperature threshold exceeded
%SYS-0-MOD_TEMPMAJORFAIL: Module {STRING} major temperature threshold exceeded

This instructs a matched syslog file:

This causes the event Event04bd1522 to be generated on the model with the IP address 10.253.9.11, even though the trap was generated by the agent.

STRING Data Type Usage Guidelines

This section provides important information about using STRING data types in your ParseMap files.

Valid STRING Data Types

As mentioned in Step 4 of To create a ParseMap file on page 46, the following are valid data types for use in variables.

STRING
Matches all string characters up to the next literal, data type or end of string.

STRINGNOWS
Matches all string characters up to the next space, literal, data type, or end of string.

INTEGER
Matches any positive integer value.

IPADDRESS
Matches any valid IPv4 address.
Whitespace in STRING Variables

Since whitespace is a valid character in the definition of the STRING variable, you should always separate multiple STRING tokens with recognizable patterns.

For example, a valid ParseMap entry could contain entries that look like these:

{STRING 1}, {STRING 2}
{STRING 1} {IPADDRESS 2} {STRING 3}
{STRING 1} literal text {STRING 2}
{STRINGNOWS 1} {STRING 2}

However, you should not have these because the resulting regular expression will be ambiguous:

{STRING 1}{STRING 2}
{STRING 2} {STRING 2}

Creating an Event Format File

Each event code that you specify in a ParseMap file must have a separate Event Format file. When an event is asserted, the text of the Event Format file appears in the Event Log. When creating the Event Format file, keep in mind that most of the information the troubleshooter receives about an event comes from the event message text.

Create the Event Format file using a text editor and place the file in the following directory: <$SPECROOT>/SG-Support/CsEvFormat. The Event Format file must be named Event<xxxxxxxx> where <xxxxxxxx> is the event code given to the event in ParseMap file. For example, if you have an event with an event code of 0xffff1A2F, SPECTRUM will use the Event Format file named Eventffff1A2F.

To make the text of the event message meaningful, you can use the variables assigned in the event’s ParseMap file as well as the built-in variable available for all Event Format files.

For complete instructions on creating an Event Format file, including the built-in variables that are available, see the Event Configuration User Guide (5188).

Example: Event Format File

The following sample Event Format file would be appropriate to use for the event generated by the ParseMap File shown in Step 4 of To create a ParseMap file on page 46.
The IP Address variable is inserted using the data type o (octet) and the variable assigned from the ParseMap file, 1. The device name variable is inserted using the data type s (string) and the variable assigned from the ParseMap file, 2. The built-in variables \{d\} \{m\} \{t\} and \{e\} show the date of the event, model name, model type name, and event ID.

\{d\} A device \{m\} of type \{t\} has reported a problem. Its ip address is \{S 1\} and the device name is \{S 2\} - \{event \{e\}\}

### Generating an Alarm Based on the Event

You can specify further processing on the event created in the ParseMap file. You can generate an alarm based on the event, or use the event as part of an Event Rule. To do this, determine all of the model types that this event could be asserted on and specify the appropriate event processing in each model type’s EventDisp file. If you want the event to be processed the same way for each model type, you can specify the event processing in a global EventDisp file.

If you have specified that an alarm will be created based on an event, you must create a probable cause file that will be displayed in the OneClick Console when the alarm is asserted. For more information about EventDisp and probable cause files, see the Event Configuration User Guide (5188).

### Apply the Changes to the SpectroSERVER

To activate the new or updated Event Format and ParseMap files, you must apply the changes to the SpectroSERVER. This can be done using the Update command found in the Event Configuration Editor, using the command line interface, or by stopping and restarting the SpectroSERVER. See the Event Configuration User Guide (5188) for more information about each of these methods.

### Enabling Event Forwarding for Agent Models

You can configure an agent’s model to forward events to models on remote landscapes by setting the SBG.AlertForwardingEnabled (0x3dc000c) attribute for the model to TRUE.
Chapter 6: Application Monitoring

SystemEDGE Application Insight Modules (AIMs)

The SystemEDGE agent provides a plug-in architecture through which it can load Application Insight Modules (AIMs) when it initializes. These AIMs provide an extensible and flexible approach to supporting application-specific semantic knowledge.

SPECTRUM supports the following AIMs:

- AIM for Apache
- AIM for Microsoft IIS
- Insight AIM
  - Insight AIM for DB2
  - Insight AIM for Oracle
  - Insight AIM for SQL Server
  - Insight AIM for Sybase

**Note:** The SystemEDGE AIMs are available from the Information tab in the Component Detail panel for a selected SystemEDGE agent.

In addition, SPECTRUM reports alarms which are sent through traps by the Insight AIMs. Each Insight AIM sends out a trap unique to its type, which lets you differentiate between the Insight AIM agent types. Detailed per-alarm information also includes the database name, the alarm type, and the alarm description.

The Insight AIM alarm types vary between agent types and cover a wide range of notifiable conditions. These AIM alarms are no different than other alarms in SPECTRUM and appear in the same tables and offer the same functionality.

**AIM for Apache**

The AIM for Apache lets you monitor the health and availability of the Apache web server.
This module works with the SystemEDGE agent to provide the following information:

- The number of "hits" your web server is receiving, which can help you keep up with daily volume and set monitor points to watch for unusual traffic loss or denial of service attacks.
- The amount of space your web log file and web server file are consuming.
- How effectively the Apache web server processes monitor idle services, warn you when the number of idle services is too low, and monitor the number of active processes.
- How much of your system resources (CPU and memory) Apache web server is using.
- Whether bottlenecks on your web server are caused by problems with the CPU, memory, disk, or network.

**AIM for Microsoft IIS**

The AIM for Microsoft IIS provides you with the information you need to monitor the Microsoft IIS application and its use of your system resources.

This module works with the SystemEDGE agent to let you do the following:

- Monitor the availability of Microsoft IIS and its services (Web, FTP, SMTP, and NNTP).
- Automatically restart any service that fails.
- Determine if Microsoft IIS starts to consume significant levels of system resources, including central processing unit (CPU) usage, disk space, and memory.
- Monitor logs for security, system, and application events across the Web, FTP, SMTP, and NNTP services.
- Detect error statistics across the Active Server Pages (ASP), Common Gateway Interface (CGI), and Internet Server Application Program Interface (ISAPI) application extension pages, including Web 404 (page-not-found) errors and ASP script errors.

**Insight AIM**

The Insight AIM provides important information about a DBMS type’s performance, configuration, availability, and health for real-time management and long-term trending and capacity planning.
The Insight AIM implements a management information base (MIB) that includes variables that are specific to each supported DBMS type. The supported DBMS types include the following:

- DB2
- Oracle
- SQL Server
- Sybase
Index

A
adding rules to a rule set • 29
aggregate status • 20
AIM
  for Apache • 51
  for Insight • 52
  for Microsoft IIS • 52
AIMs • 51
alarm condition (RFC 2790) • 1
  alarm if count is greater than • 10
  alarm if offline • 24
  alarm on start • 10
  alarm on stop • 10
  file system utilization • 24
  process instances • 10
  process start • 10
  process stop • 10
alarm conditions (RFC 2790)
  for file system monitoring rules • 3, 23
  for process monitoring rules • 3, 10
alarm, destination
  file system rule violations • 24
  process monitoring rule violation • 8
application insight modules • 51
application monitoring • 51

C
CA SystemEDGE Agent • 35, 51
children spawned by a process • 16, 17
Cisco • 37
configuration threshold (NSM Agent) • 1
  children • 16, 17
  CPU usage • 15
  handles • 17
  instances • 16
  runtime • 17
  size • 15
  threads • 16, 17
CPU time a process consumes • 15

critical alarm
  file system offline • 24
  file system utilization threshold violation • 24
critical thresholds, NSM Agent process monitoring rule • 17
Culprits list, threshold violations • 18

E
Event Format file • 48
event forwarding • 49
Event Rule • 49
event, file system utilization threshold violation • 24
event, log file entry • 36
EventDisp file • 49

F
file system monitoring rule • 1, 2
  alarm conditions • 3, 23
  creating • 23
  deleting • 26
  destination for alarms • 24
  editing • 25
  utilization thresholds • 24
file system name, file system monitoring rule setting • 24
File Systems option • 6

global collection • 27
  apply rule set to • 30
  remove rule set from • 31

H
handles opened by a process • 17
host • 2
host resources • 2
host resources monitoring • 2
host resources monitoring, network services management • 5

I
iAgent • 35
instances of a process • 16

K
Kiwi • 37

L
locating
monitored file systems • 6
monitored processes • 6
monitoring rule sets • 6
log file • 2, 35
map to process • 38
monitoring • 4, 35
monitoring, regular expression • 36
monitoring, traps • 38

M
major alarm
file system utilization threshold violation • 24
memory a process consume • 15
minor alarm
file system utilization threshold violation • 24
monitor files • 42
monitor log files • 38, 39
monitored log configuration
deleting • 44
editing • 44
monitored logs
editing configuration • 38
monitoring
file systems • 23
processes • 7
monitoring options, NSM Agent • 14
monitoring rule
editing outside rule set • 32
monitoring rule, file system • 23
monitoring rule, process
NSM Agent • 11
RFC 2790 • 9
monitoring rules workspace • 5

N
NSM Agent process monitoring rule
monitor name • 11, 13
monitoring options for configuration thresholds • 17
process match criteria • 12
status indicators • 20
NSM Agent, subagent failure alarm • 20

P
parameters, process arguments • 13
ParseMap files • 45, 46
path, process • 13
polling
watch for new instances (RFC 2790) • 10
process • 2
children • 16, 17
CPU usage • 15
handles • 17
instance count (RFC 2790) • 10
instances • 16
mapping to log file • 38
parameters • 13
path • 13
rearts • 16
runtime • 17
size • 15
start/stop (RFC 2790) • 10
threads • 16, 17
user • 13
process log file mappings
deleting • 44
editing • 44
process match criteria, NSM Agent process monitoring rule • 12
process monitoring rule • 2
adding to rule set • 29
alarm conditions • 3
creating • 8
deleting • 21
destination for alarms • 8
differentiating process instances • 9
editing • 21

R
regular expression for log file parsing • 36
regular expression, match criteria • 13
reports on events and alarms • 5
resources, host • 17
restarts for a process • 16
RFC 2790 file system monitoring rule setting utilization threshold • 24
Riverstone • 37
rule set • 27
adding rules to • 29
applied to global collection • 27
apply to global collection • 30
creating • 27
deleting • 33
deleting a rule from • 33
editing a rule in • 32
remove association with global collection • 31
view in Contents panel • 28
viewing • 6
rule, adding to rule set • 29
Running and Monitored Processes option • 5
runtime for a process • 17

S
searches
all monitored file systems • 6
all monitored processes • 6
all monitoring rule set • 6
size of a process • 15
Solaris • 37
SPECTRUM Report Gateway • 37
status indicators, NSM Agent process monitoring rule • 20
string compare, match criteria • 13
Syslog • 37
System Resources option • 5

T
thread count for a process • 16, 17
threshold type, file system monitoring rule setting • 24
threshold violations
aggregate status change as a result of • 19
alarm destination • 8, 24
alarm types • 14
evaluation policy • 18
monitoring options • 17
reports • 5
thresholds
for process monitoring rules (NSM Agent) • 3
traps, log file monitoring • 38

U
user, process • 13
utilization, file system monitoring rule setting • 24

V
viewing
monitored file systems • 6
monitored processes • 6
monitoring rule sets • 6

W
warning thresholds, NSM Agent process monitoring rule • 17
watch for new instances (RFC 2790), polling interval • 10