

Administration Guide

Sentinel Log Manager 1.2.2

July, 2014



Legal Notice

NetIQ Sentinel is protected by United States Patent No(s): 05829001.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see <http://www.netiq.com/company/legal/>.

About This Guide

This guide assumes that you have already installed Sentinel Log Manager on your machine. This guide provides an overview of Novell Sentinel Log Manager and also guides in administering the product and users.

- ♦ Chapter 1, "Overview," on page 13
- ♦ Chapter 2, "Security Considerations," on page 15
- ♦ Chapter 3, "Configuring Data Storage," on page 29
- ♦ Chapter 4, "Configuring Data Collection," on page 55
- ♦ Chapter 5, "Searching Events," on page 77
- ♦ Chapter 6, "Reporting," on page 93
- ♦ Chapter 7, "Searching and Reporting Events in a Distributed Environment," on page 109
- ♦ Chapter 8, "Configuring Tags," on page 127
- ♦ Chapter 9, "Configuring Rules and Actions," on page 137
- ♦ Chapter 10, "Configuring Users and Roles," on page 151
- ♦ Chapter 11, "LDAP Authentication," on page 161
- ♦ Chapter 12, "Implementing High Availability and Disaster Recovery," on page 169
- ♦ Chapter 13, "License Information," on page 171
- ♦ Chapter 14, "Command Line Utilities," on page 177
- ♦ Appendix A, "Search Query Syntax," on page 181
- ♦ Appendix B, "Managing Data," on page 191
- ♦ Appendix C, "Backing Up and Restoring Data," on page 193
- ♦ Appendix D, "Syslog Collector Package Policy," on page 197
- ♦ Appendix E, "Event Fields," on page 199
- ♦ Appendix F, "Troubleshooting," on page 209
- ♦ Appendix G, "Internal Audit Events," on page 211

Audience

This guide is intended for Novell Sentinel Log Manager administrators and end users.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to [Novell Documentation Feedback Web site \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html) and enter your comments there.

Additional Documentation

For more information about building your own plug-ins (for example, JasperReports), go to the [Sentinel SDK Web page \(http://developer.novell.com/wiki/index.php/Develop_to_Sentinel\)](http://developer.novell.com/wiki/index.php/Develop_to_Sentinel). The build environment for Sentinel Log Manager report plug-ins is identical to what is documented for Novell Sentinel.

For more information about the Sentinel documentation refer to the [Sentinel Documentation Web site \(http://www.novell.com/documentation/sentinel61/index.html\)](http://www.novell.com/documentation/sentinel61/index.html).

For more information about installation and system requirements, see [Sentinel Log Manager 1.2.2 Installation Guide](#).

Contacting Novell

- ♦ [Novell Web site \(http://www.novell.com\)](http://www.novell.com)
- ♦ [Novell Technical Support \(http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup\)](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- ♦ [Novell Self Support \(http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog\)](http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- ♦ [Patch Download Site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp)
- ♦ [Novell 24x7 Support \(http://www.novell.com/company/contact.html\)](http://www.novell.com/company/contact.html)
- ♦ [Sentinel TIDS \(http://support.novell.com/products/sentinel\)](http://support.novell.com/products/sentinel)

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

Contents

About This Guide	3
1 Overview	13
1.1 Before You Begin	13
1.2 Web User Interface	13
2 Security Considerations	15
2.1 Hardening	15
2.1.1 Out of the Box Hardening	15
2.1.2 Enforcing Password Policy for Users	16
2.1.3 Securing Sentinel Log Manager Data	17
2.1.4 Securing Communication with Networked Storage	17
2.2 Best Practices	17
2.2.1 Changing Passwords	17
2.2.2 Securing Communication with Collector Managers and Event Sources	19
2.2.3 Auditing Sentinel	19
2.2.4 Determining if Raw Data Files Were Tampered With	19
2.2.5 Using CA Signed Certificates	21
2.3 Network Communication Options	23
2.3.1 Communication between Sentinel Log Manager Processes	24
2.3.2 Communication between Sentinel Log Manager and the Event Source Manager Client Application	25
2.3.3 Communication between the Server and the Database	25
2.3.4 Communication with Web Browsers	25
2.3.5 Communication between the Database and Other Clients	25
2.4 Sensitive Data Locations	26
2.5 Overriding the IP Address in the Web Server	27
2.6 Applying Updates for Security Vulnerabilities in Embedded Third-Party Products	28
3 Configuring Data Storage	29
3.1 Types of Data	29
3.1.1 Raw Data	29
3.1.2 Event Data	34
3.2 Configuring Networked Storage Locations	35
3.2.1 Supported Storage Options	35
3.2.2 Types of Networked Storage	36
3.2.3 Configuring Networked Storage	36
3.2.4 Enabling or Disabling Networked Storage	40
3.2.5 Unmounting a Networked Storage Location	40
3.2.6 Changing the Networked Storage Location	41
3.3 Configuring Data Retention Policies	42
3.3.1 Raw Data Retention Policy	42
3.3.2 Event Data Retention Policies	42
3.3.3 Rules for Applying a Retention Policy	45
3.4 Configuring Disk Space Usage	46
3.5 Verifying and Downloading Raw Data Files	46
3.6 Viewing Local and Networked Storage Capacity	47
3.7 Using Sequential-Access Storage for Long Term Data Storage	49

3.7.1	Determining What Data You Need to Copy to Tape	49
3.7.2	Backing Up Data	49
3.7.3	Configuring Storage Utilization	50
3.7.4	Configuring Data Retention	50
3.7.5	Copying Data to Tape	50
3.7.6	Restoring Data	51
4	Configuring Data Collection	55
4.1	Before You Begin	55
4.2	Configuring Data Collection for Syslog Event Sources	56
4.2.1	Parsing Logic for Syslog Messages	56
4.2.2	Configuring Syslog Servers	56
4.2.3	Setting the Syslog Server Options	57
4.3	Configuring Data Collection for the Novell Audit Server	60
4.3.1	Specifying the Audit Server Settings	60
4.3.2	Setting the Audit Server Options	61
4.4	Configuring Data Collection for Other Event Sources	64
4.5	Managing Event Sources	67
4.5.1	Viewing the Event Sources Page	67
4.5.2	Filtering Event Sources	72
4.5.3	Changing the Data Logging Status of Event Sources	74
4.5.4	Changing the Associated Collector Plug-in for Event Sources	74
4.5.5	Changing the Time Zone Setting for Event Sources	74
4.5.6	Starting and Stopping Event Sources by Using the Script	75
4.6	Viewing Events Per Second Statistics	75
4.6.1	Viewing Graphical Representation of Events Per Second Value	75
4.6.2	Viewing Events Per Second Value of Event Source Servers	76
5	Searching Events	77
5.1	Running an Event Search	77
5.1.1	Running a Basic Search	78
5.1.2	Running an Advanced Search	78
5.1.3	Search Expression History	79
5.2	Viewing Search Results	80
5.2.1	Basic Event View	80
5.2.2	Event View with Details	80
5.3	Refining Search Results	83
5.4	Searching for Events with Empty or Non-Empty Fields	86
5.4.1	Searching for Events with a Non-Empty Field	86
5.4.2	Searching For Empty Fields	86
5.5	Exporting Search Results	86
5.6	Saving a Search Query	87
5.6.1	Saving a Search Query as a Report Template	87
5.6.2	Saving a Search Query as a Rule	90
5.6.3	Saving a Search Query as a Retention Policy	90
5.7	Sending Search Results to an Action	91
5.8	Configuring the Search Limit	92
6	Reporting	93
6.1	Running Reports	93
6.2	Viewing the Reports	96
6.2.1	Viewing the Report Result in PDF Format	96
6.2.2	Drilling Down into Report Results	97
6.2.3	Viewing Report Parameters	98

6.3	Scheduling a Report	98
6.4	Adding Report Definitions	99
6.4.1	Adding or Uploading a Report	99
6.5	Renaming a Report Result	100
6.6	Marking Report Results as Read or Unread	100
6.6.1	Marking a Single Report Result as Read or Unread	101
6.6.2	Marking Multiple Report Results as Read or Unread	101
6.7	Managing Favorite Reports	102
6.7.1	Adding Reports as Favorites	102
6.7.2	Removing Favorite Reports	103
6.8	Exporting Report Definitions and Report Results	103
6.8.1	Exporting a Single Report Definition	103
6.8.2	Exporting Selected Report Definitions	104
6.8.3	Exporting All Report Definitions	104
6.8.4	Exporting a Report Result	105
6.9	Deleting Reports	106
6.9.1	Deleting a Report Definition	106
6.9.2	Deleting Multiple Report Definitions	106
6.9.3	Deleting a Report Result	107
6.9.4	Deleting Multiple Report Results	107

7 Searching and Reporting Events in a Distributed Environment 109

7.1	Overview	109
7.2	Configuring Servers for Distributed Searching and Reporting	111
7.2.1	Enabling Distributed Search	111
7.2.2	Adding a Search Target Server by Using the Administrator Credentials	112
7.2.3	Adding a Search Target Server by Using the Opt-in Password	114
7.3	Searching for Events	117
7.4	Managing the Distributed Search Results	118
7.5	Viewing the Search Activities	120
7.6	Running Reports	120
7.7	Managing the Distributed Setup Configuration	121
7.7.1	Editing the Search Target Server Details	122
7.7.2	Disabling or Deleting a Search Target Server	122
7.7.3	Editing the Search Initiator Server Details	123
7.7.4	Disabling or Deleting a Search Initiator Server	124
7.8	Troubleshooting	124
7.8.1	Permission Denied	124
7.8.2	Connection Down	124
7.8.3	Unable to View Raw Data	125
7.8.4	Problems Adding Search Target	125
7.8.5	Certain Events Are Only Visible from the Local System	125
7.8.6	Cannot Run Reports on the Target Servers	125
7.8.7	Different Users Might Get Different Results	125
7.8.8	Cannot Set the Admin Role as the Search Proxy Role	125
7.8.9	Error Logs	125

8 Configuring Tags 127

8.1	Overview	127
8.2	Creating a Tag	129
8.3	Managing Tags	129
8.3.1	Using the Tag Selector Widget	130
8.3.2	Sorting Tags	130
8.3.3	Adding and Removing Tags from Favorites	130
8.3.4	Viewing and Modifying Tag Description	130

8.4	Performing Text Refined Searches	131
8.5	Deleting Tags	132
8.5.1	Deleting a Tag	132
8.5.2	Deleting Multiple Tags	132
8.6	Associating Tags with Different Objects	133
8.6.1	Associating Tags with Event Sources	133
8.6.2	Associating Tags with Event Sources Servers	133
8.6.3	Associating Tags with Collector Managers	134
8.6.4	Associating Tags with Collector Plug-ins	135
8.6.5	Associating Tags with Reports Results and Report Definition	135
8.7	Searching Tagged Events	136
9	Configuring Rules and Actions	137
9.1	Configuring Rules	137
9.1.1	Adding a Rule	137
9.1.2	Editing a Rule	138
9.1.3	Ordering Rules	138
9.1.4	Deleting a Rule	139
9.1.5	Activating or Deactivating a Rule	139
9.2	Configuring Actions	140
9.2.1	Executing a Script	141
9.2.2	Logging the Events to a File	141
9.2.3	Sending the Events to Syslog	142
9.2.4	Sending the Events by an E-Mail	143
9.2.5	Sending the SNMP Traps	144
9.2.6	Sending the Events to a Sentinel Link	144
9.2.7	Modifying an Action	147
9.2.8	Deleting an Action	148
9.3	Handling Auto-Created Event Sources without a Time Zone	148
9.4	Forwarding the Events to Another Sentinel System	150
10	Configuring Users and Roles	151
10.1	Overview	151
10.1.1	Default Roles	152
10.1.2	Filtering Data	153
10.1.3	Setting Permissions	153
10.2	Creating Roles and Users	154
10.2.1	Creating Roles	154
10.2.2	Creating Users	155
10.3	Viewing Roles and User Details	156
10.4	Viewing All Users	157
10.5	Modifying Roles and Users	157
10.5.1	Modifying Roles	157
10.5.2	Modifying User Details	158
10.6	Moving Users to Another Role	159
10.7	Deleting Roles and Users	159
10.7.1	Deleting a Role	159
10.7.2	Deleting a User	160
11	LDAP Authentication	161
11.1	Overview	161
11.2	Prerequisites	162
11.2.1	Exporting the LDAP Server CA Certificate	162
11.2.2	Enabling Anonymous Search in the LDAP Directory	162

11.3	Setting Up LDAP Authentication	162
11.4	Creating an LDAP User Account	166
11.5	Configuring Multiple LDAP Servers for Failover	166
12	Implementing High Availability and Disaster Recovery	169
12.1	High Availability	169
12.2	Disaster Recovery	170
13	License Information	171
13.1	Understanding the Licenses	171
13.1.1	Trial License	171
13.1.2	Free License	172
13.1.3	Enterprise Licenses	172
13.2	Managing the Licenses	173
13.2.1	Adding a License Key	173
13.2.2	Viewing the License Details	175
13.2.3	Deleting a License Key	175
14	Command Line Utilities	177
14.1	Managing the Sentinel Log Manager Services	177
14.2	Running the Report Development Utility	178
14.3	Getting the .jar Version Information	178
14.4	Reconfiguring Database Connection Properties	179
14.5	Sentinel Scripts	179
A	Search Query Syntax	181
A.1	Basic Search Query	181
A.1.1	Case Insensitivity	182
A.1.2	Special Characters	182
A.1.3	Operators	182
A.1.4	The Default Search Field	183
A.1.5	Tokenized Fields	184
A.1.6	Non-Tokenized Fields	186
A.2	Wildcards in Search Queries	186
A.2.1	Wildcards in Tokenized Fields	187
A.2.2	Quoted Wildcards	187
A.2.3	Leading Wildcards	187
A.3	The notnull Query	188
A.4	Tags in Search Queries	188
A.5	Range Queries	189
A.6	IP Addresses Query	189
A.6.1	CIDR Notation	189
A.6.2	Wildcards in IP Addresses	190
B	Managing Data	191
B.1	Moving Event Data Storage to a Large Partition	191
B.2	Directory Structure	192
B.3	Data Expiration Policy	192

C	Backing Up and Restoring Data	193
C.1	Parameters for the Backup and Restore Utility Script	193
C.2	Running the Backup and Restore Utility Script	195
D	Syslog Collector Package Policy	197
E	Event Fields	199
F	Troubleshooting	209
F.1	Data Retention Policies are not Displayed when there is Large Data in the Networked Storage . . 209	
F.2	Unable to Log In to the Web Interface when the System runs out of Local Disk Storage Space. . . 209	
G	Internal Audit Events	211
G.1	Authentication Events	211
G.1.1	Authentication	211
G.1.2	Failed Authentication	212
G.1.3	Web User Interface Login	212
G.1.4	Web User Interface Login Failed	212
G.1.5	User Logged In	213
G.1.6	User Logged Out	213
G.2	User Management	213
G.2.1	Create User	214
G.2.2	Create User Role	214
G.2.3	Add User To Role	214
G.2.4	Removing User From a Role	215
G.2.5	Updating User	215
G.2.6	Updating User Role	215
G.2.7	Delete User	216
G.2.8	Delete User Role	216
G.2.9	Resetting User Password	216
G.3	Event Router	217
G.3.1	Event Router is Initializing	217
G.3.2	Event Router is Running	217
G.3.3	Event Router is Stopping	218
G.3.4	Event Router is Terminating	218
G.4	Event Source Management - General	218
G.4.1	Collector Manager Initialized	219
G.4.2	Collector Manager Is Down	219
G.4.3	Collector Manager Started	220
G.4.4	Collector Manager Stopped	220
G.4.5	Collector Service Callback	220
G.4.6	Event Source Manager Callback	221
G.4.7	Initializing Collector Manager	221
G.4.8	Update Collector Manager	221
G.4.9	Lost Contact With Collector Manager	222
G.4.10	No Data Alert	222
G.4.11	Persistent Process Died	222
G.4.12	Persistent Process Restarted	223
G.4.13	Port Start	223
G.4.14	Port Stop	223
G.4.15	Reestablished Contact With Collector Manager	224
G.4.16	Restart Plugin Deployments	224
G.4.17	Restarting Collector Manager (Cold Restart)	224
G.4.18	Restarting Collector Manager (Warm Restart)	225
G.4.19	Start Event Source Group	225

G.4.20	Start Event Source Manager	225
G.4.21	Starting Collector Manager	226
G.4.22	Stop Event Source Group	226
G.4.23	Stop Event Source Manager	226
G.4.24	Stopping Collector Manager	227
G.5	Event Source Management - Event Sources	227
G.5.1	Start Event Source	227
G.5.2	Stop Event Source	227
G.5.3	Start Event Sources	228
G.5.4	Stop Event Sources	228
G.5.5	Update Event Source Configuration	228
G.6	Event Source Management - Collectors	229
G.6.1	Start Collector	229
G.6.2	Stop Collector	229
G.6.3	Update Collector Configuration	229
G.7	Event Source Management - Event Source Servers	230
G.7.1	Start Event Source Server	230
G.7.2	Stop Event Source Server	230
G.7.3	Update Event Source Server Configuration	231
G.8	Event Source Management - Connectors	231
G.8.1	Start Connector	231
G.8.2	Stop Connector	232
G.8.3	Update Connector Configuration	232
G.8.4	Data Received After Timeout	232
G.8.5	Data Timeout	233
G.8.6	File Rotation	233
G.8.7	Process Auto Restart Error	233
G.8.8	Process Start Error	234
G.8.9	Process Stop	234
G.8.10	WMI Connector Status Message	234
G.9	Data Objects	235
G.9.1	Configuration	235
G.10	Search	235
G.10.1	Event Search	235
G.11	Data Retention Policy	235
G.11.1	Create Data Retention Policy	236
G.11.2	Update Data Retention Policy	236
G.11.3	Delete Data Retention Policy	236
G.12	Disk Usage Configuration	237
G.12.1	Change Disk Usage Config	237
G.13	Report Definitions and Report Results	237
G.13.1	Remove Report Definition	237
G.13.2	Remove Report Definitions	238
G.13.3	Remove Report Result	238
G.13.4	Remove Report Results	238
G.14	General	238
G.14.1	Configuration Service	239
G.14.2	Controlled Process is started	239
G.14.3	Controlled Process is stopped	240
G.14.4	Importing Auxiliary	240
G.14.5	Importing Plugin	240
G.14.6	Load Esec Taxonomy To XML	241
G.14.7	Process Auto Restart Error	241
G.14.8	Process Restarts	241
G.14.9	Proxy Client Registration Service (medium)	242
G.14.10	Restarting Process	242
G.14.11	Restarting Processes	242
G.14.12	Starting Process	243
G.14.13	Starting Processes	243

G.14.14 Stopping Process.....	243
G.14.15 Stopping Processes.....	244
G.14.16 Store Esec Taxonomy From XML.....	244
G.14.17 Watchdog Process is started.....	244
G.14.18 Watchdog Process is stopped.....	244

1 Overview

Novell Sentinel Log Manager collects data from a wide variety of devices and applications, including intrusion detection systems, firewalls, operating systems, routers, Web servers, databases, switches, mainframes, and antivirus event sources.

Novell Sentinel Log Manager provides high event-rate processing, long-term data retention, policy based data retention, regional data aggregation, and simple searching and reporting functionality for a broad range of applications and devices. It also enables you to search events on other Sentinel Log Manager servers distributed across the globe.

- ◆ [Section 1.1, “Before You Begin,”](#) on page 13
- ◆ [Section 1.2, “Web User Interface,”](#) on page 13

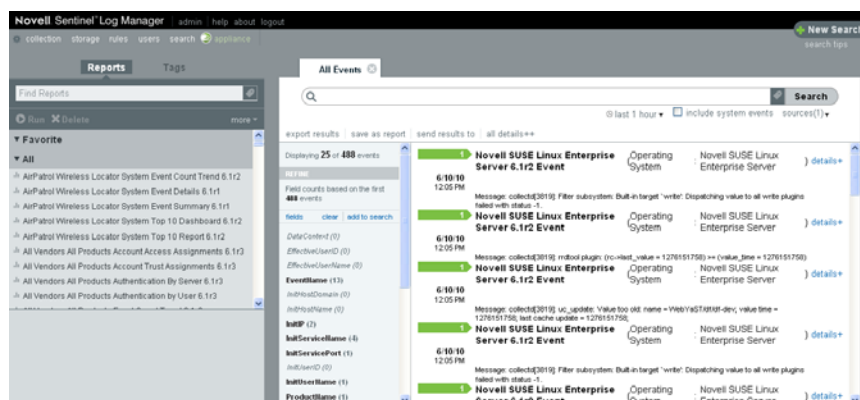
1.1 Before You Begin

- ◆ Make sure that you have installed Sentinel Log Manager. For more information, see the [Sentinel Log Manager 1.2.2 Installation Guide](#).
- ◆ To understand the Sentinel Log Manager features, see “[Product Overview](#)” in the [Sentinel Log Manager 1.2.2 Installation Guide](#).
- ◆ To understand the Sentinel Log Manager architecture, see “[Product Overview](#)” in the [Sentinel Log Manager 1.2.2 Installation Guide](#).

1.2 Web User Interface

The Novell Sentinel Log Manager comes with a Web-based user interface to configure and use Log Manager. The user interface functionality is provided by a Web server and a Java Web Start based graphical user interface (GUI). All user interfaces communicate with the server by using an encrypted connection.

Figure 1-1 Web User Interface



<name>: The user name of the logged in user is displayed here. For example, if you have logged in as an admin user, then Admin is displayed here.

Help: You can click this button to open the online documentation link for Sentinel Log Manager.

About: Click this button to read the copyright information and details about the installed version of Sentinel Log Manager.

Logout: Click this button to log out of Sentinel Log Manager Server.

Collection: Click this tab to configure event sources and event source servers to collect events and also to launch ESM. For more information, see [Chapter 4, "Configuring Data Collection," on page 55](#).

Storage: Click this tab to configure location to store data, configure data retention policies and also to monitor the health of the server. For more information, see [Chapter 3, "Configuring Data Storage," on page 29](#).

Rules: Click this tab to configure rules to filter events based on one or more of the searchable fields. For more information, see [Chapter 9, "Configuring Rules and Actions," on page 137](#).

Users: Click this tab to configure roles and users and assign them different permissions. For more information, see [Chapter 10, "Configuring Users and Roles," on page 151](#).

Search: Click this tab to configure search related attributes. For more information, see [Chapter 5, "Searching Events," on page 77](#).

Appliance: This icon indicates that the installed Sentinel Log Manager is an appliance. For more information on installing Sentinel Log Manager Appliance, see Installing the Appliance in the Sentinel Log Manager 1.2 Installation Guide.

2 Security Considerations

This section provides additional information on how to securely install, configure, and maintain Novell Sentinel Log Manager.

- ◆ [Section 2.1, “Hardening,” on page 15](#)
- ◆ [Section 2.2, “Best Practices,” on page 17](#)
- ◆ [Section 2.3, “Network Communication Options,” on page 23](#)
- ◆ [Section 2.4, “Sensitive Data Locations,” on page 26](#)
- ◆ [Section 2.5, “Overriding the IP Address in the Web Server,” on page 27](#)
- ◆ [Section 2.6, “Applying Updates for Security Vulnerabilities in Embedded Third-Party Products,” on page 28](#)

2.1 Hardening

- ◆ [Section 2.1.1, “Out of the Box Hardening,” on page 15](#)
- ◆ [Section 2.1.2, “Enforcing Password Policy for Users,” on page 16](#)
- ◆ [Section 2.1.3, “Securing Sentinel Log Manager Data,” on page 17](#)
- ◆ [Section 2.1.4, “Securing Communication with Networked Storage,” on page 17](#)

2.1.1 Out of the Box Hardening

The following sections describe the out of the box hardening mechanisms used in Sentinel Log Manager:

- ◆ [“Novell Sentinel Log Manager Application” on page 15](#)
- ◆ [“Novell Sentinel Log Manager Appliance” on page 16](#)

Novell Sentinel Log Manager Application

- ◆ All unnecessary ports are turned off.
- ◆ Whenever possible, a service port listens only for local connections and does not allow remote connections.
- ◆ Files are installed with the least privileges so that only a small number of users can read the files.
- ◆ Default passwords are not permitted to be used.
- ◆ Reports against the database runs as a user that only has select permissions on the database.
- ◆ All web interfaces require HTTPS.
- ◆ Prior to releasing the product, a vulnerability scan was run against the application and all potential security problems were addressed.

- ♦ All communication over the network use SSL by default and are configured for authentication.
- ♦ User account passwords are encrypted by default when stored on the file system or in the database.

Novell Sentinel Log Manager Appliance

In addition to the points mentioned in “[Novell Sentinel Log Manager Application](#)” on page 15, the Sentinel Log Manager Appliance, also has the following:

- ♦ The appliance includes a Just enough Operating System (JeOS). Only the required packages are installed.
- ♦ Default passwords for the appliance operating system or the control center are not permitted for use.
- ♦ The firewall is enabled by default and all unnecessary ports are closed in the firewall configuration.
- ♦ Prior to releasing the product, a vulnerability scan was run against the appliance and all potential security problems were addressed.
- ♦ It is automatically configured to monitor the syslog messages of the local operating system.

2.1.2 Enforcing Password Policy for Users

The Sentinel Log Manager utilizes standards-based mechanisms to make it easier to enforce password policies.

The installer creates and configures a PostgreSQL database with the following users.

dbauser: The database owner (database administrator user). The password is set during the installation process.

appuser: A user that is used by the Sentinel Log Manager server process (the ConnectionManager) to log in to the database. The password is randomly generated during the installation process, and it is intended for internal use only.

admin: The administrator credentials can be used to log in to the Sentinel Log Manager Web interface. The password is set during the installation process.

By default, user passwords are stored within the PostgreSQL database embedded in Sentinel Log Manager. PostgreSQL provides the option to utilize a number of these standards-based authentication mechanisms, as described in [Client Authentication \(http://www.postgresql.org/docs/8.3/static/client-authentication.html\)](http://www.postgresql.org/docs/8.3/static/client-authentication.html)

Utilizing these mechanisms affects all user accounts in Sentinel Log Manager, including users of the Web application and accounts used only by back-end services, such as dbauser and appuser.

A simpler option is to use an LDAP directory to authenticate Web application users. To enable this option by using the Sentinel Log Manager Web UI, see [Chapter 11, “LDAP Authentication,” on page 161](#). This option has no affect on accounts used by back-end services, which continue to authenticate through PostgreSQL unless you change the PostgreSQL configuration settings.

You can achieve robust Sentinel Log Manager password policy enforcement by using these standards based mechanisms and the existing mechanisms in your environment such as your LDAP directory.

2.1.3 Securing Sentinel Log Manager Data

Because of the highly sensitive nature of the data in Sentinel Log Manager, you must keep the machine physically secure and in a secure area of the network. To collect data from event sources outside the secure network, use a remote Collector Manager. For more information on remote Collector Managers, see [“Installing Additional Collector Managers”](#) in the *Sentinel Log Manager 1.2.2 Installation Guide*.

Sentinel Log Manager is compatible with disk encryption technologies. These technologies provide a higher level of data privacy when they are used on the file systems where Sentinel Log Manager stores its data. However, software-based encryption technologies, such as dm-crypt, have a significant CPU overhead, they can dramatically reduce the performance of Sentinel Log Manager by 50% or more. On the other hand, hardware-based encryption technologies have a much lower impact on the performance of the rest of the system and are available from leading hard drive manufacturers.

2.1.4 Securing Communication with Networked Storage

You must consider the security implications before deciding the type of networked storage location to use. If you are using CIFS or NFS servers as networked storage locations to store the Sentinel Log Manager event data and raw data, remember that these protocols do not offer data encryption. An alternative is to use direct attached storage (local or SAN), which does not have the same security vulnerabilities. If you choose to use CIFS or NFS, it is important to configure the CIFS or NFS server to maximize the security of your data.

For more information about configuring the networked storage location server settings, see [Section 3.2.3, “Configuring Networked Storage,”](#) on page 36.

2.2 Best Practices

Use the following best practices to secure your Sentinel Log Manager server:

- ◆ [Section 2.2.1, “Changing Passwords,”](#) on page 17
- ◆ [Section 2.2.2, “Securing Communication with Collector Managers and Event Sources,”](#) on page 19
- ◆ [Section 2.2.3, “Auditing Sentinel,”](#) on page 19
- ◆ [Section 2.2.4, “Determining if Raw Data Files Were Tampered With,”](#) on page 19
- ◆ [Section 2.2.5, “Using CA Signed Certificates,”](#) on page 21

2.2.1 Changing Passwords

- ◆ [“Operating System Users”](#) on page 17
- ◆ [“Application and Database Users”](#) on page 18

Operating System Users

- ◆ [“Server Installation”](#) on page 18
- ◆ [“Collector Manager Installation”](#) on page 18

Server Installation

The Sentinel Log Manager server installation creates a `novell` system user and `novell` group that owns the installed files within the `install_directory`. The user's home directory is set to `/home/novell`. By default, if a new user is created, the password for the user is not set in order to maximize security. If you want to log in to the system as the `novell` user, you must set a password for the user after installation.

Collector Manager Installation

System users might vary in their level of security depending on the operating system on which the Collector Manager is installed.

Linux: The installer prompts you to specify the name of the system user who owns the installed files, as well as the location to create its home directory. By default, the system user is `esecadm`; however, you can change this system username. If the user does not exist, it is created along with its home directory. By default, if a new user is created, the password for the user is not set in order to maximize security. If you want to log in to the system as the user, you must set a password for the user after installation. The default group is `esec`.

During the client installation, if the user already exists, the installer does not prompt for the user again. This behavior is similar to the behavior while installing or uninstalling software. However, you can have the installer prompt for the user again:

- 1 Delete the user and group created at the time of first installation.
- 2 Clear the `ESEC_USER` environment variables from the `/etc/profile` file.

Windows: No users are created.

The password policies for system users are defined by the operating system that is being used.

Application and Database Users

Sentinel Log Manager application users are native database users and their passwords are protected by the native database platform, unless LDAP authentication is used. These users have only read access to certain tables in the database so that they can execute queries against the database. Users authenticated by LDAP do not have read access on the database.

The `admin` user is the administrator user for Sentinel Log Manager user applications.

By default, the following database users are created during installation:

- ♦ **dbauser:** The `dbauser` is created as a superuser who can manage the database and is typically the user who can log in to the pgAdmin. The password for the `dbauser` is accepted at the time of installation. This password is stored in the `user home directory/.pgpass` file. The system follows the PostgreSQL database password policies.
- ♦ **appuser:** The `appuser` is the non-superuser used by Sentinel Log Manager to connect to the database. By default, the `appuser` uses a password randomly generated during installation, which is stored encrypted in the `/etc/opt/novell/sentinel_log_mgr/config/server.xml` file. To modify the password for `appuser`, in the database use the following command:

```
db.sh sql SIEM dbauser "ALTER ROLE appuser WITH password 'new_password'"
```

Update the `server.xml` file by using the using the `/opt/novell/sentinel_log_mgr/bin/dbconfig` utility.

For more information, see [“Command Line Utilities” on page 177](#).

NOTE: There is also a PostgreSQL database user that owns the entire database, including system database tables. By default, the postgres database user is set to NOLOGIN, so that no one can log in as the PostgreSQL user.

2.2.2 Securing Communication with Collector Managers and Event Sources

You can configure Sentinel Log Manager to securely collect data from various event sources. However, secured data collection is determined by the specific protocols supported by the event source. For example, the Check Point LEA, Syslog, and Audit Connectors can be configured to encrypt their communication with event sources.

For more information on the possible security features that can be enabled, see the [Sentinel Plug-ins Web site \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html)

2.2.3 Auditing Sentinel

Sentinel Log Manager generates audit events for many actions performed by users and also for actions performed internally for system activities. These events are tagged with the `SentinelLogManager` tag and can be included within a report by selecting `include system events` and search by using the `rv145:SentinelLogManager` query. However, you must have the necessary permissions to view system events. For more information, see [Section 10.1.2, “Filtering Data,”](#) on page 153.

Sentinel Log Manager includes reports that are pre-configured to include only the events tagged with the `SentinelLogManager` tag.

A well-audited Sentinel Log Manager not only audits the events occurring within Sentinel Log Manager, but also the infrastructure that Sentinel Log Manager is running on top of. You can set up data collection from the machines and the devices that make up the Sentinel Log Manager infrastructure and tag them with the `SentinelLogManager` tag to enable a complete auditing of the systems that can affect the behavior of Sentinel Log Manager.

2.2.4 Determining if Raw Data Files Were Tampered With

The raw data files are stored in one of the following locations:

- ♦ Local storage location: `<SLM data directory>/rawdata/online`
- ♦ Networked storage location: `<SLM networked storage directory>/rawdata_archive`

If your networked storage is NFS or CIFS, then the NFS/CIFS share is automatically mounted to the `/var/opt/novell/sentinel_log_mgr/data/archive_remote` directory on the Sentinel Log Manager server. If the networked storage is SAN, then the NFS/CIFS share is mounted to the directory configured by you.

Each raw data file is either a `.zip` file or a `.log` file. A `.zip` file contains the `.log` files in a compressed format. For more information on raw data files, see [Section 3.1.1, “Raw Data,”](#) on page 29.

You can check the integrity of raw data files present in local or networked storage by using the `Collection > Raw Data` UI.

To determine if the deleted raw data files were tampered with:

- ♦ Verify the sequence number of JSON records. All JSON records have same ChainID with a monotonically increasing ChainSequence number starting with zero. There are no gaps or missing numbers in the ChainID sequence. If a new ChainID is present, then its ChainSequence begins with zero. If there are gaps in the sequence of numbers, then the records were either tampered with or were manually deleted.
- ♦ Verify the RawDataHash against the RawData. To do this, convert the RawData value to a sequence of bytes in UTF-8 format. Calculate a 256 SHA digest against those bytes. Convert the digest to a HEX string, and compare the string with the value in RawDataHash. If they are not identical, either the RawData or the RawDataHash file was tampered with.

If, for example, you want to compute the hash of a file on the file system on Linux, specify a command similar to the following:

```
sha256sum F6673C60-573A-102D-ADE0-003048306A7C/2010-06/15-1600.zip
```

For example, if, you want to query the database for the hash of a file, you can specify a command similar to the following:

```
db.sh sql SIEM dbuser "select FILE_HASH from RAW_DATA_FILES_INFO where FILE_NAME= '/F6673C60-573A-102D-ADE0-003048306A7C/2010-06/15-1600.zip';"
```

However, there is a possibility that a person tampered with the files in such a way that the tampering cannot be detected, because the person also recomputed the sequence number or the RawDataHash. To determine if the raw data files were tampered with, there is another method by using the hash key values of each raw data file stored in the database. The Sentinel Log Manager calculates a hash key value for every raw data file and stores it in the RAW_DATA_FILES_INFO table in the database.

The table has the following columns:

- ♦ **FILE_NAME:** This column contains the relative file name in the following format:
<Event Source UUID>/<Date>/<RawDataFile>
- ♦ **STATE:** This column indicates if the raw data file is in the local storage location or the networked storage location. If the value is ARCHIVED, the raw data file is in the networked storage location. If the value is ONLINE or COMPRESSED, then, the raw data file is in the local storage location. If the value is DELETED, it indicates that the file is deleted from the disk and is not present either in local or in networked storage location.
- ♦ **FILE_HASH:** Hash value is computed after the file is compressed and placed in a .zip file. Therefore, only files in the COMPRESSED or ARCHIVED state have a hash value. The FILE_HASH column contains an SHA256 hash key value computed over the contents of the file. The file is treated as a stream of binary bytes in order to compute the hash. The hash is stored as a HEX string (lowercase).

To determine if a file is tampered with, compute the SHA256 hash, convert it to a HEX string (lowercase), then compare this computed value with the hash value stored in the RAW_DATA_FILES_INFO table. If the values are different, it indicates that either the file or the database has been tampered with.

To determine if the files were deleted in an unauthorized way, you can scan the records in the RAW_DATA_FILES_INFO table and look for files whose STATE value is ARCHIVED, ONLINE, or COMPRESSED. You can ignore those marked DELETED. If the STATE value is ARCHIVED, the raw data file should be in the networked storage location. If the STATE value is ONLINE or COMPRESSED, the raw data file should be in the local storage location or the networked storage location.

2.2.5 Using CA Signed Certificates

Novell Sentinel Log Manager uses several digital, public-key certificates as part of establishing secure TLS/SSL communications. During the initial configuration of Sentinel Log Manager, these certificates are self-signed. In some circumstances, it might be necessary to obtain certificates digitally signed by a certificate authority (CA).

You can replace the self-signed certificate with a certificate signed by a well-known CA, such as VeriSign, Thawte, or Entrust. You can also replace the self-signed certificate with a certificate digitally signed by a less common CA, such as a CA within your company or organization.

NOTE: There are many well-known CAs and identifying which CAs are most commonly used varies with the country.

This section provides information on various certificates used in Sentinel Log Manager and also provides instructions on configuring the TLS/SSL certificates to get them digitally signed by CA and then importing the digitally signed certificates into Sentinel Log Manager:

- ♦ [“Types of Certificates” on page 21](#)
- ♦ [“Configuring the TLS/SSL Certificates” on page 22](#)

Types of Certificates

- ♦ [“Web Server Certificate” on page 21](#)
- ♦ [“Java Messaging Service Certificates” on page 21](#)
- ♦ [“Client Proxy Server Certificate” on page 21](#)

Web Server Certificate

The Web server certificate is used for the following purposes:

- ♦ It is used with Web browsers to connect to the Sentinel Log Manager Web user interface.
- ♦ It is used to establish trust relationships for the REST API calls between Sentinel Log Manager instances. For example, it is used when configuring Distributed Search.

If the Web server certificate is not signed by a well-known CA and you connect to the Sentinel Log Manager Web user interface, the `Connection is Untrusted` message is displayed.

Java Messaging Service Certificates

The Java Messaging Service (JMS) certificates include the following:

- ♦ Broker Certificate
- ♦ Client Certificate

The JMS certificates are used to establish secure communications between various components of Sentinel Log Manager, including the Sentinel Log Manager server and remote Collector Managers.

Client Proxy Server Certificate

The Client Proxy Server certificate is used to establish secure communication between the Sentinel Log Manager server and client applications, including the Web user interface.

Configuring the TLS/SSL Certificates

Novell Sentinel Log Manager provides the `ssl_certs` command line tool that helps with the certificate signing process. This tool is available at:

```
<installation_root>/opt/novell/sentinel_log_mgr/setup/ssl_certs
```

The tool can be run in an interactive mode or with the command line specifications and options. To see the command line options, change to the directory that contains `ssl_certs`, then run the `-help` command.

Configuring the TLS/SSL certificates involves the following steps:

- ♦ [“Generating a Certificate Signing Request” on page 22](#)
- ♦ [“Getting the Certificate Signing Requests Signed by the CA” on page 23](#)
- ♦ [“Importing the Digitally Signed Certificates into Sentinel Log Manager” on page 23](#)

Generating a Certificate Signing Request

To obtain a digitally signed certificate, you must first generate a Certificate Signing Request, which will be presented to the CA. To generate one or more Certificate Signing Request, perform the following steps on the Sentinel Log Manager server:

- 1 Log in as the `novell` user, or switch to the `novell` user.
- 2 Change to the `setup` directory:

```
cd $APP_HOME/setup
```

- 3 Run the `./ssl_certs` command.

The following options are displayed:

1. Generate certificate signing requests
2. Import Certificate Authority root certificate
3. Import certificates signed by Certificate Authority
4. Exit

- 4 Enter 1.

The following options are displayed:

1. Web Server
2. Java Messaging Service
3. Client Proxy Service
4. All
5. Done

- 5 Specify the service for which you want to obtain the signed certificates.
- 6 Specify a filename where the Certificate Signing Request must be saved.
The default filename is based on the internal name of the certificate entry.
- 7 Select another service if required, or enter 5 to select Done to exit from the service option.
- 8 Enter 4 to exit from the TLS/SSL certificate configuration.

The Certificate Signing Requests are now saved in the specified files.

Getting the Certificate Signing Requests Signed by the CA

- 1 Submit the Certificate Signing Requests to the CA for signature.
- 2 Obtain the signed certificate files from the CA.

The details of how this is done depend on the CA. For more information, consult your CA.

Importing the Digitally Signed Certificates into Sentinel Log Manager

Copy the files that contains the digital certificates signed by the CA to the Sentinel Log Manager server. In cases where the files are signed by an enterprise or organizational CA rather than a well-known CA, you must copy the CA's self-signed root certificate to the Sentinel Log Manager server.

To import the certificate files to the Sentinel Log Manager server:

- 1 Log in as the novell user, or switch to the novell user.
- 2 Change to the setup directory:

```
cd $APP_HOME/setup
```

- 3 Run the `.ssl_certs` command.

The following options are displayed:

1. Generate certificate signing requests
 2. Import Certificate Authority root certificate
 3. Import certificates signed by Certificate Authority
 4. Exit
- 4 (Conditional) For certificates that are signed by the enterprise or organizational CAs, enter 2, then specify the name of the file that contains the CA root certificates.
 - 5 (Conditional) For certificates that are signed by a well-known CA such as Verisign or Entrust, enter 3.
 - 5a Select the service for which you obtained the signed certificates.
 - 5b Specify the name of the file that contains the CA's signed digital certificate.
 - 6 Select another service if required, or enter 5 to select Done and exit from the service option.
 - 7 Enter 4 to exit from the TLS/SSL certificate configuration.
 - 8 Restart Sentinel Log Manager.

2.3 Network Communication Options

The various components of Sentinel Log Manager communicate across the network, and there are different types of communication protocols used throughout the system. All of these communication mechanisms affect the security of your system.

- ♦ [Section 2.3.1, "Communication between Sentinel Log Manager Processes," on page 24](#)
- ♦ [Section 2.3.2, "Communication between Sentinel Log Manager and the Event Source Manager Client Application," on page 25](#)
- ♦ [Section 2.3.3, "Communication between the Server and the Database," on page 25](#)
- ♦ [Section 2.3.4, "Communication with Web Browsers," on page 25](#)
- ♦ [Section 2.3.5, "Communication between the Database and Other Clients," on page 25](#)

2.3.1 Communication between Sentinel Log Manager Processes

Sentinel Log Manager processes include the Sentinel Log Manager server, Tomcat, and Collector Manager. They communicate with each other by using ActiveMQ.

The communication between these server processes is by default over SSL via the ActiveMQ message bus. The processes use SSL by reading the following information in `/etc/opt/novell/sentinel_log_mgr/config/configuration.xml`:

```
<jms brokerURL="failover://(ssl://localhost:${activemq.port.userapps}?wireFormat.maxInactivityDuration=30000)?randomize=false" interceptors="compression" keystore="{esecurity.config.home}/etc/opt/novell/sentinel_log_mgr/config/.activemqclientkeystore.jks" keystorePassword="password" password-file="{esecurity.config.home}/etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties" username="system"/>
```

The `jms` strategy shown in this XML snippet defines how the Sentinel Log Manager process connects to the server. This snippet defines the client side settings of the connection.

Table 2-1 XML Entries in the `configuration.xml` File

XML Entry	Description
<code>ssl://</code>	Indicates that SSL is used for secure connection. You should not modify this value.
<code>localhost</code>	The hostname or IP address where the Java message service (JMS) server is running.
<code>61616</code>	The port that the JMS server is listening on.
<code>?wireFormat.maxInactivityDuration=0&activemq.copyMessageOnSend=false</code>	This is where ActiveMQ configuration parameters are passed to the transport mechanism. These entries should be modified only if you are an expert in ActiveMQ.
<code>interceptors="compression"</code>	Enables compression over the connection. You should not modify this value.
<code>keystore="/etc/opt/novell/sentinel_log_mgr/config/.activemqclientkeystore.jks"</code>	The path to the Java keystore, which is used to check if the server is trusted.
<code>keystorePassword="password"</code>	The password to the Java keystore file.
<code>password="1fef3bcdd3fbc5cd795346a9f04ddc"</code>	The password to present to ActiveMQ for authenticating the connection. This corresponds to a password in the <code>/etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties</code> file.
<code>username="system"</code>	The username to present to ActiveMQ for authenticating the connection. This corresponds to a username in the <code>/etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties</code> file.

The server-side settings are defined in the `/etc/opt/novell/sentinel_log_mgr/config/activemq.xml` file. For instructions on how to edit the `activemq.xml` file, see the [ActiveMQ Web site \(http://activemq.apache.org/\)](http://activemq.apache.org/). However, Novell does not support the modification of the server-side settings.

2.3.2 Communication between Sentinel Log Manager and the Event Source Manager Client Application

The Sentinel Log Manager Event Source Management (ESM) client application by default uses SSL communication via the SSL proxy server.

For an architectural representation, see “[Novell Sentinel Log Manager Architecture](#)” in the *Sentinel Log Manager 1.2.2 Installation Guide*.

ESM knows to use SSL by reading the following information in `/etc/opt/novell/sentinel_log_mgr/config/configuration.xml`:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedClientS
trategyFactory">
  <transport type="ssl">
    <ssl host="10.0.0.1" port="10013" keystore="./novell/sentinel/
.proxyClientKeystore" />
  </transport>
</strategy>
```

2.3.3 Communication between the Server and the Database

The protocol used for communication between the server and the database is defined by a JDBC driver.

Sentinel Log Manager uses the PostgreSQL driver (`postgresql-version.jdbc3.jar`) to connect to the PostgreSQL database, which is a Java (Type IV) implementation. This driver supports encryption for data communication. To download the driver, refer to the [PostgreSQL Download Page \(http://jdbc.postgresql.org/download.html\)](http://jdbc.postgresql.org/download.html). To configure the encryption, refer to [PostgreSQL Encryption Options \(http://www.postgresql.org/docs/8.1/static/encryption-options.html\)](http://www.postgresql.org/docs/8.1/static/encryption-options.html).

NOTE: Turning encryption on has a negative impact on the performance of the system. Therefore, this security concern needs to be weighed against your performance needs. The database communication is not encrypted by default for this reason. Lack of encryption is not a major concern because communication with the database occurs over the localhost network interface.

2.3.4 Communication with Web Browsers

The Web server is by default configured to communicate via HTTPS. For more information, see the [Tomcat documentation \(http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html\)](http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html).

2.3.5 Communication between the Database and Other Clients

You can configure the PostgreSQL SIEM database to allow connections from any client machine that uses pgAdmin or another third-party application.

The PostgreSQL is compiled with the `--with-openssl` flag. You can configure it to use encrypted communication, although that is not the default setting. Typically all database communication in Sentinel Log Manager is performed locally and not over the network.

To allow pgAdmin to connect from any client machine, add the following line in the `/var/opt/novell/sentinel_log_mgr/3rdparty/postgresql/data/pg_hba.conf` file:

```
host all all 0.0.0.0/0 md5
```

If you want to limit the client connections that are allowed to run and connect to the database through pgAdmin, specify the IP address of the host in the above line.

The following line in the `pg_hba.conf` file is an indicator to PostgreSQL to accept connections from the local machine so that pgAdmin is allowed to run only on the server.

```
host all all 127.0.0.1/32 md5
```

To allow connections from other client machines, you can add additional `host` entries in the `pg_hba.conf` file.

To provide maximum security, by default, PostgreSQL only allows connections from the local machine.

2.4 Sensitive Data Locations

For certain components, passwords must be stored so that they are available to the components when the system needs to connect to a resource such as a database or an event source. In this case, the password is first encrypted to avoid unauthorized access to the clear-text password.

Even if the password is encrypted, you must ensure that the access to the stored password data is protected in order to avoid password exposure. For example, you can set permissions to ensure that files with sensitive data are not readable by other users.

Database credentials are stored in the `/etc/opt/novell/sentinel_log_mgr/config/server.xml` file.

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
  <property name="username">appuser</property>
  <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Following is an example of Database Credentials in the `configuration.xml` file:

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.ActiveMQStrategyFactory" name="ActiveMQ">
  <jms brokerURL="ssl://
localhost:61616?wireFormat.maxInactivityDuration=0&jms.copyMessageOnSend=false
" interceptors="compression" keystore="/etc/opt/novell/sentinel_log_mgr/config/
.activemqclientkeystore.jks" keystorePassword="password"
password="ebccfebf4ec3dac874494b992a91a3c9" username="system"/>
</strategy>
```

The following database tables store passwords (/certificate) in the encrypted format. You must limit access to these tables.

- ♦ **EVT_SRC**: column: `ect_src_config` column data
- ♦ **evt_src_collector**: column: `evt_src_collector_props`
- ♦ **evt_src_grp**: column: `evt_src_default_config`
- ♦ **md_config**: column: `data`
- ♦ **integrator_config**: column: `integrator_properties`
- ♦ **md_view_config**: column: `view_data`
- ♦ **esec_content**: column: `content_context, content_hash`
- ♦ **esec_content_grp_content**: column: `content_hash`
- ♦ **sentinel_plugin**: column: `content_pkg, file_hash`

Sentinel Log Manager stores both configuration data and event data in the following locations:

Table 2-2 Locations for Configuration Data and Event Data

Components	Location for Configuration Data	Location for Event Data
Event Data	<p>The database tables and file system at <code>/etc/opt/novell/sentinel_log_mgr/config</code>.</p> <p>This configuration information includes the encrypted database, event source, integrators, and passwords.</p>	<p>The database (EVENTS, CORRELATED_EVENTS, and the EVT_SMRY_* and AUDIT_RECORD tables), and the file system at <code>/var/opt/novell/sentinel_log_mgr/data/events</code>.</p> <p>NOTE: Event data can be archived to the file system as part of the partition management job.</p>
Collector Manager	<p>The file system at <code>/var/opt/novell/sentinel_log_mgr/data/eventdata</code> and <code>/var/opt/novell/sentinel_log_mgr/data/rawdata</code>. The most sensitive configuration information is the client key pair used to connect to the message bus.</p>	<p>Event data might be cached on the file system during error conditions such as the message bus being down or event overflow. This event data is stored in the <code>/var/opt/novell/sentinel_log_mgr/data/collector_mgr.cache</code> directory.</p>

2.5 Overriding the IP Address in the Web Server

On Sentinel Log Manager servers where there are multiple IP addresses (network interface), you can configure the Sentinel Log Manager Web server to listen on a specific IP address.

- 1 Log in to the Sentinel Log Manager server as the novell user.
- 2 Create the `start_tomcat.properties` file in the `/etc/opt/novell/sentinel_log_mgr/config` directory.
- 3 Add the following line in the `start_tomcat.properties` file:

```
SERVER_IP=<IP_address>
```

where `<IP_address>` is the IP address that you want to assign to the Sentinel Log Manager Web server.

- 4 Restart the Sentinel Log Manager services:

```
/opt/novell/sentinel_log_mgr/bin/./server.sh restart
```

2.6 Applying Updates for Security Vulnerabilities in Embedded Third-Party Products

Sentinel Log Manager includes embedded third-party products such as the Sun JRE, PostgreSQL, and ActiveMQ. Sentinel Log Manager includes patches to address the security vulnerabilities (CVE) for these products when updates for Sentinel Log Manager are released.

However, each of these products has its own release cycle, which means that there might be CVEs that are discovered before a Sentinel Log Manager update is released. You need to separately review the CVEs for each embedded third-party product, and decide whether to apply these updates to your Sentinel Log Manager system outside of the Sentinel Log Manager updates.

If you decide to apply patches to address these CVEs outside of a Sentinel Log Manager update, use the instructions in the following TID available in the [Novell Support Knowledge Base \(http://www.novell.com/support/\)](http://www.novell.com/support/).

- ♦ To update the Java Runtime Environment (JRE) manually, refer to TID 7009612.

3 Configuring Data Storage

Sentinel Log Manager stores compressed event data on the server file system and then stores it in a configured location for long-term storage.

The data files are deleted from the local and networked storage locations on a configured schedule. Raw data retention is governed by a single raw data retention policy. Event data retention is governed by a set of event data retention policies. All of these policies are configured by the Sentinel Log Manager administrator.

- ♦ [Section 3.1, “Types of Data,” on page 29](#)
- ♦ [Section 3.2, “Configuring Networked Storage Locations,” on page 35](#)
- ♦ [Section 3.3, “Configuring Data Retention Policies,” on page 42](#)
- ♦ [Section 3.4, “Configuring Disk Space Usage,” on page 46](#)
- ♦ [Section 3.5, “Verifying and Downloading Raw Data Files,” on page 46](#)
- ♦ [Section 3.6, “Viewing Local and Networked Storage Capacity,” on page 47](#)
- ♦ [Section 3.7, “Using Sequential-Access Storage for Long Term Data Storage,” on page 49](#)

3.1 Types of Data

Sentinel Log Manager receives two separate but similar data streams from the Collector Managers: the event data and the raw data. The data is moved from the local storage, compressed, file-based storage to a user-configured, compressed networked storage location on a regular basis.

- ♦ [Section 3.1.1, “Raw Data,” on page 29](#)
- ♦ [Section 3.1.2, “Event Data,” on page 34](#)

3.1.1 Raw Data

The raw data files are unprocessed events that are received by the Connector and sent directly to the Sentinel Log Manager message bus. This data is written to the Sentinel Log Manager server. When the event is sent to the message bus, the following additional information is also sent without altering the original event:

- ♦ SHA-256 hash of the event
- ♦ Chaining indicator (which is reset to 0 whenever the Sentinel Log Manager event source is restarted)
- ♦ Raw Data ID (in `s_RV25`)
- ♦ Event source, Connector, Collector, and Collector Manager node IDs
- ♦ Event ID (stored in `s_RV25`)
- ♦ Event source, Connector, Collector, and Collector Manager node IDs

All raw data is sent to the Sentinel Log Manager without filtering. Because the raw data is not searched or used to generate reports, the data is not indexed.

- ♦ [“Raw Data Storage” on page 30](#)
- ♦ [“Raw Data Representation” on page 31](#)

Raw Data Storage

In Sentinel Log Manager, raw data is always stored. Raw data is stored in partitions that are based on the time and the event source. Raw data partitions are individual files. They are created every hour, and are closed within 10 minutes after the elapsed time. Older, inactive partitions are compressed.

The raw data files can be stored in one of the following locations:

- ♦ Local storage location: `<SLM data directory>/rawdata/online`
- ♦ Networked storage location: `<SLM archive directory>/rawdata_archive`

When a raw data file is closed, it is renamed to identify the closed files. Files in the open state have a `.open` extension. When they are closed, they are renamed with a `.log` extension. At the configured interval, after they are closed, they are compressed and given a `.zip` extension. The compressed raw data files are moved from the local storage to the networked storage location.

The following table describes the directory structure of the raw data in the local storage under the installation directory:

Table 3-1 Raw Data Directory Structure

Directory structure	Description
<code>/data</code>	The primary directory for all data storage.
<code>/data/rawdata</code>	The subdirectory where all raw data is stored.
<code>/data/rawdata/online</code>	The directory where all the raw data in the local storage is stored.
<code>/data/rawdata/ EventSource UUID</code>	The subdirectory name is the universally unique identifier (UUID) of the event source (for example, E20D0840-1E0A-102C-9F30-000C2949BA91). There is one subdirectory for each event source under the <code>online</code> subdirectory. That subdirectory contains all raw data received from that event source.
<code>/data/rawdata/ EventSource UUID/ Month</code>	The subdirectory name is in the <code>yyyy-mm</code> format. For example, 2009-05 indicates May 2009. Data in the event source subdirectory is partitioned by month. Each month has its own subdirectory.

Directory structure	Description
/data/rawdata/ EventSource UUID/ Month/1 Hour Data Files	<p>Each file in the Month directory contains data received during a specific one-hour period. Most data in the file has a time stamp that is within the one-hour period.</p> <p>The name of the file indicates the day of the month and the one-hour period that is represented.</p> <p>The filename format is dd-hhmm.extension.</p> <p><i>dd</i> is the day of the month.</p> <p><i>hh</i> is the hour of the day.</p> <p><i>mm</i> is the minute of the hour.</p> <p>The extension is either .open or .log or .zip (compressed).</p> <p>For example:</p> <p>A filename of 08-1300.open indicates that the file contains uncompressed data received on the 8th day of the month between 01.00 p.m. and 02.00 p.m.</p> <p>A filename 08-0900.log indicates that the file contains uncompressed data received on the 8th day of the month between 09.00 a.m. and 10.00 a.m. The file is closed, but not yet compressed.</p> <p>A filename 08-0000.zip indicates that the file contains compressed data received on the 8th day of the month between 12.00 a.m. and 01.00 a.m.</p>

If the raw data files are stored in the local storage location, the full path name of the file is in the following format:

<SLM data directory>/rawdata/online/<event source UUID>/<Date>/<RawDataFile>

For example:

/var/opt/novell/sentinel_log_mgr/data/rawdata/online/A75CF6A0-4948-102D-A615-000C29A9C3DB/2010-05/24-0600.zip

In this example, */var/opt/novell/sentinel_log_mgr/data* is the data directory for Sentinel Log Manager.

If the raw data files are stored in the networked storage location, the full path name would be as follows:

<SLM archive directory>/rawdata_archive/<event source UUID>/<Date>/<RawDataFile>

For example:

/slm_archive_data/rawdata_archive/A75CF6A0-4948-102D-A615-000C29A9C3DB/2010-05/24-0600.zip

In this example, */slm_archive_data* is the networked storage directory configured by the user.

Raw Data Representation

Each raw data event is represented as a single line in a raw data file. Each line is a JSON object with the following format:

```

{
  "EventDate": "<date>",
  "EventRecordID": "<event record uuid>",
  "RawData": "<raw data>",
  "RawDataHash": "<SHA256 hash of raw data, in hex format>",
  "EventSourceManagerID": "<uuid of event source manager>",
  "CollectorID": "<uuid of collector>",
  "EventSourceID": "<uuid of event source>",
  "ChainID": "<chain ID>",
  "ChainSequence": "<Sequence number>"
}

```

The following table describes each of the fields in the raw data event:

Table 3-2 Raw Data Representation

Field Name	Description
EventDate	<p>This is the date and time when Sentinel Log Manager received this event and not the date and time when the event occurred.</p> <p>Example: "05/07/2009 05:23.790"</p>
EventRecordID	<p>The record ID of the corresponding event record in the event store.</p> <p>Example: "595829C0-1C8F-102C-A922-000C2949BA91"</p> <p>NOTE: If no event record was created because of filtering, the record ID might not point to anything.</p>
RawData	<p>The original raw data received by the event source.</p>
RawDataHash	<p>The SHA-256 hash of the RawData value represented as a HEX string. The hash is calculated by converting the RawData value to a UTF-8 string and then performing the hash over that string.</p> <p>To detect tampering, each raw data event is stored with a SHA-256 hash value.</p> <p>Example: cc661009e2f3dc565c0c7fe25b705219004dcd8132c0b0a7e987bfdcb55e49cf</p>
EventSourceID	<p>The UUID of the event source from which the raw data originated.</p> <p>Example: A2A0C600-1C6C-102C-A781-000C2949BA91</p>
EventSourceGroupID	<p>The UUID of the event source group (Connector) to which the event source was connected when the raw data was received.</p> <p>Example: A2A0C600-1C6C-102C-A77A-000C2949BA91</p> <p>NOTE: Different raw events from the same event source can have different event source group IDs, because event sources can be moved from one Connector to another.</p>
CollectorID	<p>The UUID of the Collector that the Connector and event source were connected to when the raw data was received.</p> <p>NOTE: Different raw events from the same event source can have different Collector IDs, because event sources and event source groups can be moved from one Collector to another.</p> <p>Example: A2A0C600-1C6C-102C-A779-000C2949BA91</p>

Field Name	Description
EventSourceManagerID	The UUID of the Event Source Manager object where this raw data was received. Example: C76D2820-C395-1029-BB86-001321B5C0B3
ChainID	A random number that identifies a raw data chain. Whenever an event source is stopped and restarted between generation of raw data events, a new ChainID number is generated. To detect tampering, each raw data event is stored with a ChainID and a ChainSequence number. Example: 1241630654754
ChainSequence	A sequence number within a particular raw data chain. The raw data events in a given raw data chain must have an uninterrupted sequence of numbers starting with 0. In addition, all raw data events in a given raw data chain must appear sequentially in the files, with no other chains intermixed. If a raw data chain can span files, the sequence should continue uninterrupted into the file that represents every hour during which raw data was received. Example: 4 NOTE: If no raw data is received for the one-hour period, the file records only from the next arrival of raw data. Nonetheless, the raw data chain sequence should continue uninterrupted until a new raw data chain begins. A new raw data chain is signaled by a changed ChainID value, and a ChainSequence value of zero (0).

The following examples show three raw data records:

```
{
  "EventDate": "05\24\2010 06:15:06.676",
  "EventRecordID": "A75CF6A0-4948-102D-A61C-000C29A9C3DB",
  "RawData": "Sep 22 10:22:00 testhost Message #100",
  "RawDataHash": "7003c0e0be4ddf43a3b49026a37483f59c7f839950f581ec9fde5dea43da90f5",
  "EventSourceManagerID": "C76D2820-C395-1029-BB86-001321B5C0B3",
  "CollectorID": "A75CF6A0-4948-102D-A613-000C29A9C3DB",
  "EventSourceGroupID": "A75CF6A0-4948-102D-A614-000C29A9C3DB",
  "EventSourceID": "A75CF6A0-4948-102D-A615-000C29A9C3DB",
  "ChainID": "1274696106664",
  "ChainSequence": "0"
}
{
  "EventDate": "05\24\2010 06:15:07.358",
  "EventRecordID": "A75CF6A0-4948-102D-A624-000C29A9C3DB",
  "RawData": "Sep 22 10:22:00 testhost Message #99",
  "RawDataHash": "f5681ba965144d2d22b13188767d94540b5fe57904afcee5821854bde2afca72",
  "EventSourceManagerID": "C76D2820-C395-1029-BB86-001321B5C0B3",
  "CollectorID": "A75CF6A0-4948-102D-A613-000C29A9C3DB",
  "EventSourceGroupID": "A75CF6A0-4948-102D-A614-000C29A9C3DB",
  "EventSourceID": "A75CF6A0-4948-102D-A615-000C29A9C3DB",
  "ChainID": "1274696106664",
  "ChainSequence": "0"
}
```

```

    "ChainSequence": "1"
  }
  "EventDate": "05\24\2010 06:15:07.988",
  "EventRecordID": "A75CF6A0-4948-102D-A62A-000C29A9C3DB",
  "RawData": "Sep 22 10:22:00 testhost Message #98",
  "RawDataHash": "98435b5dba95633699b88d07782109876e8ceb4169d567602f2c92657118645d",
  "EventSourceManagerID": "C76D2820-C395-1029-BB86-001321B5C0B3",
  "CollectorID": "A75CF6A0-4948-102D-A613-000C29A9C3DB",
  "EventSourceGroupID": "A75CF6A0-4948-102D-A614-000C29A9C3DB",
  "EventSourceID": "A75CF6A0-4948-102D-A615-000C29A9C3DB",
  "ChainID": "1274696106664",
  "ChainSequence": "2"
}

```

3.1.2 Event Data

Event data is processed by the Collector running on the Collector Manager. For more information about event processing and parsing, see [Chapter 4, “Configuring Data Collection,” on page 55](#). Event data is subject to filtering rules set up on the event source, Connector, and Collector, so event data can be dropped, if necessary.

The event data partitions are closed after two days, and no more events are written to them. Even though the duration of the partition is only for one day, partitions are closed after two days to accommodate events arriving at the last moment. After the partitions are closed, they are compressed and moved to networked storage. For events that arrive late after two days (after the original partition was closed), the system creates another partition to store the late coming events. This partition is appended with the date that gives an indication of when those events arrived at data storage.

Local storage partitions are stored in the `/var/opt/novell/sentinel_log_mgr/data/eventdata` directory, which is on the local file system. Partitions are created based on the dates and retention policies.

A central partition index is maintained in the database that keeps track of all the existing partitions and their location.

The following table describes the directory structure under the installation directory where event data is stored:

Table 3-3 *Event Data Directory Structure*

Directory Structure	Description
<code>/data</code>	The primary directory for all data storage.
<code>/data/eventdata</code>	The subdirectory where all event data is stored.
<code>/data/eventdata/YYYYMMDD_<classid></code>	A partition consists of the events for a single day (midnight-midnight UTC) within a given data retention class and is held within a subdirectory named <code>YYYYMMDD_<class-id></code> . YYYYMMDD: UTC date stamp. <class_id>: UUID identifier associated with the data retention class.

Directory Structure	Description
/data/eventdata/ YYYYMMDD_GUID- POLICY- RETENTION_YYYYMMDD	The partition that stores events that arrive late after 2 days (after the original partition was closed). YYYYMMDD(prefixed date): UTC date stamp. GUID-POLICY-RETENTION: Retention policy ID. YYYYMMDD(suffixed date): Date on which the events arrived at data storage.
/data/eventdata/ YYYYMMDD_<class_id>/ events.evt	events.evt contains the binary event data for the partition. The format of the binary event data is stored as a Reliable Persistent Random Access Compressed Stream.
/data/eventdata/ YYYYMMDD_<class_id>/ index	The index directory contains the Lucene index for the partition.

3.2 Configuring Networked Storage Locations

All closed data files are copied from the local storage location to the networked storage location. The original files are retained on Sentinel Log Manager to facilitate faster searches. However, if the Sentinel Log Manager server disk space usage nears a user-defined threshold, duplicate data files are deleted from the Sentinel Log Manager server.

NOTE: While configuring networked storage, ensure that the networked storage location is larger than the local storage to avoid data loss. For more information on data storage requirement estimation, see [“Data Storage Requirement Estimation”](#) in the *Sentinel Log Manager 1.2 Installation Guide*.

- ♦ [Section 3.2.1, “Supported Storage Options,” on page 35](#)
- ♦ [Section 3.2.2, “Types of Networked Storage,” on page 36](#)
- ♦ [Section 3.2.3, “Configuring Networked Storage,” on page 36](#)
- ♦ [Section 3.2.4, “Enabling or Disabling Networked Storage,” on page 40](#)
- ♦ [Section 3.2.5, “Unmounting a Networked Storage Location,” on page 40](#)
- ♦ [Section 3.2.6, “Changing the Networked Storage Location,” on page 41](#)

3.2.1 Supported Storage Options

The Novell Sentinel Log Manager supports the following types of storage options:

- ♦ **Local Storage or SAN:** The local storage or Storage Area Network (SAN) option includes storage that is attached directly to the Sentinel Log Manager machine. This option provides the best combination of performance, security, and reliability.
- ♦ **SMB or CIFS:** The SMB protocol is also known as CIFS protocol. The latest implementation from Microsoft is referred to as SMB 2.

- ♦ **NFS:** The NFS protocol requires significant configuration to improve performance and security, and it is recommended only if you already have a well-established NFS infrastructure in your environment.

If the networked storage is an NFS server, additional configuration is necessary to ensure that the Sentinel Log Manager server has the necessary permissions. See [“Exporting the Networked Storage Volume” on page 38](#) for more information.

WARNING: Only one Sentinel Log Manager should be configured to use a particular networked storage directory (remote share). Configuring the same networked storage location across multiple Sentinel Log Manager servers can cause system failure.

3.2.2 Types of Networked Storage

You can enable networked storage on Sentinel Log Manager for both the raw data and event data.

- ♦ [“Raw Data Storage” on page 36](#)
- ♦ [“Event Data Storage” on page 36](#)

Raw Data Storage

A raw data file can be in the `.open` state when the data is currently being written, in the `.log` state when the data is no longer being written to the file but the file is not yet compressed, or in the `.zip` state when the file is compressed. The file compression process runs every 10 minutes, by default. These compressed files appear in both the local storage and networked storage locations if networked storage is configured and enabled.

If networked storage is configured and enabled, compressed raw data files are copied to the configured networked storage location every 15 minutes.

For more information on raw data storage, see [“Raw Data Storage” on page 30](#).

Event Data Storage

You can enable and configure networked storage for event data stored on the Sentinel Log Manager server.

If networked storage is enabled, the closed files are moved to networked storage every midnight UTC and also whenever the server starts. These files are compressed in the local storage location, but the file indexes are compressed before moving to the networked storage. If the networked storage location is not configured or if there is any problem while moving the closed files, attempts are made every 60 seconds to move the files to networked storage until it succeeds.

3.2.3 Configuring Networked Storage

NOTE: The NFS, SMB or CIFS, and SAN must be configured so that Sentinel Log Manager has read and write permissions.

For CIFS and NFS, if multiple Sentinel Log Manager instances are moving the closed partitions to the same networked storage location, ensure that each Sentinel Log Manager instance has its own unique directory on that networked storage location.

- ♦ “Configuring a SAN/Local Directory as a Networked Storage Location” on page 37
- ♦ “Configuring an SMB or CIFS Server as a Networked Storage Location” on page 37
- ♦ “Configuring an NFS Server as a Networked Storage Location” on page 38

Configuring a SAN/Local Directory as a Networked Storage Location

This is the preferable configuration for the best performance, security, and reliability.

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Configuration* tab.

The configuration page is displayed.

- 4 From the Data Storage Location section, select *SAN (locally mounted)* as the networked storage location.

Data Storage Location

Networked storage is not configured.

Configure Networked Storage Location:
 NFS CIFS SAN (locally mounted)

Note: The SAN partition must already be mounted (manually) to the location specified below.

Location:

Test

- 5 In the *Location* field, specify the local directory path or the location on which the storage area network (SAN) is mounted.

The SAN partition you must be manually mounted before the location is specified.

- 6 Click *Test* to check if the write permissions for the specified location are available.

If the location is configured properly, a message is displayed confirming that the test is successful.

If the location is not configured, the test fails, the reason for failure is displayed.

- 7 Click *Save* to configure the specified networked storage location.

Configuring an SMB or CIFS Server as a Networked Storage Location

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Configuration* tab.
- 4 In the Data Storage Location section, select *CIFS*.

Data Storage Location

Networked storage is not configured.

Configure Networked Storage Location:
 NFS CIFS SAN (locally mounted)

Server:

Share:

Username:

Password:

Mount options:

5 Specify the following information

Server: Specify the IP address or hostname of the machine where the CIFS server, also known as the SMB server is configured.

Share: Specify the share name of the SMB or CIFS server. The mounted shares are unmounted when the server stops and are mounted again when the server starts. If the configured share unmounts, the Sentinel Log Manager server detects this and mounts it again.

Username: Specify the username (if one is assigned) to access the share.

Password: Specify the password (if one is assigned) to access the share.

Mount Options: Specifies the options that are used while mounting the networked storage location of the SMB or the CIFS server.

You can also specify a new mount options. For more information about the available NFS mount options, see the [mount.cifs \(8\) - Linux man page \(http://linux.die.net/man/8/mount.cifs\)](http://linux.die.net/man/8/mount.cifs).

The default mount options are `file_mode=0660,dir_mode=0770`.

6 (Optional) Click *Restore Defaults* to restore the default mount options.

7 Click *Test* to mount the SMB or CIFS server and to check the write permissions on the server. If the CIFS server is configured properly, a message is displayed that the test is successful.

If the CIFS server is not configured, the test fails, and the reason for failure is displayed.

8 Click *Save* to configure the specified networked storage location.

Configuring an NFS Server as a Networked Storage Location

The NFS protocol requires significant configuration to improve performance and security, and it is recommended only when you already have a well-established NFS infrastructure in your environment.

- ♦ [“Exporting the Networked Storage Volume” on page 38](#)
- ♦ [“Configuring NFS as a Networked Storage Location” on page 39](#)

Exporting the Networked Storage Volume

The NFS server needs to export (share) the networked storage volume to the Sentinel Log Manager server so that the networked storage is readable by the `root` user on the Sentinel Log Manager server. The settings described in this section indicate one method to achieve this readability:

- ♦ The NFS server must have a user and a group with a UID and a GID that correspond to the `nove11` user and group on the Sentinel Log Manager server.

In the following examples, the user on the NFS server is `nove11` with `UID=5555` and the group is `nove11` with `GID=5555`. The Sentinel Log Manager server has the hostname `log-manager-server`, which can be resolved by the NFS server.

- ♦ The networked storage destination directory on the NFS server must be owned by the `novell` user and group. In the following examples, the networked storage destination is `/archive`.
- ♦ The `root` user on the Sentinel Log Manager server must be mapped to the `novell` user and group on the NFS server.

- ♦ **Linux:** Add the following line to the `/etc/exports` file:

```
/archive log-manager=server(rw,root_squash,anonuid=5555,anongid=5555)
```

- ♦ **Solaris:** Add the following line to the `/etc/dfs/dfstab` file:

```
/usr/bin/share -F nfs -o sec=sys,rw=log-manager-server,anon=5555 -d "/archive" /archive
```

- ♦ **HP-UX:** Add the following line to the `/etc/exports` file:

```
archive -access=log-manager-server,anon=5555
```

You can speed up the archiving process by adding the `async` option. However, this might increase the risk of lost or corrupt networked storage if the NFS server crashes. The following examples demonstrate using the `async` option:

- ♦ **Linux:** Add the following line to the `/etc/exports` file:

```
/archive log-manager=server(rw,root_squash,anonuid=5555,anongid=5555),async
```

- ♦ **HP-UX:** Add the following line to the `/etc/exports` file:

```
archive -access=log-manager-server,anon=5555,async
```

For information on security recommendations for NFS, see [Section 2.1.3, “Securing Sentinel Log Manager Data,” on page 17](#).

Configuring NFS as a Networked Storage Location

You must configure networked storage in the Sentinel Log Manager administrator interface as follows:

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Configuration* tab.
- 4 In the Data Storage Location section, select the *NFS* option.

Data Storage Location

Networked storage is not configured.

Configure Networked Storage Location:
 NFS CIFS SAN (locally mounted)

Server:

Share:

Mount options:

- 5 Specify the following information:

Server: Specify the IP address or hostname of the machine where the NFS server is configured.

Share: Specify the share name of the NFS server.

The mounted shares are unmounted when the server stops and are mounted again when the server starts. If the configured share unmounts, the Sentinel Log Manager server detects this and mounts it again.

Mount Options: Specifies the options that are used while mounting the networked storage location of the NFS server.

You can also specify a new mount options. For more information about the available nfs mount options, see [NFS \(5\) Linux Programmer's Manual \(http://unixhelp.ed.ac.uk/CGI/man-cgi?nfs+5\)](http://unixhelp.ed.ac.uk/CGI/man-cgi?nfs+5).

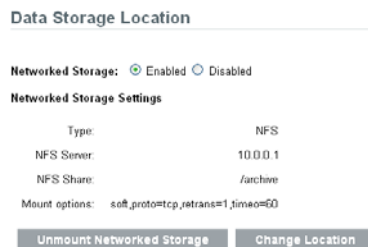
The default mount options are `soft,proto=tcp,retrans=1,timeo=60`.

- 6 (Optional) Click *Restore Defaults* to restore the default mount options.
- 7 Click *Test* to verify the configuration of the NFS server and to check the write permissions on the server. If the NFS server is configured properly, a message is displayed that the test is successful. If the NFS server is not configured, the test fails and the reason for failure is displayed. This procedure tests a subset of all of the settings that are necessary for the NFS server and client.
- 8 Click *Save* to configure the specified networked storage location.

3.2.4 Enabling or Disabling Networked Storage

The options to enable and disable uncorked storage appear only when the data storage location is configured. However, event search and reporting work even when the data storage is disabled.

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Configuration* tab.



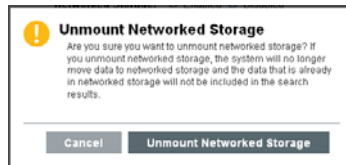
- 4 To enable writing to data storage location, select *Enabled*. You can write both the raw data and event data to the configured networked storage location. To configure the networked storage locations, refer to [“Configuring Networked Storage” on page 36](#).
- 5 To disable writing to the data storage location, select *Disabled*. This selection disables the writing of raw data and event data storage. You cannot write to the data storage location, but you can still read the stored data. Search shows the events that are stored, and you can also download the stored raw data.
- 6 Click *Save*.

3.2.5 Unmounting a Networked Storage Location

If the networked storage location is unmounted, data storing is disabled and searches and reports results include only the local storage data. The *Unmount Networked Storage* option appears only if the data storage location is configured.

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.

- 3 Click the *Configuration* tab.
- 4 To unmount the data storage location, select *Unmount Networked Storage*.
A confirmation message is displayed, asking if you really want to unmount the networked storage.



If you unmount networked storage, Sentinel Log Manager can no longer access the data in the networked storage. If the networked storage location is configured to a remote location such as NFS or SMB/CIFS, the networked storage location is unmounted.

- 5 Click *Unmount Networked Storage*.

3.2.6 Changing the Networked Storage Location

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Configuration* tab.
- 4 In the Data Storage Location section, select *Change Location*. The *Change Location* option is displayed only if the networked storage location is configured.

A confirmation message is displayed, asking if you want to change the networked storage location.

- 5 Click *Change Location*.

The following page allows you to configure a new networked storage location.

Data Storage Location

Changing the networked storage location is a three step process:

1. Configure the new networked storage location. Network storage will temporarily be disabled.
2. Copy the files from the old networked storage location to the new networked storage location. This you do manually.
3. After copying the files, click the "Copy Done" button to start storing data to the new networked storage location.

Disable data collection if local storage fills up before networked storage is resumed at new location.

Configure New Networked Storage Location:

NFS CIFS SAN (locally mounted)

Server:

Share:

Mount options:

- 6 Select the option to disable data collection.
You can select this option to avoid filling up the local storage before data is being moved to the new location. If this option is not selected and if the local storage is filled up before the new data storage location is configured, the oldest data is deleted to make space for the incoming data.
- 7 Configure the new data storage location.
For more information about configuring the NFS or SMB/CIFS or local/SAN networked storage locations, see "[Configuring Networked Storage](#)" on page 36.

- 8 Click *Save* to save the changes and configure the new networked storage location.
- 9 Manually copy the files from the old networked storage location to the new networked storage location.
- 10 After copying the files, select the *Copy Done* option to start data storage at the new location.
- 11 (Optional) Click *Cancel* to return to the previous networked storage configuration.

3.3 Configuring Data Retention Policies

The data retention policies control when data is deleted from the system. A retention policy contains a filter that is used to identify the events for which the retention policy applies and the minimum and maximum number of days these events should be kept in the system.

You can configure one or more data retention policies to control the duration for which specific types of events are retained in Sentinel Log Manager. Except for the Raw Data Retention policy, all of the configured policies apply to the event data.

The configured retention policies are displayed in the data retention policy table. By default, the data retention policy table is refreshed every 30 seconds to reflect the changes made by multiple administrators.

- ♦ [Section 3.3.1, “Raw Data Retention Policy,” on page 42](#)
- ♦ [Section 3.3.2, “Event Data Retention Policies,” on page 42](#)
- ♦ [Section 3.3.3, “Rules for Applying a Retention Policy,” on page 45](#)

3.3.1 Raw Data Retention Policy

The Raw Data Retention policy controls the duration for which the raw data is kept in the system before it is deleted. The Raw Data Retention policy cannot be deleted or disabled. However, you can modify the *Keep at most* and *Keep at Least* values, which determine the maximum number of days after which the raw data file is deleted and the minimum number of days for which a raw data file is kept.

The process to delete raw data files runs every time the server is started, every hour because that is when the raw data files are closed, and whenever the *Keep at most* value is changed. All the files exceeding the retention time are removed permanently from the local and networked storage locations.

3.3.2 Event Data Retention Policies

The event data retention policies control the duration for which different types of event data are kept in the system before being deleted.

- ♦ [“Adding a Data Retention Policy” on page 42](#)
- ♦ [“Activating or Deactivating a Data Retention Policy” on page 44](#)
- ♦ [“Modifying a Data Retention Policy” on page 44](#)
- ♦ [“Deleting a Data Retention Policy” on page 44](#)

Adding a Data Retention Policy

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.

- 3 Click the *Configuration* tab.
- 4 In the Data Retention section, click the *Add a policy* option located at the top right corner of the policy table.

Data Retention [Add a policy](#)

Active	Name	At Least	At Most	Size	Events	Edit
<input checked="" type="checkbox"/>	Default Data Retention	90		0 MB	0	Edit
<input checked="" type="checkbox"/>	Raw Data Retention	NA	365	0 MB	NA	Edit

Policy Name: *

Filter: *

Keep at least: * Days

Keep at most: Days

[Cancel](#) [Save](#)

- 5 Specify a name for the retention policy.

The policy name must be unique and must contain alphanumeric characters. If a duplicate policy name is specified, an error message is displayed when you save the retention policy.

- 6 Specify a filter value. The filter value uses the same syntax as searches.

For example, assume that the filter field contains a filter such as `sev:[3 TO 5] AND (evt:"SyslogNICListener")`. This filter value matches all the events with a severity of 3, 4 or 5 and event name `SyslogNICListener`.

For more information, see [Section 5.1.2, "Running an Advanced Search," on page 78](#).

- 7 Click the *show tips* link to view the tag names that can be used to define the retention policy filter.

For example, use `sev:[0 TO 1]` to define a retention policy that applies to all events with a severity of 0 or 1.

- 8 In the *Keep at least* field, specify the minimum number of days to retain the events in the system. The value must be a valid positive integer.

- 9 (Optional) Specify the maximum number of days for which the events should be retained in the system.

The value must be a valid positive integer and must be greater than or equal to the *Keep at least* value. If no value is specified, the system retains the events in the system until the space is available.

- 10 Click *Save*. The newly created policy is displayed under the data retention table.

The table also contains the following additional columns:

- ◆ **Size:** Displays the amount of space used to store the events for the respective retention policy.
- ◆ **Events:** Displays the number of events for the selected retention policy.

The policies are sorted in alphabetical order by policy name. The default retention policy is always shown as the last policy in the list.

If there is any error when saving a retention policy, an error message is displayed at the top of the policy table.

For more information, see ["Data Expiration Policy" on page 192](#).

Activating or Deactivating a Data Retention Policy

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Configuration* tab.
The data retention policy table is displayed in the Data Retention section.
- 4 To activate a retention policy, select the check box in the *Active* column.
- 5 To deactivate the retention policy, clear the check box next to the policy.
You cannot deactivate the default data retention policy.

Modifying a Data Retention Policy

You cannot modify the name of the default data retention policy. You can only modify the *Keep at Least* and *Keep at Most* values for a data retention policy.

You can edit only one policy at a time. If you try to modify a second policy while you are in the process of modifying the first, the first policy opened for modification is closed without saving the changes.

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Configuration* tab.
The data retention policy table is displayed in the *Data Retention* section.
- 4 To edit the retention policy, click the *Edit* link next to the configured policy.
The policy editor opens within the policy table.
- 5 Specify the minimum and maximum days to store events.
- 6 Click *Save* to save the changes to the existing policy.

Deleting a Data Retention Policy

You can delete only those policies that are configured by you. You cannot delete the default data retention policies and the Raw Data Retention policy.

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Configuration* tab.
The data retention policy table is displayed in the Data Retention section.
- 4 To delete the retention policy, click the *Edit* link next to the configured policy.
The policy editor opens within the policy table.

Data Retention

[Add a policy](#)

Active	Name	At Least	At Most	Size	Events	Edit
<input type="checkbox"/>	test					

Policy Name: *

Filter: *

[show tips](#)

Keep at least: * Days

Keep at most: Days

[Delete](#) [Cancel](#) [Save](#)

Active	Name	At Least	At Most	Size	Events	Edit
<input checked="" type="checkbox"/>	Default Data Retention	90		91.14 MB	470.02 K	Edit
<input checked="" type="checkbox"/>	Raw Data Retention	90	365	222 MB	NA	Edit

5 Click *Delete*. A confirmation message is displayed.

6 Click *Delete*.

The selected data retention policy is deleted from the data retention table.

3.3.3 Rules for Applying a Retention Policy

You can apply multiple data retention policies, including the default data retention policy, to event data.

While applying a retention policy, consider the following:

- ◆ Disk usage and space availability on both the local and networked storage
- ◆ Data retention policy

The above factors are interdependent and influence the order in which Sentinel Log Manager chooses to delete data from the local storage or networked storage locations. For more information, see [Section B.3, “Data Expiration Policy,” on page 192](#).

To determine how long an event can be retained before deleting it from the local and networked data storage, apply the following rules:

1. If an event meets the criteria of only one data retention policy filter, that data retention policy is applied to the event.
2. If an event does not meet the criteria for any of the data retention policies, the default data retention policy is applied to that event.
3. If an event meets the criteria for more than one of the data retention policies, the following guidelines are used to determine which data retention policy should be applied:
 - ◆ If the maximum retention period of a policy is shorter than the others, that policy is applied. (If the maximum retention period is not specified for a policy, then the policy is considered to have a long maximum retention period.)
 - ◆ If multiple matching policies have the same shortest maximum retention period, the policy with the longest minimum retention period is applied.
 - ◆ If multiple matching policies have the same shortest maximum retention period and the same longest minimum retention period, the system arbitrarily applies one of the policies.

NOTE: Events that are received considerably after they were originally generated are updated with a current time stamp and stored in the current file. This affects how long they stay in the system before they are deleted.

3.4 Configuring Disk Space Usage

If networked storage is enabled, the event data is copied to the networked storage location after two days, and a local copy remains until space is available. Raw data is moved to the networked storage location after approximately one hour.

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Configuration* tab.

In the *Disk Space Usage* section, the *Local Storage Size* field displays the total storage size currently used by Sentinel Log Manager.

- 4 Specify the local storage utilization value:
 - ◆ Specify a value to start the data storage from local storage when the specified value is reached.
 - ◆ Specify a value to stop the data storage from local storage when the specified value is reached.

These settings are the settings at which Sentinel Log Manager starts (and stops) deleting the duplicate data files that are in local storage. These copies are kept in the local storage until this disk usage threshold is reached in order to speed up searches and reports. When the threshold is reached and files are deleted, the networked storage becomes the sole location for the data.

Networked storage size specifies the value of the networked storage space.

- 5 Specify the maximum archive size to be used as part of the total available archive size.

3.5 Verifying and Downloading Raw Data Files

The raw data files for each event source are compressed and moved to networked storage every hour and the file hash is computed for networked storage files. The file hash is used to check the integrity of the files in the networked storage.

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *storage* link in the upper left corner of the page.
- 3 Click the *Raw Data* tab.
- 4 In the *Raw Data* section, select the desired Collector and Connector combination from the Event Source hierarchy drop-down list.
- 5 The *Event Source* field displays the list of associated event sources (hostnames or IP addresses). Select the event source from the drop-down list.

The table displays the list of local and networked storage raw data files for the selected event source.

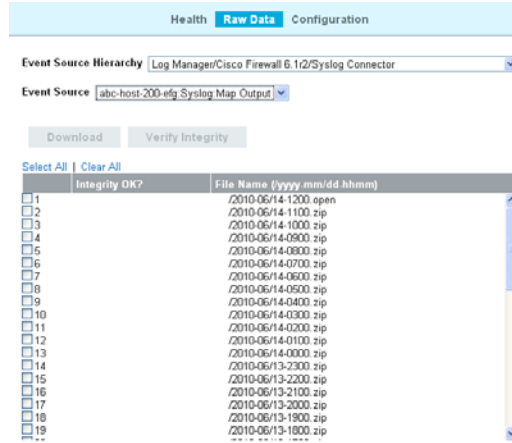
- 6 Click *Select All* to select all the files in the table.
- 7 To select a raw data file, select the check box next to the raw data file.

The *Verify Integrity* and *Download* options are only enabled when you select a file from the table.

- Click *Verify Integrity* to verify the integrity of the selected files in the networked storage by comparing the hash values for the selected files in the networked storage.

If integrity verification is successful, a green icon is displayed next to the filename in the *Integrity Ok?* column. If it fails, a red icon is displayed.

The hash is computed and updated in database only for the files in the networked storage, but not for the local raw data files. Because the raw data files are updated until they are moved to networked storage, the hash value cannot be computed or updated for these files. It is not possible to check the integrity of the local raw data files.



- Select the raw data file, then click *Download* to download the selected networked storage and local raw data files.

The selected files are downloaded in the form of a zip file that contains a .csv (comma separated values) file. If the networked storage files are selected, the zip file also contains a hash file corresponding to each of the networked storage files downloaded.

The SHA-256 algorithm is used to generate the file hash and the generated hash is Base64 encoded.

- Click *Close*.

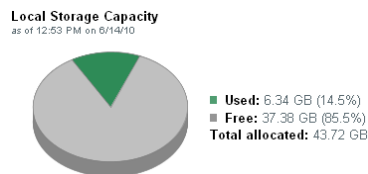
3.6 Viewing Local and Networked Storage Capacity

The Health page, available only to administrators, displays local and networked data capacity. For more information on configuring networked storage, see [Section 3.2, “Configuring Networked Storage Locations,”](#) on page 35.

To view the local storage and networked storage capacity:

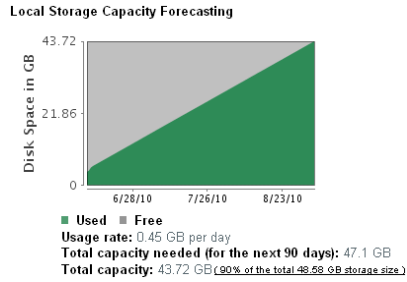
- Log in to Sentinel Log Manager as an administrator.
- Click the *storage* link in the upper left corner of the page.

The health page is displayed.



The gray color indicates the free data space and the green color indicates used data storage space.

The Health page of Sentinel Log Manager also displays forecasts about the local storage capacity.

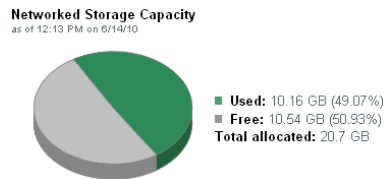


If the networked storage location is not configured, the following message is displayed on the Health page:

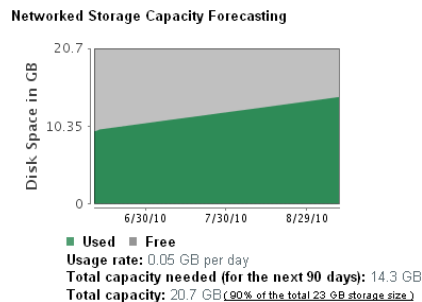
Networked Storage Status
The networked storage location has not been configured. To configure it, click [here](#)

The [Click here](#) link displays the Data Storage Location page, where you can configure the networked storage location. For more information, see “[Configuring Networked Storage Locations](#)” on page 35.

If Sentinel Log Manager is configured to show the networked storage location, the Health page displays the networked storage capacity:



The Health page of Sentinel Log Manager also forecasts the networked storage capacity.



3.7 Using Sequential-Access Storage for Long Term Data Storage

Sentinel Log Manager requires the data to be on a storage system that supports random access, such as data on your typical hard drive. It does not support interfacing with the data stored on tape directly.

You can also search the raw data directly by using tools such as `egrep` or a text editor, but this search may not be sufficient for your requirements. The search mechanism provided by Sentinel Log Manager on event data is much more powerful than these tools.

The high-level approach to configure Sentinel Log Manager is to retain data for a longer duration so you can perform searches and run reports on the data you regularly need to access, and to copy the data to tape before Sentinel Log Manager deletes it. To search or run reports on data that was copied to tape, but deleted from Sentinel Log Manager, copy the data from the tape back to Sentinel Log Manager.

This section describes how to use tape or any other storage mechanism that Sentinel Log Manager does not support.

- ♦ [Section 3.7.1, “Determining What Data You Need to Copy to Tape,” on page 49](#)
- ♦ [Section 3.7.2, “Backing Up Data,” on page 49](#)
- ♦ [Section 3.7.3, “Configuring Storage Utilization,” on page 50](#)
- ♦ [Section 3.7.4, “Configuring Data Retention,” on page 50](#)
- ♦ [Section 3.7.5, “Copying Data to Tape,” on page 50](#)
- ♦ [Section 3.7.6, “Restoring Data,” on page 51](#)

3.7.1 Determining What Data You Need to Copy to Tape

There are two types of data in Sentinel Log Manager:

- ♦ **Raw Data:** For more information on raw data, see [Section 3.1.1, “Raw Data,” on page 29](#).
- ♦ **Event Data:** For more information on event data, see [Section 3.1.2, “Event Data,” on page 34](#).

If you want to perform searches or reports on the data, copy both the raw data and the event data to tape so that you can copy both sets of data back into Sentinel Log Manager, when the data is needed. If you want to store data only to comply with legal requirements, copy only the raw data to the tape.

3.7.2 Backing Up Data

Events should be moved to networked storage regularly. The following types of data can be backed up in Sentinel Log Manager:

Configuration data: This option includes non-event or raw data backup. It is faster because it contains small amount of data, including all the installation directories except the `data` directory.

Data: This option backs up all the data in the local storage and networked storage directories. This option takes a longer time to complete.

NOTE: Networked storage directories can be located on a remote machine.

Some of the best practices that you can follow are:

- ◆ Periodically export all the Event Source Management configurations and save them. When the environment is relatively stable, you can generate a full Event Source Management export including the entire tree of the Event Source Management components. This action captures the plug-ins as well as the configuration of each node. The resulting `.zip` file should be backed up and moved to networked storage as a normal file.

If changes such as updating plug-ins or adding nodes are made to Event Source Management later, you must export the configuration and save it again.

- ◆ Back up the entire installation directory, instead of particular sections, so there is no risk of manual mistakes and the process is quicker.

For information on backing up and restoring data, see [Appendix C, “Backing Up and Restoring Data,”](#) on page 193.

3.7.3 Configuring Storage Utilization

You should configure local and networked storage space to store data before the data is deleted from the Sentinel Log Manager server. While configuring the storage space, ensure that your storage system is not 100% utilized to avoid undesirable behaviors such as data corruption. Additionally, you should also have additional space in your networked storage to copy data from tape back into Sentinel Log Manager. You do this by decreasing the archive utilization setting.

3.7.4 Configuring Data Retention

You can configure the duration for the data to remain on the disk before it is deleted. If your hard drive storage space is not sufficient to store data long enough to meet your legal requirements, you can use tape storage to store data beyond the specified duration.

You must configure data retention policies so that the data that you want to search and report is retained within the Sentinel Log Manager server until you no longer need it. Additionally, a data retention policy should ensure that Sentinel Log Manager is not prematurely deleting the data because of storage utilization limits. If the storage utilization limit is exceeded and you notice that the data is being prematurely deleted, change the data retention policy to expand the data storage space.

3.7.5 Copying Data to Tape

You can set up a process to copy raw data and event data to tape, depending on the data that you need.

The following sections describe how each type of data is stored in Sentinel Log Manager so that you can set up copy operations to copy the data out of Sentinel Log Manager onto tape.

- ◆ [“Copying Raw Data to Tape”](#) on page 51
- ◆ [“Copying Event Data to Tape”](#) on page 51

Copying Raw Data to Tape

Raw data partitions are individual files. They are created every hour, and are closed within 10 minutes after the elapsed time. When a raw data file is closed, it is renamed to identify it as a closed file. Files in the open state have a `.open` extension. When they are closed, they are renamed to have a `.log` extension. At a configured interval, after they are closed, they are compressed and stored in a `.zip` file. After the files are compressed, they are moved to networked storage from the local storage.

The directory hierarchy in which the raw data files are placed is organized by the event source and the date of the raw data. You can use this hierarchy to periodically copy a batch of raw data files to tape. For more information on raw data directory hierarchy, see [Table 3-1, “Raw Data Directory Structure,” on page 30](#).

You cannot copy files that are in the process of being compressed. You must wait until the raw data files are compressed and moved to networked storage before copying them to tape. The presence of a `.log` file with the same name as the zip file indicates that the file is still in the process of being compressed. You must also ensure that the raw data files are copied to the tape before the interval configured in the Raw Data Retention policy expires so that the data is not lost.

Copying Event Data to Tape

Event data partitions are created every 24 hours, but they are not closed for roughly 48 hours (in case some data arrives late). Event data is stored in the `data/eventdata` directory with subdirectory names prefixed with the year, month, and day when the partition was created (yyyymmdd). For example, the path to a complete event data partition, relative to the installation directory, is `data/eventdata/20090101_408E7E50-C02E-4325-B7C5-2B9FE4853476`. You can use this hierarchy to know when a partition is closed. Subdirectories whose date is at least 48 hours old should be in the closed state.

For more information on the event data directory hierarchy, see [Table 3-3, “Event Data Directory Structure,” on page 34](#).

You should wait until event data partitions have been copied to networked storage before copying them to tape. Before you copy, make sure that the directory is not currently being copied from local storage. To do this, see if there is a local storage directory partition of the same name. If the corresponding local storage directory partition is not present, the networked storage directory partition is not being copied. If the corresponding local storage directory partition is still present, make sure that all of the files in the local storage directory partition are also in the networked storage directory partition and that they are all of the same size. If they are all present and of the same size, it is highly likely that they are not currently being copied.

3.7.6 Restoring Data

The event data restoration feature of Novell Sentinel Log Manager enables you to restore old, lost, or deleted event data. You can also restore the data from other systems. You can select and restore the event partitions by using the Sentinel Log Manager user interface. You can also control when these restored event partitions expire.

NOTE: The Data Restoration feature is a licensed feature. This feature is not available with the free or trial licenses. For more information, see [Section 13.1, “Understanding the Licenses,” on page 171](#).

- ♦ [“Enabling Event Data for Restoration” on page 52](#)
- ♦ [“Viewing Event Data Available for Restoration” on page 52](#)

- ♦ [“Restoring Event Data” on page 52](#)
- ♦ [“Configuring Restored Event Data to Expire” on page 53](#)

Enabling Event Data for Restoration

To enable event data for restoration, you must copy the event directories that you want to restore to one of the following locations:

- ♦ The local storage data directory on the Sentinel Log Manager server. For example, `/var/opt/novell/sentinel_log_mgr/data/eventdata`
- ♦ The `eventdata_archive` directory of the configured networked storage directory of the Sentinel Log Manager server.

Viewing Event Data Available for Restoration

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *Storage* link in the upper left corner of the page, then select the *Configuration* tab.

The Data Restoration section does not initially display any data. It looks similar to the following graphic:



- 3 Click *Find Data* to search and display all event data partitions available for restoration.

The Data Restoration table chronologically lists all the event data that can be restored. The table displays the date of the event data, the name of event directory, and the location. The *Location* column indicates whether the event directory was found in the local data directory of Sentinel Log Manager or in the configured networked storage directory.

- 4 Continue with [“Restoring Event Data” on page 52](#) to restore the event data.

Restoring Event Data

- 1 Select the check box in the *Restore* column next to the partition that you want to restore.

Click *Select All* to select all partitions listed.

Click *Clear All* to deselect all the selected partitions.

The *Restore Data* button is enabled when the Data Restoration section is populated with the restorable data.

- 2 Click *Restore Data* to restore the selected partitions.

The selected events are moved to the *Restored Data* section. It might take approximately 30 seconds for the *Restored Data* section to reflect the restored event partitions.

- 3 (Optional) Click *Refresh* to search for more restorable data.

- 4 To configure the restored event data to expire according to data retention policy, continue with [“Configuring Restored Event Data to Expire” on page 53](#).

Configuring Restored Event Data to Expire

The restored partitions do not expire by default, according to any data retention policy checks. To enable the restored partitions to return to the normal state and also to allow them to expire according to the data retention policy, select *Set to Expire* for data that you want to expire according to the data retention policy, then click *Apply*.

The restored partitions that are set to expire are removed from the Restored Data table and returned to normal processing.

It might take about 30 seconds for the Restored Data table to reflect the changes.

4 Configuring Data Collection

Sentinel Log Manager can collect data from a wide range of event sources, such as intrusion detection systems, firewalls, operating systems, routers, databases, switches, mainframes, antivirus applications, and Novell applications. A modular architecture divides the task of protocol-level connections (Connectors) and the parsing logic (Collectors) for specific event sources.

Novell Sentinel Log Manager supports a wide variety of protocols by using the Connector plug-ins and specific event parsing by using the Collector plug-ins.

The configuration required to connect to and parse events from a new data source varies depending on the type of event source and the communication method selected.

The best source of information for configuring data collection for a specific device is the detailed documentation available with each Collector and Connector plug-in. This guide includes several basic examples of common data collection scenarios, but the documents that come with the Collector and Connector plug-ins provide much more detail about configuration options.

- ♦ [Section 4.1, “Before You Begin,” on page 55](#)
- ♦ [Section 4.2, “Configuring Data Collection for Syslog Event Sources,” on page 56](#)
- ♦ [Section 4.3, “Configuring Data Collection for the Novell Audit Server,” on page 60](#)
- ♦ [Section 4.4, “Configuring Data Collection for Other Event Sources,” on page 64](#)
- ♦ [Section 4.5, “Managing Event Sources,” on page 67](#)
- ♦ [Section 4.6, “Viewing Events Per Second Statistics,” on page 75](#)

4.1 Before You Begin

- ♦ For a list of supported Connectors and event sources packaged with this release, see “[System Requirements](#)” in the *Sentinel Log Manager 1.2.2 Installation Guide*.
- ♦ To download the new, additional and updated Collector and Connector plug-ins, and for documentation on Collectors and Connectors, see the [Sentinel Plug-ins Web site \(http://support.novell.com/products/sentinel/secure/sentinelplugins.html\)](http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
- ♦ For more information on editing Collectors that are already included in Sentinel Log Manager and about adding new Collectors, refer to the [Sentinel Plug-In SDK Web site \(http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel\)](http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

NOTE: Sentinel Log Manager 1.2 and later do not support Legacy Collectors. When you run a Legacy Collector, an error is displayed in the Status field of the Collector and the Collector does not start. You must use an equivalent JavaScript Collector, then move the Legacy Collector event source nodes to the newly added JavaScript Collector.

4.2 Configuring Data Collection for Syslog Event Sources

Events can be collected from various data sources by using the Syslog Connector. Sentinel Log Manager is preconfigured to accept syslog data from syslog event sources that send data over TCP (port 1468), UDP (port 1514), or SSL (port 1443). You can also configure Sentinel Log Manager to listen on additional ports.

To get started with syslog data collection, configure your syslog event sources to send their data to one of these ports. When Sentinel Log Manager receives data from configured event sources, it automatically chooses the most suitable Collector to parse the data, parses the data into events, and stores the event and raw data in the configured networked storage location.

The following sections describe how you can configure the event sources to send data to the Sentinel Log Manager and how you can configure new syslog ports to receive data:

- ◆ [Section 4.2.1, “Parsing Logic for Syslog Messages,” on page 56](#)
- ◆ [Section 4.2.2, “Configuring Syslog Servers,” on page 56](#)
- ◆ [Section 4.2.3, “Setting the Syslog Server Options,” on page 57](#)

4.2.1 Parsing Logic for Syslog Messages

Sentinel Log Manager can receive, store, and search against events from any syslog source. If the data source is recognized, Sentinel Log Manager automatically chooses the most suitable Collector to parse the data, parses the data into events, and stores the event and raw data in the configured networked storage location.

You can filter the collected data to drop any unwanted events. Messages from recognized data sources are parsed into fields such as `target IP address` and `source username`. Messages from unrecognized data sources are placed in a single field for storage, searching, and reporting.

The Generic Event Collector collects and processes data from unrecognized event sources that have suitable connectors. If the data was generated by a supported event source, the Generic Event Collector analyses the received data and attempts to parse the information. If the Generic Event Collector does not understand the message, it does minimal parsing and places the bulk of the text in the *Message* (Msg) field.

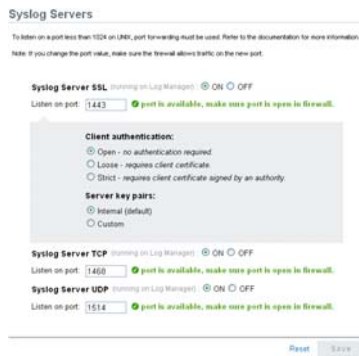
4.2.2 Configuring Syslog Servers

When you point your syslog event sources (an application or a system that logs the event) to Sentinel Log Manager, it automatically creates an event source entry to track data received from the event source. It also allows you to manage how the data is processed. An entry is created for each unique IP address or hostname that appears in the header portion of the syslog messages. This entry enables you to identify the machines generating the syslog messages, regardless of whether they are being aggregated by a syslog relay or not.

The Sentinel Log Manager Web interface allows you to configure ports to listen on to receive syslog data.

To add or remove syslog servers, use the Event Source Management interface. For more information, see [“Configuring Data Collection for Other Event Sources” on page 64](#).

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *collection* link in the upper left corner of the page.
- 3 Select the *Event Source Servers* tab.



- 4 In the *Syslog Server* section, specify the TCP, UDP, and SSL port numbers for the syslog servers. The default ports for TCP, UDP, and SSL are 1468, 1514, and 1443.
- 5 To start or stop the data collection for each of the syslog servers, select the on or off options next to them.
- 6 To change the port values, specify a valid port value. The following table shows the status messages you see after entering the valid or non-valid port values.

Status Icon	Message
Green Check Mark Icon	If the specified port is valid and is not in use, a <code>port is valid and open</code> message is displayed.
Red Cross Icon	If the specified port is not valid (non-numeric or not between 1 to 65535), a <code>port is not valid</code> message is displayed.
Red Cross Icon	If the specified port is valid but it is already in use, or if the syslog server does not have permission to use it, a <code>port is valid but not open</code> message is displayed.

- 7 Set the appropriate client authentication and server key pairs settings for the SSL syslog server. For more information on setting the client authentication, see [“Configuring Client Authentication for the SSL Syslog Server” on page 58](#). The SSL Syslog server is automatically restarted if any changes are made here.
- 8 (Optional) Click *Reset* to change the specified settings to previous settings.
- 9 Click *Save* to save the new settings. The *Save* button is disabled until a valid port is specified for all of the servers.

4.2.3 Setting the Syslog Server Options

You can configure the type of client and server authentication for syslog servers that uses SSL.

- ♦ [“Configuring Client Authentication for the SSL Syslog Server” on page 58](#)
- ♦ [“Listening on Ports Below 1024” on page 59](#)

Configuring Client Authentication for the SSL Syslog Server

The client authentication settings determine how strictly the SSL syslog server verifies the identity of syslog event sources that are attempting to send their data. You should use a strict client authentication policy that is applicable in your environment to prevent rogue syslog event sources from sending undesired data into Sentinel Log Manager.

Open: No authentication is required. Sentinel Log Manager does not request, require, or validate a certificate from the event source.

Loose: A valid X.509 certificate is required from the event source, but the certificate is not validated. It does not need to be signed by a certificate authority.

Strict: A valid X.509 certificate is required from the event source, and it must be signed by a trusted certificate authority. If the event source does not present a valid certificate, Sentinel Log Manager does not accept its event data.

- ♦ [“Creating a Trust Store” on page 58](#)
- ♦ [“Importing a Certificate into the Trust Store” on page 58](#)
- ♦ [“Server Key Pair” on page 59](#)

Creating a Trust Store

For strict authentication, you must have a trust store that contains the public certificate of the certificate authority (CA) that signed the event source certificate. After you have a DER or PEM certificate, you can create the trust store by using the TruststoreCreator utility that comes with Log Manager.

- 1 Log in to the Sentinel Log Manager server as novell.
- 2 Go to `/var/opt/novell/sentinel_log_mgr/data/updates/done`.
- 3 Use the following command to extract the `syslog_connector.zip` file:

```
unzip syslog_connector.zip
```
- 4 Copy the `TruststoreCreator.sh` or `TruststoreCreator.bat` file to the machine that has the certificates.
or
Copy the certificates to the machine with the TruststoreCreator utility.
- 5 Run the `TruststoreCreator.sh` utility as follows:

```
TruststoreCreator.sh -keystore /tmp/my.keystore -password password1 -certs /  
tmp/cert1.pem,/tmp/cert2.pem
```

In this example, the TruststoreCreator utility creates a keystore file called `my.keystore` that contains two certificates (`cert1.pem` and `cert2.pem`). It is protected by the password `password1`. The keystore file must be imported into the trust store.

Importing a Certificate into the Trust Store

For strict authentication, the administrator can import a certificate by using the *Import* button. This helps ensure that only authorized event sources are sending data to Log Manager. The trust store must include public certificate of the certificate authority (CA) that signed the event source certificate.

The following procedure must be run on the machine that has the trust store on it. You can open a Web browser on the machine with the trust store or move the trust store to any machine with a Web browser.

NOTE: If the CA is signed by another CA, then you must import the chain of CA certificates until the root CA.

To import a trust store:

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *collection* link at the upper left corner of the page.
- 3 Click the *Event Source Servers* tab.
- 4 In the Syslog Server section, select the *Strict* option under *Client authentication*.
- 5 Click *Browse* and browse to the trust store file (for example, *my.keystore*)
- 6 Specify the password for the truststore file.
- 7 Click *Import*.
- 8 (Optional) Click *Details* to see more information about the trust store.
- 9 (Optional) Click *Reset* to change to previous settings before saving
- 10 Click *Save*.

After the trust store is successfully imported, you can click *Details* to see the certificates included in the trust store.

Server Key Pair

Sentinel Log Manager is installed with a built-in certificate, which is used to authenticate the Sentinel Log Manager server to the event sources. This certificate can be overridden with a certificate signed by a public certificate authority (CA).

To replace the built-in certificate:

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *collection* link at the upper left corner of the page.
- 3 Select the *Event Source Servers* tab.
- 4 In the Syslog Server section, under *Server key pairs*, select *Custom*.
- 5 Click *Browse* and browse to the trust store file.
- 6 Specify the password for the truststore file.
- 7 Click *Import*.
- 8 (Optional) If there is more than one public-private key pair associated with the file, select the desired key pair, and click *OK*.
- 9 Click *Details* to see more information about the server key pair.
- 10 Click *Reset* to change the specified settings to previous setting before saving it
- 11 Click *Save*.

Listening on Ports Below 1024

NOTE: The instructions in this section assume that your firewall is enabled and is compatible with the `iptables` command. If this is not the case, there are probably options in your firewall configuration interface to allow you to configure the same port forwarding as described here.

Because Sentinel Log Manager runs as the `novell` user, it cannot directly listen on ports that are lower than 1024. To listen on a port that is lower than 1024, use port forwarding to forward data to a port that Sentinel Log Manager can directly listen on. Use the `/opt/novell/sentinel_log_mgr/bin/config_firewall.sh` script to setup port forwarding.

You must run the following port forwarding command as `root`:

```
iptables -t nat -A PREROUTING -p <protocol> --destination-port <incoming port> -j REDIRECT --to-ports
```

The following command is an example of how to forward events from the default syslog server port 514 to the Novell Sentinel Log Manager port 1514 for syslog UDP traffic:

```
iptables -t nat -A PREROUTING -p udp --destination-port 514 -j REDIRECT --to-ports 1514
```

4.3 Configuring Data Collection for the Novell Audit Server

Sentinel Log Manager has enhanced support for Novell Audit servers. Data collection for Novell Audit server can be configured by using a simplified Web interface. Many Novell products send data to Sentinel Log Manager by using a Platform Agent. The data is received by an event source server called the Audit Server, which is packaged with Sentinel Log Manager. The audit server is similar in many ways to a syslog server. For more information on configuring logging for Novell products, see the Novell Audit 2.0.2 documentation, which packages the platform agent.

The following sections describe the procedure to configure the audit server port to receive data and also to set the audit server options:

- [Section 4.3.1, “Specifying the Audit Server Settings,” on page 60](#)
- [Section 4.3.2, “Setting the Audit Server Options,” on page 61](#)

4.3.1 Specifying the Audit Server Settings

To specify the data collection settings for the Audit server:

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *collection* link in the upper left corner of the page.
- 3 Select the *Event Source Servers* tab.

Audit Servers

To listen on a port less than 1024 on UNIX, port forwarding must be used. Refer to the documentation for more information.

Note: If you change the port value, make sure the firewall allows traffic on the new port.

Audit Server (running on Log Manager) ON OFF

Listen on port: 1289 ✔ port is available, make sure port is open in firewall.

Client authentication:

Open - no authentication required.

Less - requires client certificate.

Strict - requires client certificate signed by an authority.

Server key pairs:

Internal (default)

Custom

If too many events are received: Write events to a maximum of 1000 files. [more...](#)

Idle Connection: Pause connection if idle for 15 minutes

Event Signatures: Request Novell Audit Event Signatures

- 4 In the *Audit Server* section, select the *On* and *Off* options to start or stop the data collection for the audit server.

- 5 In the Audit Server section, specify the port on which the Sentinel Log Manager server listens to messages from the event sources.

For more information about setting the port, see [“Port Configuration and Port Forwarding for the Audit Server” on page 61](#).

- 6 Set the appropriate client authentication and server key pairs settings.

For more information about client authentication, see [“Client Authentication for the Audit Server” on page 62](#).

The Audit server and all related Audit Connectors are automatically restarted if any changes are made here.

- 7 Select the Sentinel Log Manager server behavior when the number of events received exceeds the buffer capacity.

WARNING: If you select *Drop oldest messages*, there is no supported method for recovering dropped messages,

- 8 Select *Idle Connection* to disconnect event sources that have not sent data for a certain period of time.

The event source connections are automatically re-created when they start sending data again.

- 9 Specify the number of minutes before an idle connection is disconnected.

- 10 (Optional) Select *Event Signatures* to receive a signature with the event.

To receive a signature, the Platform Agent on the event source must be configured properly.

- 11 (Optional) Click *Reset* to change the specified settings back to the previous settings before saving

- 12 Click *Save* to save the new settings.

The *Save* button is disabled until a valid port is specified for the server.

These settings might affect data collection for several servers (for example, multiple eDirectory instances). However, they do not start or stop services on the event source machines.

Changes on this page take effect immediately.

To view the health of the Audit server and its event sources, see [Section 4.5, “Managing Event Sources,” on page 67](#).

4.3.2 Setting the Audit Server Options

Administrators can change the settings for how Sentinel Log Manager listens for data from the event source applications, set the port on which Sentinel Log Manager listens, and select the type of authentication between the event source and Sentinel Log Manager.

- ♦ [“Port Configuration and Port Forwarding for the Audit Server” on page 61](#)
- ♦ [“Client Authentication for the Audit Server” on page 62](#)

Port Configuration and Port Forwarding for the Audit Server

By default, Sentinel Log Manager listens on port 1289 for messages from the server. When the port is changed, the system checks whether the specified port is valid and open.

Binding to ports lower than 1024 requires `root` privileges, so you should use a port higher than 1024. You can change the source devices to send data to a higher port or use port forwarding on the Sentinel Log Manager server.

To change the Platform Agent to send data to a different port:

- 1 Log in to the event source machine.
- 2 Open the `logevent` file for editing. The file location depends on the operating system:
 - ♦ Linux: `/etc/logevent.conf`
 - ♦ Windows: `C:\WINDOWS\logevent.cfg`
 - ♦ NetWare: `SYS:\etc\logevent.cfg`
 - ♦ Solaris: `/etc/logevent.conf`
- 3 Set the `LogEnginePort` parameter to the desired port.
- 4 Save the file.
- 5 Restart the Platform Agent.

The method varies by operating system and application. Reboot the machine or refer to the application-specific documentation on the [Novell Documentation Web Site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) for more instructions.

To configure port forwarding on the Sentinel Log Manager server:

- 1 Log in to the Sentinel Log Manager server operating system as `root` (or `su` to `root`).
- 2 Open the `/etc/init.d/boot.local` file for editing.
- 3 Add the following command at the end of the bootup process:

```
iptables -A PREROUTING -t nat -p protocol --dport incoming port -j DNAT --to-destination IP:rerouted port
```

Replace *protocol* with `tcp` or `udp`, *incoming port* is the port with the messages are arriving, and *IP:rerouted port* with the IP address of the local machine and an available port above 1024.

- 4 Save the changes.
- 5 Reboot. If you cannot reboot immediately, run the `iptables` command in [Step 3](#) from a command line.

Client Authentication for the Audit Server

The event sources send their data over an SSL connection, and the Client authentication setting for the Sentinel Log Manager server determines what kind of authentication is performed for the certificates from the audit server on the event sources.

Open: No authentication is required. Log Manager does not request, require, or validate a certificate from the event source.

Loose: A valid X.509 certificate is required from the event source, but the certificate is not validated. It does not need to be signed by a certificate authority.

Strict: A valid X.509 certificate is required from the event source, and it must be signed by a trusted certificate authority. If the event source does not present a valid certificate, Log Manager does not accept its event data.

- ♦ [“Creating a Trust store” on page 63](#)
- ♦ [“Importing a Certificate into the Trust Store” on page 63](#)
- ♦ [“Server Key Pair” on page 64](#)

Creating a Trust store

For strict authentication, you must have a trust store that contains the public certificate of the certificate authority (CA) that signed the event source certificate. After you have a DER or PEM certificate, you can create the trust store by using the CreateTrust store utility that comes with Log Manager.

- 1 Log in to Sentinel Log Manager server as novell.
- 2 Go to `/var/opt/novell/sentinel_log_mgr/data/updates/done`.
- 3 Unzip the `audit_connector.zip` file:

```
unzip audit_connector.zip
```
- 4 Copy `TruststoreCreator.sh` or `TruststoreCreator.bat` to the machine with the certificates
or
Copy the certificates to the machine with the `TruststoreCreator` utility
- 5 Run the `TruststoreCreator.sh` utility:

```
TruststoreCreator.sh -keystore /tmp/my.keystore -password password1 -certs /tmp/cert1.pem,/tmp/cert2.pem
```

In this example, the `TruststoreCreator` utility creates a keystore file called `my.keystore` that contains two certificates (`cert1.pem` and `cert2.pem`). It is protected by the password `password1`.

Importing a Certificate into the Trust Store

For strict authentication, the administrator can import a certificate. This helps ensure that only authorized event sources are sending data to Log Manager. The trust store must include public certificate of the certificate authority (CA) that signed the event source certificate.

The following procedure must be run on the machine that has the trust store on it. You can open a Web browser on the machine with the trust store or move the trust store to any machine with a Web browser.

NOTE: If the CA is signed by another CA, then you must import the chain of CA certificates until the root CA.

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *collection* link in the upper left corner of the page.
- 3 Select the *Event Source Servers* tab.
- 4 In the Audit Server section, select the *Strict* option under *Client authentication*.
- 5 Click *Browse* and browse to the trust store file (for example, `my.keystore`)
- 6 Specify the password for the trust store file.
- 7 Click *Import*.
- 8 (Optional) Click *Details* to see more information about the trust store.
- 9 (Optional) Click *Reset* to change the specified settings back to the previous setting before saving.
- 10 Click *Save*.

After the trust store is imported successfully, you can click *Details* to see the certificates included in the trust store.

Server Key Pair

Log Manager is installed with a built-in certificate, which is used to authenticate the Sentinel Log Manager server to the event sources. This certificate can be overridden with a certificate signed by a public certificate authority (CA).

To replace the built-in certificate:

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *collection* link in the upper left corner of the page.
- 3 Select the *Event Source Servers* tab.
- 4 In the Audit Server section, under *Server key pairs*, select *Custom*.
- 5 Click *Browse* and browse to the trust store file.
- 6 Specify the password for the trust store file.
- 7 Click *Import*.
- 8 (Optional) If there is more than one public-private key pair in the file, select the desired key pair and click *OK*.
- 9 (Optional) Click *Details* to see more information about the server key pair.
- 10 (Optional) Click *Reset* to change the specified settings back to the previous setting before saving.
- 11 Click *Save*.

4.4 Configuring Data Collection for Other Event Sources

The *Advanced* tab in Sentinel Log Manager Web UI is used to launch the Event Source Management interface, which monitors and configures advanced data collection capabilities beyond the settings currently available in the web interface. Some connectors and collectors must be configured in the Event Source Management, such as the WMS connector for Windows, Database connectors, and SDEE connectors for Cisco devices.

You can perform the following tasks through the Event Source Management window:

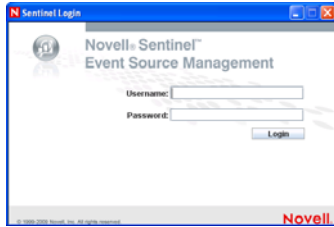
- ♦ Add or modify connections to event sources by using Configuration wizards.
- ♦ View the real-time status of the connections to event sources.
- ♦ Import or export configuration of event sources to or from the Live View.
- ♦ View and configure Connectors and Collectors that are installed.
- ♦ Import or export Connectors and Collectors from or to a centralized repository.
- ♦ Monitor data flowing through the Collectors and Connectors.
- ♦ View the raw data information.
- ♦ Design, configure, and create the components of the Event Source Hierarchy, and execute required actions by using these components.

Java 1.6.0.20 and later is required to launch the Event Source Management Web UI. If Java is not installed in your system, click the *Download Java* link to download the latest version of Java. The Java Download page opens in a new tab.

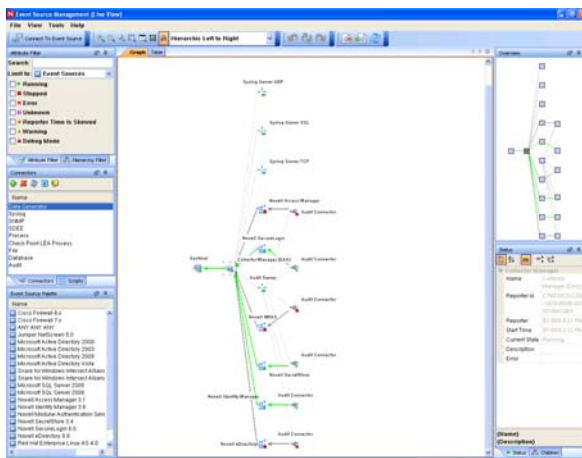
NOTE: If you are using openSUSE11.1, update your JRE to latest JRE 1.6 update. Then use the Java Web Start (`javaws`) launcher command to launch the Event Source Management.

Use the following procedure to launch the Event Source Management (Live View) window:

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *collection* link at the upper left corner of the page.
- 3 Click the *Advanced* tab.
- 4 Click the *Launch* button to launch the Event Source Management (ESM) interface.
- 5 The Novell Sentinel Event Source Management Login window is displayed.



- 6 Specify the username and password to log in to Novell Sentinel Log Manager, then click *Login*. Only users with Administrator role are allowed to log in to ESM. The Event Source Management (Live View) window is displayed.



The Event Source Management (Live View) interface provides a set of tools to manage and monitor connections between Sentinel Log Manager and the event sources that are providing data to Sentinel Log Manager. The graphical interface shows the current event sources and the software components that are processing data from that event source. Each component can be easily deployed to integrate the devices in the enterprise, and it can be monitored in real time within the ESM interface.

The following table describes the various components of the Event Source Management (Live View) interface.

Component	Description
Sentinel	The single Sentinel icon represents the main Sentinel Server that manages all events collected by the Sentinel system. The Sentinel object is installed automatically through the Sentinel installer.

Component	Description
Collector Manager	Each Collector Manager icon represents another instance of a Collector Manager process. Multiple Collector Manager processes can be installed throughout the enterprise. As each Collector Manager process connects to Sentinel, the object is automatically created in Event Source Management. For more information on installing a remote Collector Manager, see “Installing Additional Collector Managers” .
Collector	Collectors instantiate the parsing logic for data from a particular event source. Each Collector icon in Event Source Management interface refers to a deployed Collector script as well as the runtime configuration of a set of parameters for that Collector. You can download the Collectors from the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html) . For more information on customizing or creating new Collectors, refer to the Novell Developer’s Kit for Sentinel Web site (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) .
Connector	Connectors are used to provide the protocol-level communication with an event source, using industry standards such as syslog, JDBC, and so forth. Each instance of a Connector icon in Event Source Management interface represents the Connector code as well as the runtime configuration of that code. You can download the Connectors from the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html) . For more information on customizing or creating new Connectors, refer to the Novell Developer’s Kit for Sentinel Web site (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) .
Event Source Server	An event source server (ESS) is considered as part of a Connector, and is used when the data connection with an event source is inbound rather than outbound. The ESS represents the daemon or server that listens for these inbound connections. The ESS caches the received data, and one or more Connectors connects to the ESS to fetch a set of data for processing. The Connector requests only the data from its configured event source (defined in the metadata for the event source) and that matches additional filters.
Event Source	The event source represents the actual source of data for Sentinel. Unlike other components, this is not a plug-in, but is a container for metadata, including runtime configuration, about the event source. In some cases a single event source could represent many real sources of event data, if multiple devices are writing to a single file.

The changes take effect immediately for all new incoming events. However, it might take some time for events already in the queue to be processed.

For more information, refer to the Event Source Management section of the [Sentinel User Guide \(http://www.novell.com/documentation/sentinel61\)](http://www.novell.com/documentation/sentinel61).

4.5 Managing Event Sources

The event sources interface displays the health of the event source and the volume of data being received from it in events per second. The Event Sources page lists all the event sources, such as Syslog, Audit, File, and Database, that are configured in the Event Source Management interface.

You can refine the displayed event sources by selecting Collector Managers, Event Source Servers, and Collector Plug-ins. You can also specify a filter on the event source name and select particular event source health states you want to view. All of these selections and filters are stored on a per-user basis, so that each time you login to Sentinel Log Manager server you can view event sources that match your last selections. You can also perform filtering based on tags. For more information, see [Section 8.7, “Searching Tagged Events,”](#) on page 136.

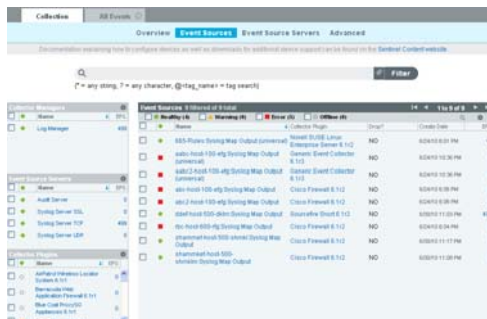
This section has the following information:

- ◆ [Section 4.5.1, “Viewing the Event Sources Page,”](#) on page 67
- ◆ [Section 4.5.2, “Filtering Event Sources,”](#) on page 72
- ◆ [Section 4.5.3, “Changing the Data Logging Status of Event Sources,”](#) on page 74
- ◆ [Section 4.5.4, “Changing the Associated Collector Plug-in for Event Sources,”](#) on page 74
- ◆ [Section 4.5.5, “Changing the Time Zone Setting for Event Sources,”](#) on page 74
- ◆ [Section 4.5.6, “Starting and Stopping Event Sources by Using the Script,”](#) on page 75

4.5.1 Viewing the Event Sources Page

The Event Sources page consists of different sections as shown in [Figure 4-1 on page 67](#).

Figure 4-1 Event Sources Page



Collector Managers: Lists all the Collector Managers associated with the Sentinel Log Manager system.

Event Source Servers: Lists all the event source servers associated with the Sentinel Log Manager system.

Collector Plug-ins: Lists all the Collector plug-ins associated with the Sentinel Log Manager system.

The Event Sources section in the right pane lists the event sources based on the options selected from the left pane.

NOTE: The Event Sources page shows event sources that were already configured or automatically detected. To manually configure additional event sources, use the Event Source Management user interface described in [“Configuring Data Collection for Other Event Sources”](#) on page 64.

This section has the following information:

- ◆ “Viewing Event Sources” on page 68
- ◆ “Viewing Collector Managers” on page 70
- ◆ “Viewing Event Source Servers” on page 70
- ◆ “Viewing Collector Plug-ins” on page 71

Viewing Event Sources

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Select *Collection > Event Sources*.

The Event Sources page is displayed.

Health	Name	Collector Plugin	Drop?	Create Date	EPS
Green	665-Rules:Syslog:Map Output (universal)	Novell SUSE Linux Enterprise Server 6.1r2	NO	6/24/10 6:01 PM	<1
Red	aabc-host-100-efg:Syslog:Map Output (universal)	Generic Event Collector 6.1r3	NO	6/24/10 10:36 PM	0
Red	aabc2-host-100-efg:Syslog:Map Output (universal)	Generic Event Collector 6.1r3	NO	6/24/10 10:36 PM	0
Red	abc-host-100-efg:Syslog:Map Output	Cisco Firewall 6.1r2	NO	6/24/10 6:06 PM	0
Red	abc2-host-100-efg:Syslog:Map Output	Cisco Firewall 6.1r2	NO	6/24/10 6:06 PM	0
Green	ddef-host-500-dklm:Syslog:Map Output	Sourcefire Snort 6.1r2	NO	6/30/10 11:03 PM	499
Red	rbc-host-600-rfg:Syslog:Map Output	Cisco Firewall 6.1r2	NO	6/24/10 6:04 PM	0
Green	shammef-host-500-shmkl:Syslog:Map Output	Cisco Firewall 6.1r2	NO	6/30/10 11:17 PM	0
Green	sharmkef-host-500-shmklm:Syslog:Map Output	Cisco Firewall 6.1r2	NO	6/30/10 11:08 PM	0

The following table explains each column of the event source section:

Columns	Description
Health Icon	<p>The colored icon indicates the event source health.</p> <p>Green: Indicates that the event source is healthy and Sentinel Log Manager has received data from it.</p> <p>Red: Indicates that the Sentinel Log Manager server is reporting an error about connecting to or receiving data from this event source.</p> <p>Gray: Indicates that the event source is turned off. Sentinel Log Manager is not processing any data from it.</p> <p>Orange: Indicates that the event source is running with some warnings.</p> <p>You can sort the event sources based on their health status.</p>
Name	<p>The event source name is the name given to the event source by the system (if it was auto-created) or by a user. For syslog event sources, if the event source was auto-created by the system, the name is a combination of the hostname/IP address and the Collector connection mode the event source is using.</p> <p>You can rename any event source at any time through the Event Source management interface.</p> <p>You can sort the event sources in alphabetical order based on their names.</p>

Columns	Description
Collector Plugin	<p>Specifies the name of the Collector plug-in that the event source is connected to.</p> <p>NOTE: This is the name of the Collector plug-in, not the name of the Collector instance.</p> <p>You can sort the event sources based on Collector plug-in name.</p>
Drop	<p>Specifies whether data from the associated event source should be dropped or not.</p> <p>YES: If <i>Drop Data</i> is set to YES, all data received from the event source is dropped. This means that the raw data is not saved and events are not generated.</p> <p>NO: If <i>Drop Data</i> is set to NO, all raw data from the event source is saved and events are generated. When it is set to NO, raw data is always saved, regardless of whether a filter is set on the event source using the Event Source Management user interface. However, if a filter is set, events might not be generated if the filter causes the data to be ignored.</p> <p>You can sort the event sources based on the drop data status.</p>
Create Date	<p>Specifies the date and time when the event source was created.</p> <p>You can sort the event sources based on when they were created.</p>
EPS	<p>Specifies the events per second value received from the event source. You can sort the event sources based on their events per second value.</p> <p>NOTE: If you see a value of less than one (<1) in this column, it indicates that the EPS rate is greater than zero, but less than one.</p>

- To select or deselect the event sources, select the check boxes next to the respective event source. To select all the available event sources, select the check box at the top of the column.
- To sort the event sources by *Health*, *Name*, *Collector Plugin*, *Drop Data*, *Create Date*, and *EPS* values, click the respective column header. The selected column header is displayed in bold. When you first click the column header, the event sources are arranged in the ascending order. A blue down-arrow is displayed to indicate that the sort order is ascending. When you click the column header for the second time, the sort order is changed to descending, and a blue up-arrow is displayed to indicate that the sort order is descending.
- To view additional information about an event source, click the *Name* or *EPS* value of an event source. A dialog box is displayed with the additional information.

Collector Plugin:	Generic Event Collector 6.1r3
Description:	This Collector parses data from Generic Event Collector; see documentation for supported subproducts and connection modes.
Version:	6.1r3
Release Date:	8/6/09 2:26 PM
Scripting Language:	javascript
Matching Rule:	None
Applications:	None
Universal:	YES
Event Sources:	2
Events Per Second:	0
Health:	Error
Event Sources Healthy:	0
Event Sources With Warning:	0
Event Sources With Error:	2

Viewing Collector Managers

- 1 Log in to Sentinel Log Manager as administrator.
- 2 Select *Collection > Event Sources*.

The Collector Manager section is displayed in the Event Sources page with the following details:



Health	Name	EPS
<input type="checkbox"/>	Log Manager	0

Health: Indicates the health of the Collector Managers. You can sort the Collector Managers based on their health status.

Name: Displays the name of the Collector Managers. You can sort the Collector Managers in alphabetical order based on their names.

EPS: Displays the events per second value received from the event sources. You can sort the Collector Manager based on the events per second value.

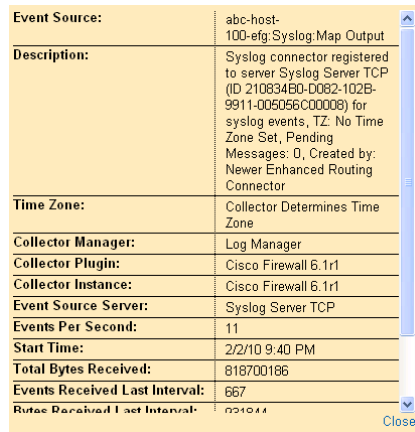
- 3 To select or deselect the Collector Managers, select the check boxes next to the respective Collector Manager.

To select all the available Collector Managers, select the check box located at the top of the column.

The right pane displays the list of event sources connected to the selected Collector Managers.

If none of the Collector Managers are selected, the event sources table displays all the configured event sources.

- 4 To sort the Collector Managers by *Health*, *Name*, and *EPS* values, click the respective column header. When you click the column header the respective column header displays in bold text.
- 5 To get additional information about the Collector Managers, click the *Name* or *EPS* value column, a dialog box is displayed with the additional information.



Event Source:	abc-host-100-efg:Syslog:Map Output
Description:	Syslog connector registered to server Syslog Server TCP (ID 210834E0-D082-102B-9911-005056C00008) for syslog events, TZ: No Time Zone Set, Pending Messages: 0, Created by: Newer Enhanced Routing Connector
Time Zone:	Collector Determines Time Zone
Collector Manager:	Log Manager
Collector Plugin:	Cisco Firewall 6.1r1
Collector Instance:	Cisco Firewall 6.1r1
Event Source Server:	Syslog Server TCP
Events Per Second:	11
Start Time:	2/2/10 9:40 PM
Total Bytes Received:	818700196
Events Received Last Interval:	667
Bytes Received Last Interval:	6210.44

Viewing Event Source Servers

- 1 Log in to the Sentinel Log Manager server as administrator.
- 2 Select *collection > Event Sources*.

The Event Source Servers section is displayed as follows:

Health	Name	EPS
	Audit Server	0
	Syslog Server SSL	0
	Syslog Server TCP	0
	Syslog Server UDP	0

Health: Indicates the health of the event source server. You can sort the event source servers based on their health status.

Name: Displays the names of the event source server used to parse the data from the event sources (for example, syslog Server SSL). You can sort the event source server in alphabetical order based on their names.

EPS: Displays the events per second value received from the event sources. You can sort the event source servers based on the events per second value.

- To sort the event source servers by *Health*, *Name*, and *EPS* values, click the respective column header. The selected column header displays in bold text.
- To view additional details, click the *Name* or *EPS* value column. A dialog box is displayed with the additional information.

Event Source Server:	Audit Server
Description:	Server is listening for Novell Audit messages on port 1,289 and can buffer 20,000 messages.
Collector Manager:	Log Manager
Event Sources:	0
Port:	1289
Events Per Second:	0
Start Time:	1/18/10 6:41 PM
Total Bytes Received:	0
Bytes Received Last Interval:	0
Interval:	1 minute, 358 milliseconds
Last Time Bytes Received:	No Time
Health:	Healthy

[Close](#)

Viewing Collector Plug-ins

- Log in to the Sentinel Log Manager server as administrator.
- Select *collection > Event Sources*.

Health	Name	EPS
	Cisco Firewall 6.1r1	0
	Cisco Switch 6.1r1	0
	Cisco VPN 3000 6.1r1	0
	Enterasys Dragon 6.1r1	0
	Extreme Networks Summit Series 6.1r1	0
	Generic Event Collector 6.1r2	0
	HP HP-LUX 6.1r1	0
	IBM AIX 6.1r1	0

Health: Indicates the aggregate health of all event sources that are connected to the Collector plug-in.

With the exception of the green icon (healthy state), the icon does not necessarily mean that all event sources connected to the Collector plug-in are in state indicated by the icon.

The red icon (error state) indicates that one or more event sources connected to the Collector plug-in are in an error state. To get a detailed information, click the *Name* or *EPS* column value to view help information.

Name: Displays the names of the Collector plug-in used to parse the data from the event sources (for example, Cisco Firewall 6.1r1). You can sort the Collector plug-ins in alphabetical order based on their names. This lists all the configured Collector plug-ins and not the Collector instances.

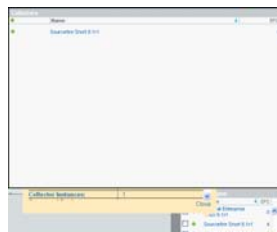
EPS: Displays the events per second value received from the event sources. You can sort the Collector based on the events per second value.

- 3 To select or deselect the Collector plug-ins, select the check boxes next to the respective Collector plug-in.

To select all the available Collector plug-ins, select the check box at the top of the column.

- 4 To sort the Collector plug-ins by *Name* or *EPS* values, click the appropriate column header. When you click the column header the respective column header displays in bold text.

The *Collector Instances* field displays the number of instances of the Collector plug-in. Clicking on the *Collector Instances* field displays a *Collectors* window with a list of Collector instances associated with the Collector plug-in.



- 5 When you click the *Collector Plugin* column, a dialog box is displayed with additional information about the Collector plug-in.

Collector Manager:	Log Manager
Start Time:	2/2/10 6:25 PM
Event Sources:	32
Events Per Second:	152
Health:	Healthy
Close	

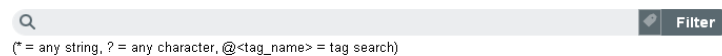
4.5.2 Filtering Event Sources

- 1 Log in to the Sentinel Log Manager server as an administrator.
- 2 Select *Collection > Event Sources*.
- 3 To filter the event sources by name, type a name value in the filter text box, then click *Filter*.

Matching is case insensitive. The name value can contain wildcard characters. Use *** to match zero or more characters and use *?* to match one character. If no wildcard characters are specified in the name value, it is assumed that the name value is intended to mean *contains <name value>*, or **<name value>**.


For example, an event source value of *abc* is interpreted as **abc**. Some examples of common filter types are:

- ♦ If the event source name starts with *abc*, enter the filter value as *abc**.
- ♦ If the event source name ends with *abc* enter the filter value as **abc*.
- ♦ If the event source name contains *abc* enter the filter value as *abc* or **abc**.



The event source table displays the list of event sources whose name matches the value entered in the filter input box.

- 4 To filter event sources based on tags, do one of the following:

- ◆ Click , then select the tags from the dialog box, based on which to search the events.
- ◆ Specify the following search criteria:

@<tag_name>

For example, @HIPAA displays all events tagged with HIPPA tag.

- 5 To view the event sources based on the health status, select the *Healthy*, *Warning*, *Error*, or *Offline* check boxes.



The Event source table displays the list of event sources with the selected health states.

If none of the health states are selected, health state filtering is not performed. It is essentially equivalent to selecting all four health states.

- 6 In the Event Source section, click the *Next*, *Previous*, *First*, and *Last* arrow links to scroll through all the event sources.

The Event Source section displays 30 event sources per page.

- 7 To view the event search result for an event source, select the event source from the list and click the *Search* icon.

A search is performed using the universally unique identifier (UUID) of the event source (for example, rv24 : "2CBFB8A0-F24B-102C-A498-000C").

If multiple event sources are selected for search, the rv24 : <UUID> expressions are combined with the OR operator in the search filter expression.

- 8 To display the event sources connected to particular Collector Managers, select one or more Collector Managers from the Collector Managers section.

If none of the Collector Managers are selected, event sources refinement is not performed based on the Collector Managers. This is not the same as selecting all Collector Managers, because it also includes event sources that are not connected to any Collector Manager.

To select or deselect the event source servers, select the check boxes next to the respective event source server.

- 9 To display only event sources connected to particular event source servers, select one or more event source servers from the Event Source Servers section.

If none of the event source servers are selected, event sources refinement is not performed based on the event source servers. This is not the same as selecting all event source servers, because it also includes event sources that are not connected to any event source server.

To select or deselect the event source servers, select the check boxes next to the respective event source server.

- 10 To display only those event sources connected to particular Collector plug-ins, select one or more Collector plug-ins from the *Collectors Plugins* section.

If none of the Collector plug-ins are selected, event sources refinement is not performed based on the Collector plug-in. It is essentially equivalent to selecting all of the Collector plug-ins.

4.5.3 Changing the Data Logging Status of Event Sources

- 1 Log in to Sentinel Log Manager as administrator.
- 2 Select *collection > Event Sources*.
- 3 To change the data logging status for one or more event sources, select the event sources from the list.
- 4 Click *Configure*, then select either *Drop Data* or *Allow Data* option,

Drop Data: If *Drop Data* is selected, the selected event sources drop all the events received. Messages are not sent to the Collectors the selected event sources are connected to.

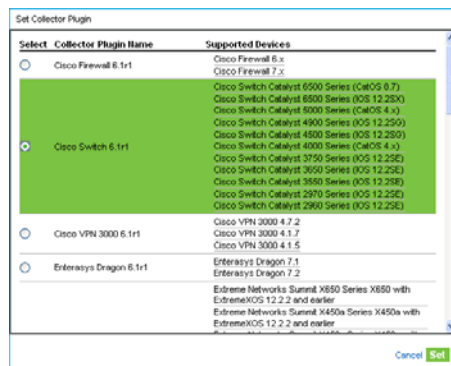
Allow Data: If *Allow Data* is selected, the selected event sources forward events received to the Collectors they are connected to.

NOTE: If you select a large number of event sources to change, it may take a while to complete. The event sources list does not show the Drop state (*YES* or *NO*) until after the changes are complete, and the display is refreshed from the database.

4.5.4 Changing the Associated Collector Plug-in for Event Sources

- 1 Log in to Sentinel Log Manager as an Administrator.
- 2 Select *collection > Event Sources*.
- 3 Select the event sources from the list, then click *Configure*.
- 4 Select the *Collector Plugin* option.

The Set Collector Plugin window is displayed with the *Collector Plugin Name* and *Supported Devices* information.



- 5 Select a new Collector plug-in, then click *Set*.

The event sources are connected to the selected Collector plug-in.

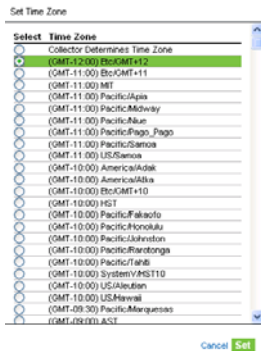
NOTE: If you select a large number of event sources to change, it may take a while to complete. The event sources list does not show the new Collector plug-in until after the changes are complete, and the display is refreshed from the database.

4.5.5 Changing the Time Zone Setting for Event Sources

- 1 Log in to the Sentinel Log Manager server as Administrator.
- 2 Select *collection > Event Sources*.

- 3 To change the time zone setting for one or more event sources, select the event sources from the list, click the *Configure* link, and select the *Time Zone* option.

The *Set Time Zone* window is displayed.



- 4 Select a new time zone, then click *Set*.

The selected event sources are set to the new time zone setting.

NOTE: If you select a large number of event sources to change, it may take a while to complete. The event sources list does not show the new time zone until after the changes are complete, and the display is refreshed from the database.

4.5.6 Starting and Stopping Event Sources by Using the Script

You can start or stop event sources by using the `./esm_manager.sh` script in the console.

- 1 Log in to the console as the `novell` user.
- 2 Change to the `/opt/novell/sentinel_log_mgr/bin` directory.
- 3 (Conditional) To start an event source, specify the command as follows:

```
./esm_manager.sh <event_source_ID> start
```

- 4 (Conditional) To stop an event source, specify the command as follows:

```
./esm_manager.sh <event_source_ID> stop
```

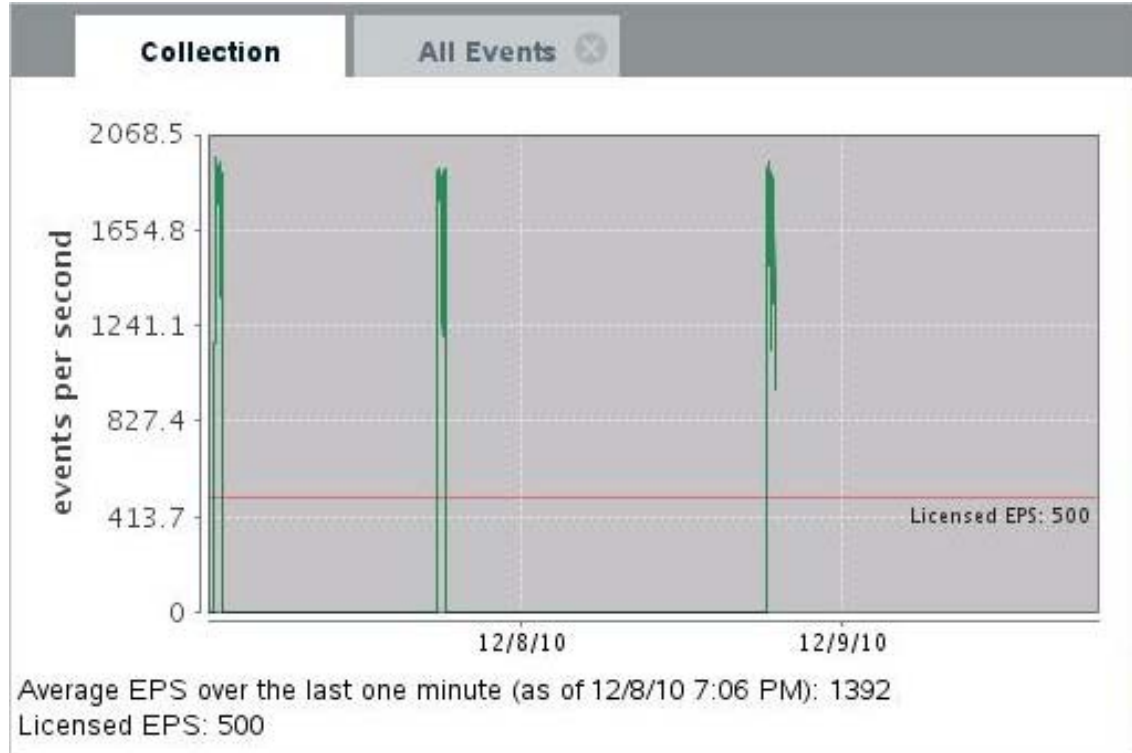
4.6 Viewing Events Per Second Statistics

- ♦ [Section 4.6.1, “Viewing Graphical Representation of Events Per Second Value,”](#) on page 75
- ♦ [Section 4.6.2, “Viewing Events Per Second Value of Event Source Servers,”](#) on page 76

4.6.1 Viewing Graphical Representation of Events Per Second Value

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *collection* link in the upper left corner of the page.
- 3 In the *Overview* section, you can view the events per second (eps) value of the incoming events in the last one minute.

The graph shows the last 90 day statistics of all the events coming to the Sentinel Log Manager server. The graph also includes a EPS indicator that enables you to determine whether the current EPS rate is exceeding the licensed EPS rate or is close to the licensed EPS rate.



4.6.2 Viewing Events Per Second Value of Event Source Servers

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click the *collection* link in the upper left corner of the page.
- 3 Click the *Event Sources* tab.
The Event Sources page is displayed.
- 4 The *EPS* column of the *Event Source Servers* section specifies the events per second value received from all the event source servers.

5 Searching Events

Sentinel Log Manager provides you with an option to perform a search on events. Each time you perform a search for an event, a page opens with the search results. You can refine your search results again.

Searches in Sentinel Log Manager automatically search both local data and data that is compressed and stored in a configured network storage location. With the necessary configuration, users can also search system events generated by Sentinel Log Manager, view the raw data for each event, or perform distributed searches across multiple Sentinel Log Manager servers. By default, events are returned in a reverse chronological order. This sort order relates to how the events are stored in the file system partitions.

You can refine search results, view search results, export search results, save search queries as report templates, and send search results to a configured action.

You can also search Sentinel Log Manager servers which are distributed across different geographic location. For more information, see [Chapter 7, “Searching and Reporting Events in a Distributed Environment,”](#) on page 109.

- ♦ [Section 5.1, “Running an Event Search,”](#) on page 77
- ♦ [Section 5.2, “Viewing Search Results,”](#) on page 80
- ♦ [Section 5.3, “Refining Search Results,”](#) on page 83
- ♦ [Section 5.4, “Searching for Events with Empty or Non-Empty Fields,”](#) on page 86
- ♦ [Section 5.5, “Exporting Search Results,”](#) on page 86
- ♦ [Section 5.6, “Saving a Search Query,”](#) on page 87
- ♦ [Section 5.7, “Sending Search Results to an Action,”](#) on page 91
- ♦ [Section 5.8, “Configuring the Search Limit,”](#) on page 92

5.1 Running an Event Search

Users can run simple or advanced searches. Basic event information includes event name, source, time, severity, information about the initiator (represented by an arrow icon), and information about the target (represented by a bull’s-eye icon)

- ♦ [Section 5.1.1, “Running a Basic Search,”](#) on page 78
- ♦ [Section 5.1.2, “Running an Advanced Search,”](#) on page 78
- ♦ [Section 5.1.3, “Search Expression History,”](#) on page 79

5.1.1 Running a Basic Search

By default, the search results include all events generated by the Sentinel system operations. These events are tagged with the `sentinel` tag. If no query is specified and you click *Search* for the first time after the Sentinel installation, the default search returns all events with severity 3 to 5. Otherwise, the Search feature reuses the last specified search query.

To search for a value in a specific field, use the ID of the event name, a colon, and the value. For example, to search for an authentication attempt to Sentinel by user2, use the following text in the search field:

```
evt>LoginUser AND sun:user2
```

An advanced search can narrow the search for a value to a specific event field. The advanced search criteria are based on the event IDs for each event field and the search logic for the index. Advanced searches can include the product name, severity, source IP, and the event type. For example:

- ◆ `pn:NMAS AND sev:5`

This searches for events with the product name NMAS and severity five.

- ◆ `sip:10.0.0.01 AND evt:"Set Password"`

This searches for the initiator IP address 10.0.0.1 and a "Set Password" event.

Multiple advanced search criteria can be combined by using various operators. The advanced search criteria syntax is modeled on the search criteria for the Apache Lucene open source package. For more information on building search criteria, see [Appendix A, "Search Query Syntax," on page 181](#).

To run a basic text search:

5.1.2 Running an Advanced Search

An advanced search can narrow the search for a value to a specific event field. The advanced search criteria are based on the short names for each event field and the search logic for the index. For more information on the field names, their descriptions, the short names that are used in advanced searches, and for information on the fields are visible in the basic and detailed event views, see [Table E-1, "Event Fields," on page 199](#). For more information on the search procedure, see [Section 5.1.1, "Running a Basic Search," on page 78](#).

NOTE: For more information on the tag names, click the *search tips* link.

To search for a value in a specific field, use the short name of the field, a colon, and the value. For example, to search for an authentication attempt to Sentinel Log Manager by user2, use the following text in the search field:

```
evt:<eventmane> AND sun:user2
```

Other advanced searches could include the product name, severity, source IP, and the event type. For example:

- ◆ `pn:NMAS AND sev:5` (This search is for events with the product name NMAS and severity five.)
- ◆ `sip:123.45.67.89 AND evt:"Set Password"` (This search is for the initiator IP of 123.45.67.89 and an event of 'Set Password'.)

Multiple advanced search criteria can be combined by using the following operators:

- ◆ AND (must be capitalized)

- ◆ OR (must be capitalized)
- ◆ NOT (must be capitalized and cannot be used as the only search criterion)
- ◆ +
- ◆ -

The following special characters must be escaped by using a \ symbol:

+ - && | | ! () { } [] ^ " ~ * ? : \

The advanced search criteria syntax is modeled on the search criteria for the Apache Lucene open source package. For more information on the search criteria, see [Lucene Query Parser Syntax \(http://lucene.apache.org/java/2_3_2/queryparsersyntax.html\)](http://lucene.apache.org/java/2_3_2/queryparsersyntax.html).

To run an advanced search:

- 1 Log in to Sentinel Log Manager.
- 2 Click *New Search*.

A new tab is displayed.

- 3 To search based on tags, you can do one of the following:

- ◆ Click the tags widget , and select the tags from the pop-up, based on which you want to search the events.
- ◆ Specify the following query:

@<tagname>

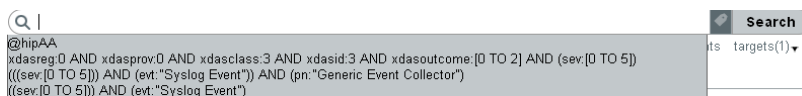
For example, @SentinelLogManager lists all the system events.

- 4 Click *Search*.
- 5 If distributed search is configured, click *targets* to select the server in a distributed environment, from which to search for events. For more information on Distributed Search, see [Chapter 7, "Searching and Reporting Events in a Distributed Environment,"](#) on page 109.

5.1.3 Search Expression History

Sentinel Log Manager allows you to select a search expression from the search history list. The search history displays a maximum of 15 search expressions. When you enter a value in *Search* you can select one of the recently used searches and run it with the selected time parameters

Figure 5-1 Search Expression History List



- ◆ When you enter a text value in *Search*, the closely matched search expressions appear in the recently used search expression list.
- ◆ When the text is not entered in *Search*, the search history displays all the recently used search expressions. The most recent search expression appears at the top of the list.
- ◆ For each user, a maximum of 250 search expressions is stored. If the number of search expressions exceeds 250, the oldest expressions are deleted from the list.

5.2 Viewing Search Results

Searches return a set of events. You can view the search results in the basic view or in the advanced view.

When results are sorted by relevance, only the top 50,000 events can be viewed. When they are sorted by time, all the events in the system are displayed.

- ◆ [Section 5.2.1, “Basic Event View,”](#) on page 80
- ◆ [Section 5.2.2, “Event View with Details,”](#) on page 80

5.2.1 Basic Event View

The information in each event is grouped into General Event information, Initiator information, Target information, Observer Information, Reporter information, and Customer values and retention policy information.

To view the raw data information:

- 1 Launch the Event Source Management (Live View) window.
- 2 Select the *Open Raw Data Tap* option to display the *Raw Data* window.

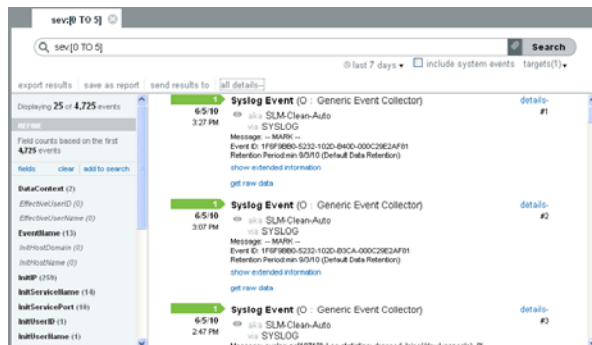
You can view the detailed information in the *Raw Data Details* section.

NOTE: You must have the necessary permissions to view all data. For more information, see [Section 10.1.3, “Setting Permissions,”](#) on page 153.

Occasionally, the search engine might index events faster than they are inserted into the data directory. If you run a search that returns events that were not added the data directory, you get a message indicating that some events match the search query, but they are not found in the data directory. If you run the search again later, the events are added to the data directory and the search is shown as successful.

5.2.2 Event View with Details

- 1 To view details about all events, click the *all details* link at the top of the search results page. You can expand or collapse the details for all events on a page by using the *all details++* or *all details--* link.



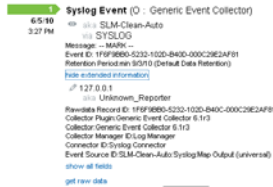
- 2 To view details such as the Message, Event ID, and default data retention duration information for any individual event, click the *details+* link next to the event.

You can expand or collapse the information for the events by clicking the *details+* or *details-* link.



3 Click the *show extended info* link to view additional details of the events.

You can expand or collapse this information by using the *show extended information* or *hide extended information* links.



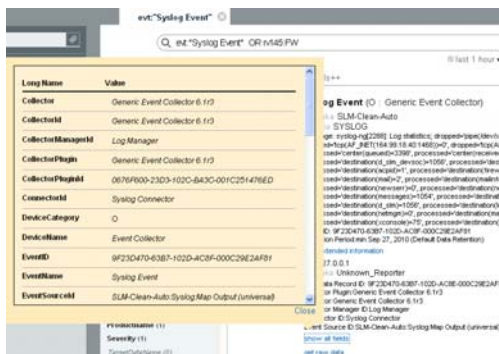
The detailed view displays information such as the Source IP address, Rawdata Record ID, Collector Script, Collector name, Collector Manager ID, Connector ID, and Event Source ID information for the incoming events.

- ◆ **Rawdata Record ID:** Displays the raw data record ID and provides information about the raw data record that initiated the event.
- ◆ **Collector Plugin:** Displays the name of the collector plug-in script.
- ◆ **Collector:** Displays the name of the collector.
- ◆ **Collector Manager ID:** Displays the name of the Collector Manager.
- ◆ **Connector ID:** Displays the name of the Connector.
- ◆ **Event Source ID:** Displays the name of the Collector Manager.

If the Collector, Collector Manager, Connector, and EventSource plug-in instances are deleted, the IDs are displayed instead of the names.

4 Click the *show all fields* link to view information about all associated fields for the particular event.

The list shows only the event fields that have values.



5 (Optional) Click the *get raw data* link to open a new *Raw Data* tab with event source hierarchy and event source fields populated, based on the information received from the event.



NOTE: You must have the necessary permissions to perform this step. For more information, see [Section 10.1.3, “Setting Permissions,”](#) on page 153.

If the search result is a system or an internal event, the *get raw data* link does not appear.

To verify and download the raw data files, see [Section 3.5, “Verifying and Downloading Raw Data Files,”](#) on page 46.

Events View in Free Versions of Sentinel Log Manager

On systems running with the free license, events that are received while the system averages more than 25 EPS are tagged with the `OverEPSLimit` tag. These events are displayed as `Over EPS Limit` in the search results, and the details of such events are not accessible until you upgrade the system with the enterprise license.

The following image shows a sample search result that includes the `OverEPSLimit` tagged events:

Figure 5-2 Search Results with Tagged Events

The screenshot displays a search results page for "All Events". The interface includes a search bar at the top with a magnifying glass icon and a "Search" button. Below the search bar, there are filters for "whenever" and "include system events", and a "targets(1)" dropdown. The main content area shows a list of events, each with a colored arrow icon indicating its severity or type. The events listed are:

- Juniper Netscreen Series Event** (Green arrow): 3/23/11 5:29 AM. Message: inetd[161]: [ID 317013 daemon.notice] telnet[412] from INSIDE_ADDR1 32781.
- Juniper Netscreen Series Event** (Green arrow): 3/23/11 5:29 AM. Message: inetd[161]: [ID 317013 daemon.notice] telnet[412] from INSIDE_ADDR1 32781.
- Monitoring on interface normal** (Blue arrow): 3/23/11 5:29 AM. PEER >> QUERY | XDAS_AE_QUERY_ASSOC_CONTEXT >> XDAS_OUT_SUCCESS. Message: (Secondary) Monitoring on interface 2 normal.
- Juniper Netscreen Series Event** (Green arrow): 3/23/11 5:29 AM. Message: ftpd[482]: [ID 511507 daemon.debug] FTPD: command: STOR syslog.unx.
- Over EPS Limit** (Red arrow with lock icon): Your license has expired. Please upgrade your licenses to see the full details of this event.
- Over EPS Limit** (Red arrow with lock icon): Your license has expired. Please upgrade your licenses to see the full details of this event.
- Over EPS Limit** (Red arrow with lock icon): Your license has expired. Please upgrade your licenses to see the full details of this event.
- Deny protocol by Access Group** (Yellow arrow): 3/23/11 5:29 AM. PEER >> SEND FAILURE | XDAS_AE_SEND_DATA_VIA_ASSOC >> XDAS_OUT_DENIAL. ASA 445.

On the left side, there is a "REFINE" pane with a search bar and a list of event fields with their counts in parentheses: DataContext (0), EffectiveUserID (0), EffectiveUserName (0), EventName (0), InitHostDomain (0), InitHostName (0), InitIP (0), InitServiceName (0), InitServicePort (0), InitUserID (0), InitUserName (0), and ProductName (0).

After you upgrade the system with the enterprise license, the full details of all the tagged events are available when you perform the search again. You can use the `OverEpsLimit` tag to specifically search for any such tagged events by adding `rv145:OverEpsLimit` to the search criteria.

5.3 Refining Search Results

The search refinement pane to the left of the search results can be used to narrow the search results by selecting one or more values for an event field. Users can refine the results for one or more event fields.

The set of event fields that is displayed in the search refinement pane is configurable on a per-user basis.

For more information on each of these event fields, see [Appendix E, "Event Fields," on page 199](#).

For performance considerations, the maximum sample size used to calculate the event field value statistics is 50,000 events. The actual sample size is displayed in the field count label as:

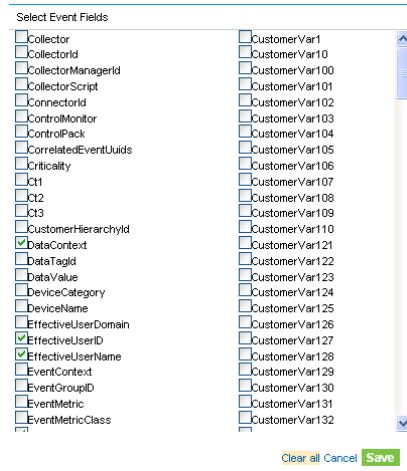
Field counts based on the first `<sample-size>` events, where `<sample-size>` is replaced by the actual sampling size.

To refine search results:

- 1 Log in to Novell Sentinel Log Manager.
- 2 Run an event search.

For more information on how to run an event search, see “Running an Event Search” on page 77.

- 3 Click *fields* in the REFINE section. The Select Event Fields window is displayed.



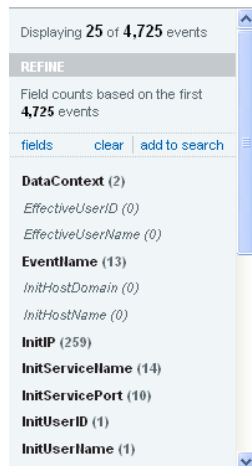
- 4 To refine the search, select the event fields from the available fields, and click *Save*.

To deselect all the selected event fields, click the *Clear all* link.

To undo any changes, and click *Cancel*.

The selected event fields are displayed in the *REFINE* pane.

A count at the right side of each event field displays the number of unique values that exist for that field in the data directory. The calculation is based on the first 50,000 events found.



The event field selection is on a per-user basis. Each user can have a different set of selected event fields.

- 5 Click each event field to view the unique values for that event field.



For example, if the search results contain events that had severities 1, 2, 5, and 4, the event field is displayed as *Severity (4)*.

The top 10 unique values are initially displayed in the order of most frequent to least frequent.

The value next to the check box represents the unique value for that event field and the value at the far right represents the number of times the value appears in the search result.

If there are multiple unique values occurring the same number of times in a search, the values are ordered by the most recent occurrence of the value.

For example, if events of severity 1 and 4 occurred 34 times in the search results, and an event of severity 4 was logged most recently, the unique value 4 appears at the top of the list.

To display the unique values in the order of least frequent to most frequent, click *reverse*.

When there are more than 10 unique values, you can view and filter either the top 10 or the bottom 10 unique values. You are not allowed to refine your search on both the conditions at the same time.

In following scenarios, the number of events returned from a refinement are greater than the number of values listed for an event field:

- ◆ If the refinement performs a new search with additional terms intersected with the initial search string, such as by using an AND operator, the new search is run against all events in the system, including the result set from the initial search. If new events that came into the system match the refined search, they are shown in the resulting set and the event count is greater than the field value count.
- ◆ If there are more than 50,000 events, the event field statistics is calculated only on the first 50,000 events.

There could be an event field value that occurs 50 times in the first 50,000 events, but it could occur 1,000 times in all other stored events. In this scenario, the displayed value count is 50, but when the search is refined with this value it returns 1,000 events.

6 To apply the selected unique values in the search refinement term pop-up, then click *OK*.

Selected event field values are listed under the event field in the *REFINE* pane.

The right pane displays the refined search results, which contain only the selected values.



7 Repeat [Step 3](#) through [Step 6](#) to further refine the search.

8 (Optional) Click *clear* to clear the selected unique event field values from the *REFINE* pane and to return to the original search results.

9 (Optional) Click *add to search* to add the refined search values to the current search tab and to recalculate the search statistics.

If you have already added the event field value to the current search tab, clicking *clear* does not return to the previous search results.

5.4 Searching for Events with Empty or Non-Empty Fields

Sentinel Log Manager allows you to search for events that have empty fields as well as fields with any value.

- [Section 5.4.1, “Searching for Events with a Non-Empty Field,” on page 86](#)
- [Section 5.4.2, “Searching For Empty Fields,” on page 86](#)

5.4.1 Searching for Events with a Non-Empty Field

In Sentinel Log Manager, you cannot use wildcards to search for all events with a particular field and any value. Wildcards do not work in Lucene because it does not allow the * or ? characters to be the first character of a search value.

For example, if you want to find all events whose `sn` field has a value and it is not empty, the search would fail if the query is `sn: *`

Instead, you must use the `notnull` field that has been added and associated with every event. The `notnull` field contains a list of fields in the event that have a non-empty value. You can use this field to find events with non-empty values.

For example, to query for events where the `sn` field is not empty, run the following query:

```
notnull:sn
```

5.4.2 Searching For Empty Fields

To find all events whose `sn` field is empty, run the following query:

```
sev:[0 TO 5] NOT notnull:sn
```

This query includes all events whose `sev` field contains a value between 0 and 5, but excludes events that have `sn` in the `notnull` field. This effectively leaves only events whose `notnull` field does not have `sn` in it, that is events whose `sn` field is empty.

In Lucene search syntax, NOT terms must be combined with one or more non-NOT terms. In the example discussed above, this is accomplished by combining the `sev:[0 TO 5]` term. The NOT terms are applied to all the events found by the non-NOT terms.

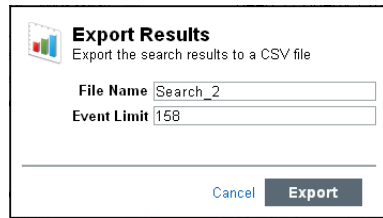
5.5 Exporting Search Results

You can use the *Export Results* link to export your search results as a .zip file.

The *export results* link is displayed at the top of the search result after performing a search.

- 1 Log in to Sentinel Log Manager.
- 2 Perform a search.
- 3 To export the search result, click the *export results* link.

An Export Results window is displayed.



4 Specify the following information:

File Name: Specify a filename to which you want to export the search results.

Event Limit: Specify the maximum number of events to be saved. The default value for the event limit is the number of search results displayed.

All the search results are written into a `.csv` file. These files are then compressed into a `.zip` for download.

5 Click *Export* to export the search result to a file.

A download file dialog box is displayed with an option to save the `Search_xevents.zip` file on your local machine.

To maintain the consistency between the total search results in the Sentinel Log Manager user interface and the exported events, it is important that the time of the client and the server are synchronized. If the time is not synchronized, there might be differences in the total number of events displayed in the Sentinel Log Manager user interface and the exported events.

6 Click *OK* to save the file.

The CSV file is UTF-8 encoded. Ensure that you have set the character encoding to UTF-8 to view the appropriate results.

5.6 Saving a Search Query

You can save the search query as a report template, a rule, or as a retention policy.

- ♦ [Section 5.6.1, “Saving a Search Query as a Report Template,” on page 87](#)
- ♦ [Section 5.6.2, “Saving a Search Query as a Rule,” on page 90](#)
- ♦ [Section 5.6.3, “Saving a Search Query as a Retention Policy,” on page 90](#)

5.6.1 Saving a Search Query as a Report Template

You can save a search query as a report template by using the *Save as Report* link in the Sentinel Log Manager /Web UI. You can use this report as a reference to create future reports. You can save the search query as a search report or as Jasper report.

- ♦ [“Saving the Query as a Search Report” on page 87](#)
- ♦ [“Saving the Query as a Jasper Report” on page 88](#)

Saving the Query as a Search Report

- 1 Log in to Novell Sentinel Log Manager.
- 2 Perform a search.

- To save the search query, click the *save as report* link.
The Save as Report dialog box is displayed.

Save As Report
Save the search query as a Report Template

Report Name:

Report Type: Event List Visualization

Search Query: (sev:[0 TO 5]) NOT at1*
NOT at1*" NOT at1*" NOT at1*"

DEFAULT REPORT RESULT PARAMETERS:

Name:

Targets:

Email To:

Event Limit:

Generate Report Results on save using current search query

- Specify the following information:

Report Name: Specify a name for the report template.

Report Type: Specify the *Event List* option to save the report in the search report format.

Search Query: Specifies the query used for the search.

- Specify the following information in the *Default Report Result Parameters* section:

Name: Specify a name for the report.

Email To: To mail the report template to a user, specify the e-mail address in the *Email Report to* field. To send the report template to more than one user, enter multiple e-mail addresses separated by commas.

Sources: This option displays the number of sources that can be searched for events. This option is useful if distributed search is enabled. To select the sources that you want searched, click the *Selected Sources* link, then select the sources.

Event Limits: To save more than 1000 results in a report, use the *Event Limits* text field to specify the number of results to show.

By default, 1000 results are stored in a report template.

- (Optional) To generate report results immediately when you save the report results, select *Generate report results on save using current search query*.
- Click *Save* to save the report definition.

You can see the saved report definition in the Report Viewer pane in the Sentinel Log Manager interface. To view the reports, see [“Viewing the Reports” on page 96](#).

Saving the Query as a Jasper Report

- Log in to Novell Sentinel Log Manager.
- Perform a search.
- To save the search query, click the *save as report* link.

A Save as Report dialog box is displayed.

- Specify the following information:

Report Name: Specify a name for the report template.

Report Type: Specify the *Visualization* option to save the report in the search report format.

Search Query: Specifies the query used for the search.

5 Specify any of the following information in the *Default Result Parameters* field, as required:

- ◆ **Name:** Specify the name of the report.
- ◆ **Sources:** This option displays the number of sources that can be searched for events. This option is useful if distributed search is enabled. To select the sources that you want searched, click the *Selected Sources* link, then select the sources.
- ◆ **Language:** Choose the language in which the report labels and descriptions should be displayed. The reports written by Novell typically provide labels and descriptions in English, French, German, Italian, Japanese, Traditional Chinese, Simplified Chinese, Spanish, or Portuguese.

The default value is the language with which the current user logged in, if that language is supported by the report. If the report does not support the language, the report's default language is used.

The data in the report is displayed in the language originally used by the event source.

- ◆ **Date Range:** If the report includes time period parameters, choose the date range. All time periods are based on the local time for the browser.
 - ◆ **Current Day:** Specify this option to list events from midnight of the current day until 11:59:59 p.m of the current day. If the current time is 8:00:00 a.m, the report shows 8 hours of data.
 - ◆ **Previous Day:** Specify this option to list events from midnight of previous day until 11:59:00 p.m of the previous day.
 - ◆ **Week To Date:** Specify this option to list events from midnight Sunday of the current week until the end of the selected day.
 - ◆ **Previous Week:** Specify this option to list the last seven days of events.
 - ◆ **Month to Date:** Specify this option to list events from midnight the first day of the current month until the end of the selected day.
 - ◆ **Previous Month:** Specify this option to list events of a month, from midnight of the first day of the previous month until 11:59:00 p.m of the last day of the previous month.
 - ◆ **Custom Date Range:** Specify this option to list events for a specific period. If you select this option, you must also specify a start and end date.
- ◆ **Email Report To:** Specify a valid Email ID, if you want the report to be mailed.
- ◆ **Event Limit:** Specify the maximum number of event search results to be included in the report.
- ◆ **Minimum Severity:** Specify the minimum severity value of the events to be displayed. The default value is 0.
- ◆ **Maximum Severity:** Specify the maximum severity value of the events to be displayed. The default value is 5.
- ◆ **Preview:** Click *Preview* to view the selected report before saving.

6 To save the report result along with the report template, click *Generate report results on save using current search query*.


7 Click *Save* to save the report definition.

You can see the saved report definition in the Report Viewer pane in the Sentinel Log Manager interface. To view the reports, see [“Viewing the Reports” on page 96](#).

5.6.2 Saving a Search Query as a Rule

While performing a search, you can save the search criteria you specified as a rule and then associate the configured actions to the rule. For more information, see [Chapter 9, “Configuring Rules and Actions,”](#) on page 137.

- 1 Log in to Novell Sentinel Log Manager.
- 2 Perform a search.
- 3 Click *save query as*, then select *save as rule*.
The Save as Rule dialog box is displayed.



Save as Rule

Save the search query as a Rule

Rule name: *

Filter: *

Perform the following actions:

to localhost:514 (see Actions)

- 4 Specify a name for the rule.
- 5 Select an action that needs to be executed the when one or more events meet the criteria of the rule.
- 6 Click *Save*.

5.6.3 Saving a Search Query as a Retention Policy

While performing a search, you can save the specified search query as a retention policy. For more information on retention policy, see [Section 3.3, “Configuring Data Retention Policies,”](#) on page 42.

- 1 Log in to Novell Sentinel Log Manager.
- 2 Perform a search.
- 3 Click *save query as*, then select *save as retention policy*.
The Save as Retention Policy dialog box is displayed.

Save as Retention Policy
 Save the search query as a retention policy

Policy Name: *

Filter: * (sev: 4) NOT st:"I" NOT st:"A" NOT st:"P"

Keep at least: * Days

Keep at most: Days

[Cancel](#) **Save**

- 4 Specify a name for the retention policy.
- 5 In the *Keep at least* field, specify the minimum number of days to retain the events in the system. The value must be a valid positive integer.
- 6 (Optional) In the *Keep at most* field, specify the maximum number of days for which the events should be retained in the system.
 The value must be a valid positive integer and must be greater than or equal to the *Keep at least* value. If no value is specified, the system retains the events in the system until the space is available in the local storage.
- 7 Click *Save*.

5.7 Sending Search Results to an Action

You can send search results to a selected actions such as e-mailing or writing to a file in Sentinel Log Manager by using the *send results to* link at the top of the search results. The *send results to* link is displayed after performing a search.

- 1 Log in to Novell Sentinel Log Manager.
- 2 Perform a search.
- 3 To send the search results to an action, click the *send results to* link.
 A Send Results To window is displayed.

Send Results To
 Perform the following action on the search results:

Action to ..\data\log_to_file_events.txt (see Actions)

Event Limit

[Cancel](#) **Send**

- 4 The *Action* field displays the list of actions. Select an action from the drop-down list.
 For more information about actions and configuring actions, see [Section 9.2, "Configuring Actions,"](#) on page 140.
- 5 In the *Event Limit* field, specify the maximum number of events to be sent to the action.
 The default value for the event limit is the number of search results obtained for that particular search.
- 6 Click *Send* to send the search results to the selected action.

5.8 Configuring the Search Limit

Searches initiate when users perform activities, such as:

- ♦ Run a search in the *Search* interface.
For more information, see [Section 5.1, “Running an Event Search,”](#) on page 77.
- ♦ Generate a report or drill down into report results.
For more information, see [Chapter 6, “Reporting,”](#) on page 93.
- ♦ Search events with specific tags.
For more information, see [Chapter 8, “Configuring Tags,”](#) on page 127
- ♦ Search events from specific event sources.
For more information, see [Section 4.4, “Configuring Data Collection for Other Event Sources,”](#) on page 64.

Searches that retrieve a large number of results, cover a large time range, or access networked storage can be resource-intensive; therefore running concurrent searches can slow down the system performance.

Sentinel Log Manager allows you to set the maximum number of searches you can run simultaneously to maintain stable performance. Sentinel Log Manager queues up searches that are initiated beyond the set limit. When both searches and reports are in queue, searches process first. If there are reports in queue for more than 1 hour, such reports process first. For information about the search performance, see [“Search and Reports Performance”](#) in the [Sentinel Log Manager 1.2.2 Installation Guide](#).

To configure the number of simultaneous searches:

- 1 Log in to the Sentinel Log Manager server with a user account that is a member of the administrator role.
- 2 Click *search setup > Configuration*.
- 3 Specify the maximum number of simultaneous searches that you want Sentinel Log Manager to run.
- 4 Click *Save*.

6 Reporting

When the Sentinel Log Manager page is loaded for the first time, all the report definitions in the system are loaded and displayed in the left pane of the page.

Sentinel Log Manager is prepackaged with a variety of Jasper reports, some of which are general and some of which are device-specific (For example, SUSE Linux). Some of the reports are flexible to allow users to specify the columns to be displayed in the results. These reports use a Lucene-based query language.

Users can run, schedule, and e-mail PDF reports. They can also run any report as a search and then interact with the results as they would any search, such as refining the search or performing an action on the results. For more information, see [Chapter 5, “Searching Events,” on page 77](#).

You can also run reports on Sentinel Log Manager servers which are distributed across different geographic location. For more information, see [Chapter 7, “Searching and Reporting Events in a Distributed Environment,” on page 109](#).

All report results are depend on the data viewing permissions associated with the user's role.

The following sections describe the reporting feature of Novell Sentinel Log Manager:

- ◆ [Section 6.1, “Running Reports,” on page 93](#)
- ◆ [Section 6.2, “Viewing the Reports,” on page 96](#)
- ◆ [Section 6.3, “Scheduling a Report,” on page 98](#)
- ◆ [Section 6.4, “Adding Report Definitions,” on page 99](#)
- ◆ [Section 6.5, “Renaming a Report Result,” on page 100](#)
- ◆ [Section 6.6, “Marking Report Results as Read or Unread,” on page 100](#)
- ◆ [Section 6.7, “Managing Favorite Reports,” on page 102](#)
- ◆ [Section 6.8, “Exporting Report Definitions and Report Results,” on page 103](#)
- ◆ [Section 6.9, “Deleting Reports,” on page 106](#)

6.1 Running Reports

You can run and schedule report definitions that are saved in the system. You can also view the report results of the report definitions.

The Report Viewer pane of the Sentinel Log Manager page displays all the report definitions in the system. Because the reports run asynchronously, you can simultaneously perform other tasks in the application.

You can run a report by using the desired parameters such as a start and an end date, and save the report results with a name of your choice. After the report runs, the results can be viewed by clicking the *View Report PDF* icon next to the relevant report result list. If the report format chosen is Jasper report, the results are displayed in the PDF format. If the report format chosen is search report, the results are displayed in a new search results tab.

If the Sentinel Log Manager server was restarted while a report was processing, you can either cancel or restart the report by selecting the relevant buttons. If you restart the report, it is run with the same parameters that were used the first time. If the report was run with a relative time setting (such as *Last 12 hours*), the time period for rerunning the report is based on the current date and time and not the date and time when the report was initially run.

Use the following procedure to run a report:

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section, select the report you want to run, then click *Run*.

The Run Report Name window is displayed.



- 3 Specify if you want to run the report now or if you want to schedule it to run at a certain time.
- 4 Specify a name to identify the report results.

Because the username and time are also used to identify the report results, the report name does not need to be unique.

- 5 (Optional) If your Sentinel Log Manager is configured for distributed search, click the *Selected Targets* link in the *Targets* section to select the source machines on which the reports can be run. For more information on distributed search, see [Chapter 7, "Searching and Reporting Events in a Distributed Environment,"](#) on page 109.
- 6 (Optional) To run a search report, specify the following parameters:

Parameter	Description
Maximum Results	Specify the maximum number of event search results to include in the report.
Durations	<p>If the report includes time period parameters, choose the date range. All time periods are based on the local time for the browser.</p> <ul style="list-style-type: none"> ◆ Last 1 hour: Shows events for the last hour. ◆ Last 12 hours: Shows events for the last 12 hours. ◆ Last 24 hours: Shows events for the last 24 hours. ◆ Last 7 days: Shows events for the last seven days. ◆ Last 30 days: Shows events for the last 30 days. ◆ Last 60 days: Shows a month of events, from midnight of the first day of the previous month until 11:59 p.m. of the last day of the previous month. ◆ Last 90 days: Shows events for the last 90 days. ◆ Whenever: Shows all events stored in the system. ◆ Custom Date Range: If you selected <i>Custom Date Range</i>, set the start date (From Date) and the end date (To Date) for the report.

7 (Optional) To run a Jasper report, specify the following parameters:

Jasper reports can also have additional parameters defined when you create the Jasper report. To view the description for an additional parameter via a tool tip, mouse over the parameter names on the Run Report form.

Parameter	Description
Help	Click <i>Help</i> to open the <code>doc_plugin.pdf</code> and to read the getting started notes for the selected Jasper report.
Maximum Results	Specify the maximum number of event search results to include in the report.
Language	<p>Choose the language in which the report labels and descriptions should be displayed. The possible values are English, French, German, Italian, Japanese, Traditional Chinese, Simplified Chinese, Spanish, or Portuguese.</p> <p>The default value is the language with which the current user logged in, if that language is supported by the report. If the report does not support the language, the report's default language (typically English) is used.</p> <p>The data in the report is displayed in the language that was originally used by the event source.</p>
Date Range	<p>If the report includes time period parameters, choose the date range. All time periods are based on the local time for the browser.</p> <ul style="list-style-type: none">◆ Current Day: Shows events from midnight of the current day until 11:59:00 p.m. of the current day. If the current time is 8:00:00 AM, the report shows 8 hours of data.◆ Previous Day: Shows events from midnight yesterday until 11:59:00 p.m. yesterday.◆ Week To Date: Shows events from midnight Sunday of the current week until the end of the selected day.◆ Previous Week: Shows events for the last seven days.◆ Month to Date: Shows events from midnight the first day of the current month until the end of the selected day.◆ Previous Month: Shows events for a month, from midnight of the first day of the previous month until 11:59:00 p.m. of the last day of the previous month.◆ Custom Date Range: Shows events for a period whose start and end date are chosen.
Primary Top N	Specify a maximum number of value for the search event.
Primary Event Field	Specify the primary event tag for primary grouping.
Event Field	Specify the secondary event tag.
Minimum Severity	Specify the minimum severity value of the events to be displayed. The default value is 0.
Maximum Severity	Specify the maximum severity value of the events to be displayed. The default value is 5.

- 8 Specify the e-mail address in the *Email Report to* field. If you want to mail the report to more than one user, specify the e-mail addresses separated by a comma.
To enable mailing reports, configure the mail relay under *Rules > Configuration*.
- 9 Click *Run*.
A report results entry is created and mailed to the chosen recipients.

6.2 Viewing the Reports

Novell Sentinel Log Manager users can view the report template and report results that are in the system. The reports are loaded and displayed in the left pane of the page. Click *More > Show All Reports* to view all reports or click *More > Only Show Scheduled Reports* to show only the scheduled reports.

The report results for each users varies depending on the data security settings configured for the role of that user.

All the report results are ordered by the creation time. If there is more than one report, the *show more* link displays the other report results.

In the Report Viewer, the *Favorites* and *Other* sections show the number of unread reports with a blue dot next to them.

The count next to *Favorite* and *Other* shows the number of report definitions under the Favorite and Other sections.

A blue dot next to the report result indicates that the report result is unread. For more information, see [“Marking Report Results as Read or Unread” on page 100](#).

- ♦ [Section 6.2.1, “Viewing the Report Result in PDF Format,” on page 96](#)
- ♦ [Section 6.2.2, “Drilling Down into Report Results,” on page 97](#)
- ♦ [Section 6.2.3, “Viewing Report Parameters,” on page 98](#)

6.2.1 Viewing the Report Result in PDF Format

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section, select the report definition that you want to run, then click *Run*.
- 3 Click the report definition to view the report results in the Report Viewer pane. An unread report result appears with a blue dot next to it.
- 4 Select a report result.
- 5 To view the report in PDF format, click the PDF icon.
- 6 View the report parameter values used to run the report at the bottom left corner of the page.
When a report definition is expanded, some report definitions display a *Sample Report* link, if a report definition contains a sample report.
- 7 Click *Sample Report* to display a *View* link.
- 8 Click *View* to find out how the completed report looks with a set of sample data.
Report results are organized from the newest to the oldest.

On systems running with the free license, any report results that are generated while the event flow averages more than 25 EPS for the particular time period do not include the details of the events that are tagged with the `OverEPSLimit` tag. Sentinel Log Manager tags such report results with the `CreatedDuringEval` tag.

The following image shows a sample report result that includes the `OverEPSLimit` tagged events:

ProductName	Severity	InitUserName	InitIP	TargetIP
Internal 10/7/10 2:08:56 AM	1	admin	10.0.0.1	10.0.0.1
Internal 10/7/10 2:03:21 AM	1	admin	10.0.0.1	10.0.0.1
Internal 10/7/10 1:56:51 AM	1	admin	10.0.0.1	10.0.0.1
Internal 10/7/10 1:55:27 AM	1	admin	10.0.0.1	10.0.0.1
NewDataObject				
Internal 10/7/10 2:16:01 AM	1	10.0.0.1		10.0.0.1
Over EPS Limit				
	1			
10/7/10 2:13:56 AM				
	1			
10/7/10 2:12:57 AM				
	1			
10/7/10 2:12:56 AM				
	4			
10/7/10 2:12:56 AM				
	1			
10/7/10 2:12:56 AM				
	5			
10/7/10 2:12:56 AM				

After you upgrade the system to an enterprise license, you can run the tagged reports again to verify that they include the events that were originally tagged as `OverEPSLimit`. To specifically search for the tagged report results, enter `CreatedDuringEval` in the report search criteria.

6.2.2 Drilling Down into Report Results

The drill-down viewing option provides the ability to launch a search with the same query and time frame that was used to generate the report. This option allows users to view details of the event used to generate the report.

Drill-down feature is available only on reports that run against the file-based event store, or multiple event stores, in the case of a distributed query. It is not available on Sentinel Log Manager configuration reports which run against the database.

Drill-down feature is available only on reports that specify the Lucene query in the `main.jrxml` file of the report. This is true for most reports that are written by Novell, with the exception of a few reports that rely on multiple subreports, such as the Novell Top Ten reports.

The report results that were generated in versions of Sentinel Log Manager older than 1.1 are not drillable. However, to enable these reports as drillable, you can run the report again after upgrading to Sentinel Log Manager 1.1 or higher.

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section, select the report you want to run, then click *Run*.
- 3 Click the report definition to view the report results in the Report Viewer pane. An unread report result appears with a blue dot next to it.

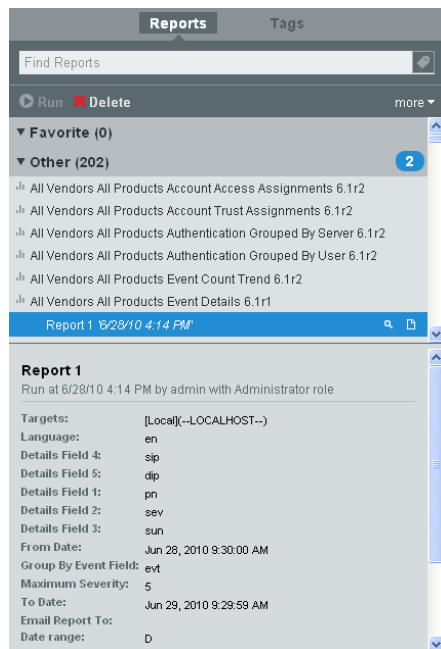
- 4 Select a report result.
- 5 Click the drill-down icon to launch the drill-down query.

6.2.3 Viewing Report Parameters

The Report Viewer pane on the left side of the page displays a status pane at the bottom left corner of the page. The status pane displays the parameter information associated with the selected report. It also displays the error messages, if the report execution resulted in an error.

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section, click a report definition to expand it.
- 3 Select the report to view the parameters associated with the selected report.

The report parameters are displayed in the status pane.



6.3 Scheduling a Report

Sentinel Log Manager also allows you to schedule a report to run at regular intervals. You can run the report immediately or schedule it to run later, either once or on a recurring basis. For scheduled reports, choose a frequency and specify a time for the report to run. The report runs based on the time settings of the Sentinel Log Manager server.

- ◆ **Now:** This is the default. It runs the report immediately.
- ◆ **Once:** Runs the report once at the specified date and time.
- ◆ **Daily:** Runs the report once a day at the specified time.
- ◆ **Weekly:** Runs the report once a week on the same day at the specified time.
- ◆ **Monthly:** Runs the report on the same day of the month every month, starting at the specified date and time. For example, if the start date and time is May 26, 2010 4:00:00 p.m., the report runs on the 26th day of the month at 4:00:00 p.m. every month.

NOTE: All time settings are based on the machine's local time.

Report schedules can be removed or modified by using the *Delete* and *Edit* links.

6.4 Adding Report Definitions

Reports in Sentinel Log Manager are designed as plug-ins (special `.zip` or `.rpz` files that include the report definition in addition to the metadata and resources used by the report). New or updated reports can be uploaded into Sentinel Log Manager by users who are members of a role with the *Manage Reports* permission.

The primary sources for new or updated reports are:

- ♦ **Solution Packs:** Solution Packs provide a framework within which sets of content can be packaged into controls, each of which is designed to enforce a specific business or technical policy. They are created in Sentinel Solution Designer and contain different types of plug-ins, including Sentinel Log Manager reports. For more information on Solution packs, see the [Sentinel Plug-ins Web Site](http://support.novell.com/products/sentinel/sentinel61.html). (<http://support.novell.com/products/sentinel/sentinel61.html>)
- ♦ **JasperForge iReport:** You can modify or write reports by using JasperForge iReport, which is a graphical report designer for JasperReports. iReport is an open source report development tool that is available for download from [JasperForge.org](http://jasperforge.org) (http://jasperforge.org/plugins/project/project_home.php?group_id=83) (as of the time of this publication).

New or modified reports can include additional database fields that are not presented in the Sentinel Log Manager interface. They must adhere to the file and format requirements of the report plug-ins. For more information about database fields and file and format requirements for report plug-ins, see the [Sentinel SDK Web site](http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

This section has the following information:

- ♦ [Section 6.4.1, “Adding or Uploading a Report,” on page 99](#)

6.4.1 Adding or Uploading a Report

Use the following procedure to add or upload a report:

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section.
- 3 Click the *more* drop-down list in the Report Viewer pane and select *Upload*.
- 4 Browse and select the report plug-in `.zip`, `.rpz`, or `.spz` file from your local machine.
- 5 Click *Open*.
- 6 Click *Upload*.

The new report definition is added to Report Template list in alphabetical order and can be run immediately, if necessary.

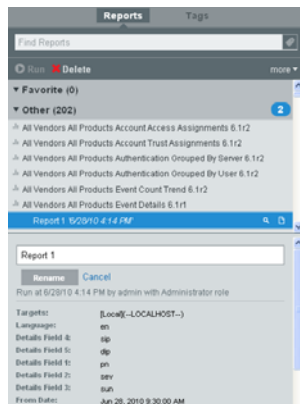
Sentinel Log Manager verifies the unique ID of the report to determine whether an older or identical version of the report already exists in the report repository. If it does, Sentinel Log Manager displays the details of both the reports so that the user can decide whether to cancel the action or replace the existing report with the current report.

If the same report already exists in the report repository, decide based on the unique ID of the report whether to replace the existing report or not.

Sentinel Log Manager displays details of both the reports.

6.5 Renaming a Report Result

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section.
- 3 Click a report definition to view the report results in the Report Viewer pane.
- 4 Select a report result.
- 5 Do one of the following:
 - ◆ Click the *more* drop-down list in the Report Viewer pane and select *Rename*.
 - ◆ Double-click the report name in the status pane.



- 6 Specify a name in the bottom left status pane.
- 7 Click *Rename*.

The selected report result is renamed under the report definition.

6.6 Marking Report Results as Read or Unread

When a report result is created under a report definition, the report result is in unread state. An unread report result appears with a blue dot next to the report result in the Report Viewer. When you view a report result, the blue dot is removed to indicate that the report has been read. You can also manually mark a report result as read or unread without viewing it.

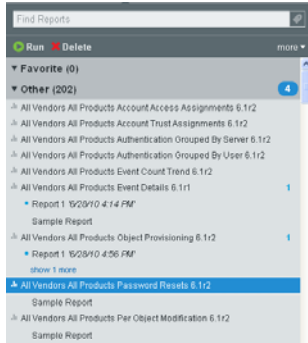
In the Report Viewer, each of the report templates or definitions shows the number of unread reports next to it.

NOTE: The reports marked as read or unread are on a per-user basis. Each user can have a different set of read or unread reports.

- ◆ [Section 6.6.1, “Marking a Single Report Result as Read or Unread,” on page 101](#)
- ◆ [Section 6.6.2, “Marking Multiple Report Results as Read or Unread,” on page 101](#)

6.6.1 Marking a Single Report Result as Read or Unread

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section.
- 3 To mark a report as read, select an unread report result (a report result with a blue dot next to it) in the Report Viewer pane.



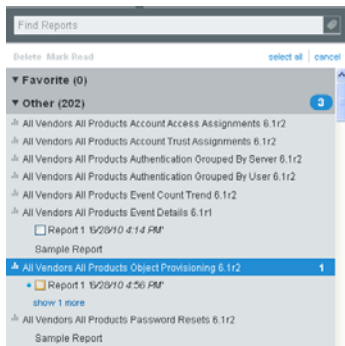
- 4 Click the *more* drop-down list and select *Mark Read*.
The report result changes to the Read state and the blue dot is removed.
- 5 To Mark a report as unread, select a read report result without a blue dot next to it in the *Reports* section.



- 6 Click the *more* drop-down list and select *Mark Unread*.
The report result changes to the Unread state and a blue dot is added next to the report result.

6.6.2 Marking Multiple Report Results as Read or Unread

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section.
- 3 Click the *more* drop-down list in the Report Viewer pane and click *Select Multiple Results*.
A check box is displayed next to each report result in the Report Viewer pane.



- 4 Select the check boxes next to the report results that you want to select.

To mark read reports as unread, select reports without the blue dot next to them. To mark unread reports as read, select the reports with the blue dot next to them.

You can also use the *select all* link to select all the available report results. To deselect all the selected reports, click the *clear all* link.

If the report results are not selected, the *Mark Read* or *Mark Unread* links are disabled.

- 5 To mark reports as read, click the *Mark Read (x)* link.

(x) indicates the number of reports selected.

The selected report results change to the Read state and the blue dot is removed.

- 6 To mark reports as unread, click the *Mark Unread (x)* link.

The selected report results change to the Unread state and the blue dot is added.

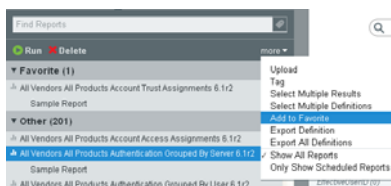
6.7 Managing Favorite Reports

- ◆ [Section 6.7.1, “Adding Reports as Favorites,” on page 102](#)
- ◆ [Section 6.7.2, “Removing Favorite Reports,” on page 103](#)

6.7.1 Adding Reports as Favorites

You can mark individual report definitions as Favorite so that they are easier to find.

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section.
- 3 Select a report definition from *Other*.
- 4 Click the *more* drop-down list in the Report Viewer pane and click *Add to Favorite*.

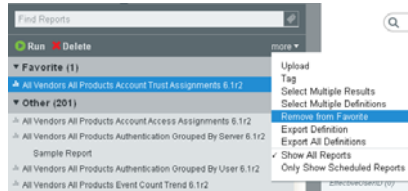


The selected report definition is displayed in *Favorite* in the Reports Viewer pane.

NOTE: The reports marked as favorites are on a per-user basis. Each user can have a different set of favorite reports.

6.7.2 Removing Favorite Reports

- 1 Log in to Sentinel Log Manager.
- 2 In the Reports section.
- 3 Select a report definition from *Favorite*.
- 4 Click the *more* drop-down list in the Report Viewer pane and click *Remove from Favorite*.



- 5 The selected report definition is removed from *Favorite* and added to *Other* in the Report Viewer pane.

6.8 Exporting Report Definitions and Report Results

You can export report definitions and report results. You can export report definitions from one Sentinel Log Manager instance and export it into another instance of Sentinel Log Manager. The report results can be exported and saved or sent to another user

NOTE: When you export report definitions, only the report definitions are exported. None of the report results are exported.

- ♦ [Section 6.8.1, “Exporting a Single Report Definition,” on page 103](#)
- ♦ [Section 6.8.2, “Exporting Selected Report Definitions,” on page 104](#)
- ♦ [Section 6.8.3, “Exporting All Report Definitions,” on page 104](#)
- ♦ [Section 6.8.4, “Exporting a Report Result,” on page 105](#)

6.8.1 Exporting a Single Report Definition

You can use the *Export Definition* option to export the selected report as a .zip file. The *Export Definition* option is only available when a report definition is selected.

- 1 Log in to Novell Sentinel Log Manager.
- 2 Select a report definition in the Report Viewer pane.
- 3 Click the *more* drop-down list in the Report Viewer pane and select *Export Definition*.



The report is zipped into a file and provided to you for download.

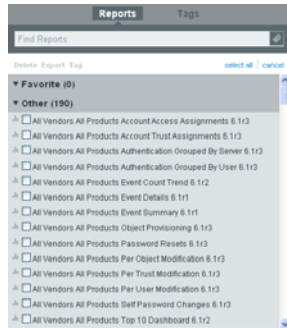
The Opening <Selected Report Name>.zip dialog box provides the option to save the <Selected Report Name>.zip file on your local machine.

- 4 Save the file to the location you prefer.

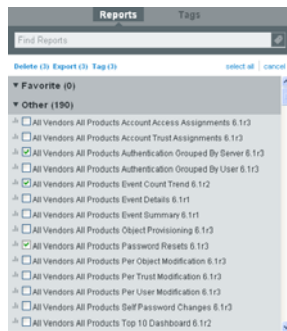
6.8.2 Exporting Selected Report Definitions

You can export the selected reported definitions as a .zip file.

- 1 Log in to Novell Sentinel Log Manager.
- 2 Click the *more* drop-down list in the Report Viewer pane, then select the *Select Multiple Definitions* option.



- 3 Select the report definitions that you want to export.

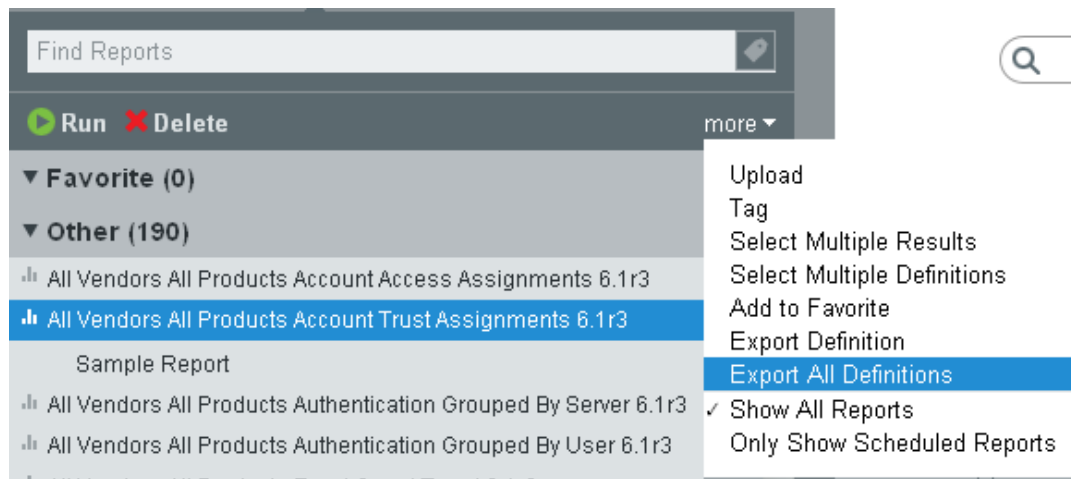


- 4 Click *Export*.
The *Opening reportexport.zip* dialog box is displayed with the option to save it.
- 5 Save the file to a location you prefer.

6.8.3 Exporting All Report Definitions

You can use the *Export All Definitions* option to export all reports as a .zip file.

- 1 Log in to Sentinel Log Manager.
- 2 Select the *All* or *Favorite* list of the Report Viewer pane.
- 3 Click the *more* drop-down list in the Report Viewer pane and select *Export All Definitions*.



All reports are zipped into a file and provided to you for download.

The *Opening reportexport.zip* dialog box is displayed with the option to save the file.

- 4 Save the file to a location of your preference.

6.8.4 Exporting a Report Result

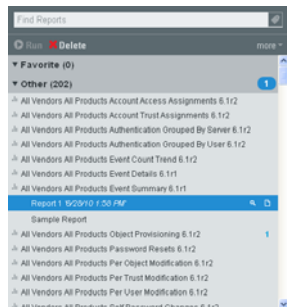
You can export the report result to a file.

- 1 Log in to Novell Sentinel Log Manager.
- 2 Select a report definition in the Report Viewer pane.

A list of available report results appear.

- 3 Select the report result.

The *View Report PDF* icon is displayed next to the report result.



- 4 Click the icon.

A dialog box appears with an option to export and save the file as *<Report Def name>_<Report result name>.pdf*.

- 5 Click OK to save the file.

6.9 Deleting Reports

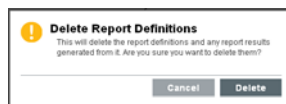
You can delete a report definition or a report result. If a report definition is deleted, all associated report results are also deleted.

- ◆ [Section 6.9.1, “Deleting a Report Definition,” on page 106](#)
- ◆ [Section 6.9.2, “Deleting Multiple Report Definitions,” on page 106](#)
- ◆ [Section 6.9.3, “Deleting a Report Result,” on page 107](#)
- ◆ [Section 6.9.4, “Deleting Multiple Report Results,” on page 107](#)

6.9.1 Deleting a Report Definition

- 1 Log in to Novell Sentinel Log Manager as a user with permission to manage reports.
- 2 Select a report definition in the Report Viewer pane.
- 3 Click the *Delete* button in the Report Viewer pane.

The following confirmation message is displayed:

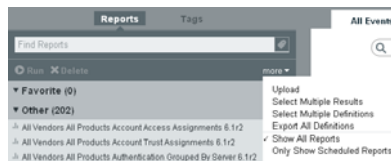


- 4 Click *Delete* to delete the selected report definition.
The selected report definition is deleted from the Report Viewer pane.

6.9.2 Deleting Multiple Report Definitions

You can select multiple report definitions and delete all of them.

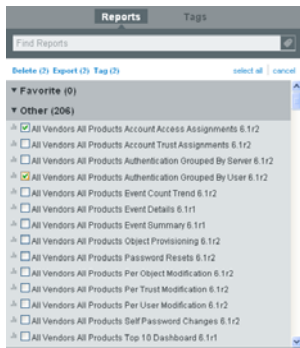
- 1 Log in to Novell Sentinel Log Manager.
- 2 Click the *more* drop-down list in the Report Viewer pane and select *Select Multiple Definitions*.



- 3 A check box is displayed next to each report result in the Report Viewer pane. Select the check boxes to select the report definitions that you want to delete.

You can also use the *select all* link to select all the available report definitions. To clear all the selected reports, click *Clear all*.

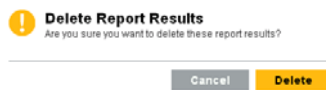
If the report definitions are not selected, the *Delete* and *Mark Read* links are disabled.



4 The *Delete(x)* in the Report Viewer pane shows the number of selected report definitions, where *(x)* is the number of selected report results.

5 Click *Delete(x)*.

The following confirmation message is displayed.



6 Click *Delete*.

The selected report definitions are deleted.

6.9.3 Deleting a Report Result

1 Log in to Novell Sentinel Log Manager.

2 Select a report result under a report definition from the Report Viewer pane.

3 Click the *Delete* button in the Report Viewer pane.

The following confirmation message is displayed.



4 Click *Delete* to delete the selected report result.

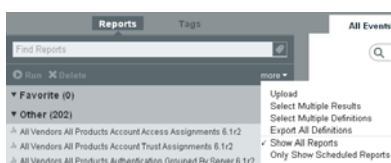
The selected report result under the report definition is deleted from the Report Viewer pane.

6.9.4 Deleting Multiple Report Results

You can select multiple report results and delete all of them.

1 Log in to Novell Sentinel Log Manager.

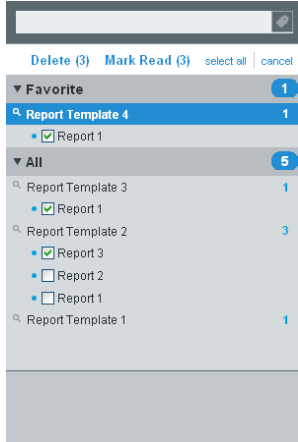
2 Click the *more* drop-down list in the Report Viewer pane and select *Select Multiple Results*.



- 3 A check box is displayed next to each report result in the Report Viewer pane. Select the check boxes to select the report results.

You can also use the *select all* link to select all the available report results. To clear all the selected reports, click *Clear all*.

If the report results are not selected, the *Delete* and *Mark Read* links are disabled.



- 4 The *Delete(x)* option in the Report Viewer pane shows the number of selected report results, where (*x*) is the number of selected report results.

- 5 Click *Delete(x)*.

- 6 Click *Delete*.

The selected report results are deleted.

7 Searching and Reporting Events in a Distributed Environment

The Sentinel Log Manager Distributed Search feature enables you to search for events and run reports not only on your local Sentinel Log Manager server, but also on other Sentinel Log Manager servers distributed across the globe.

- ♦ [Section 7.1, “Overview,” on page 109](#)
- ♦ [Section 7.2, “Configuring Servers for Distributed Searching and Reporting,” on page 111](#)
- ♦ [Section 7.3, “Searching for Events,” on page 117](#)
- ♦ [Section 7.4, “Managing the Distributed Search Results,” on page 118](#)
- ♦ [Section 7.5, “Viewing the Search Activities,” on page 120](#)
- ♦ [Section 7.6, “Running Reports,” on page 120](#)
- ♦ [Section 7.7, “Managing the Distributed Setup Configuration,” on page 121](#)
- ♦ [Section 7.8, “Troubleshooting,” on page 124](#)

NOTE: The Distributed Search and Report feature is a licensed feature. This feature is not available in systems running with the free license. For more information, see [Section 13.1, “Understanding the Licenses,” on page 171](#).

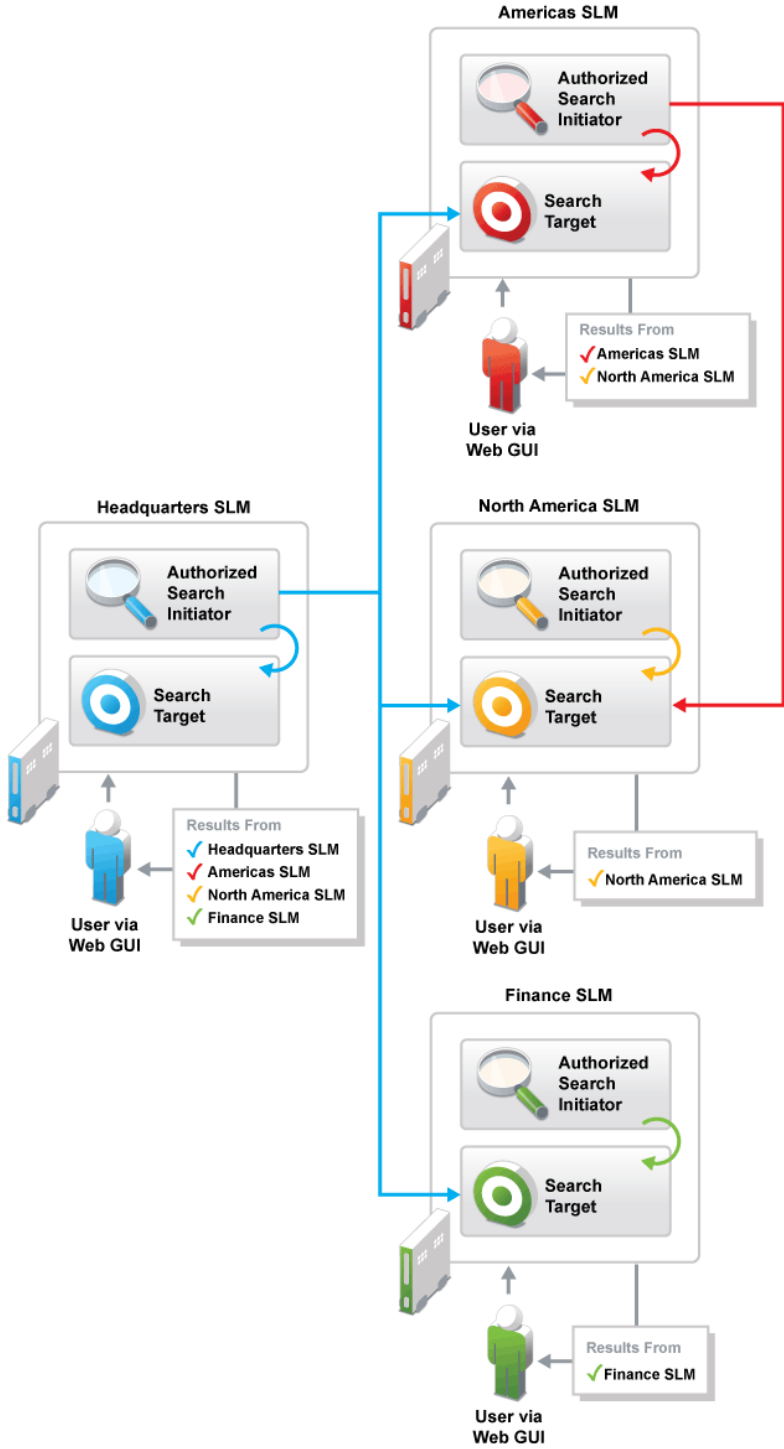
7.1 Overview

The Distributed Search feature facilitates searching events and reporting event data from local and remote Sentinel Log Manager servers. When you are working with multiple servers, you can perform a search or run a report on just one server and have it automatically run a search or report across the selected remote servers. The server on which the search is initiated is referred to as the search initiator, and the remote servers are referred to as the search targets or target servers.

When you run a search or report on the search initiator, search queries are sent to each selected target server. The target server authenticates the search initiator server, using a password that is exchanged during configuration. Event data is returned to the search initiator, where it is merged, sorted, and consolidated for presentation. Individual search results display the target servers from which they were received. The search status for each server is available for viewing and troubleshooting.

[Figure 7-1](#) shows an illustration of how you can set up the Sentinel Log Manager servers across the globe for distributed searching and reporting.

Figure 7-1 Distributed Search Setup



7.2 Configuring Servers for Distributed Searching and Reporting

To configure a search initiator for distributed search, you must first enable distributed searching on the search initiator server.

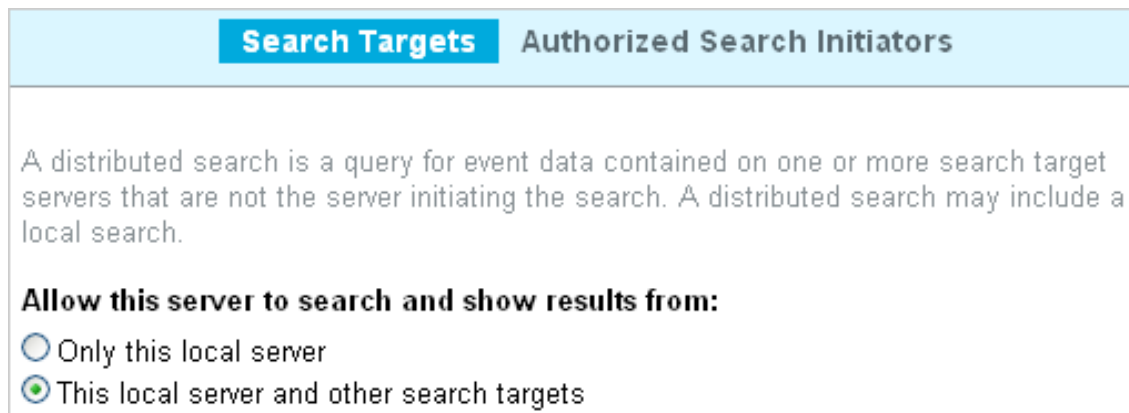
After you enable distributed search, you need to add target servers to the search initiator server. If you know the administrator username and password for the target server, you can add the target server directly from the search initiator.

If you do not know the administrator username and password for a target server, you can set up the search initiator with an opt-in password that allows administrators of target servers to add their target servers to the search initiator. When you do this, administrators of target servers do not need to share their usernames and passwords with you. You must share the opt-in password with the target server administrator.

- ♦ [Section 7.2.1, “Enabling Distributed Search,” on page 111](#)
- ♦ [Section 7.2.2, “Adding a Search Target Server by Using the Administrator Credentials,” on page 112](#)
- ♦ [Section 7.2.3, “Adding a Search Target Server by Using the Opt-in Password,” on page 114](#)

7.2.1 Enabling Distributed Search

- 1 Log in to the search initiator as an administrator.
- 2 Click *search setup* > *Search Targets*.



Search Targets Authorized Search Initiators

A distributed search is a query for event data contained on one or more search target servers that are not the server initiating the search. A distributed search may include a local search.

Allow this server to search and show results from:

Only this local server

This local server and other search targets

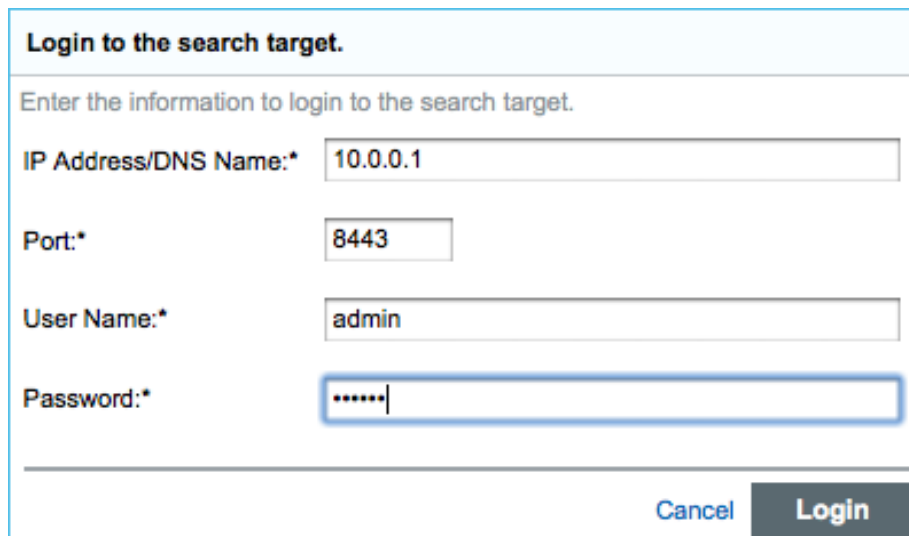
- 3 Select *This local server and other search targets*.
- 4 Do one of the following to add target servers to your search initiator:
 - ♦ If you are the administrator of the search initiator and you know the administrator username and password on the target server, continue with [Section 7.2.2, “Adding a Search Target Server by Using the Administrator Credentials,” on page 112](#).
 - ♦ If you are the administrator of the search initiator and you do not know the administrator username and password on the target server, you can set an opt-in password to allow administrators of target servers to add their target servers to the search initiator. Continue with [Section 7.2.3, “Adding a Search Target Server by Using the Opt-in Password,” on page 114](#).

7.2.2 Adding a Search Target Server by Using the Administrator Credentials

If you are the administrator of the search initiator and you know the administrator username and password on the target server, you can add the target server while you are logged in to your search initiator server.

IMPORTANT: You should ensure that the target server that you add is able to communicate with the search initiator. The target server should be able to communicate through TCP/IP. The IP address or hostname of the target server must be accessible through firewalls, NATs, etc. You can use the ping command to ensure that there is communication from both ways. If there is a communication failure between the servers, an error is displayed in the extended status page. For more information, see [Section 7.4, “Managing the Distributed Search Results,”](#) on page 118.

- 1 Log in to the search initiator as an administrator.
- 2 Click *search setup > Search Targets*.
- 3 Click the *Add* link.
- 4 Specify the following information:



Login to the search target.

Enter the information to login to the search target.

IP Address/DNS Name:* 10.0.0.1

Port:* 8443

User Name:* admin

Password:*

Cancel Login

- ♦ **IP Address/DNS Name:** IP address or the DNS name of the target server.
 - ♦ **Port:** Port number of the target server. The default port number is 8443. The target server and search initiator do not need to be on the same port.
 - ♦ **User Name:** User name to log in to the target server. This must be a user with administrator privileges.
 - ♦ **Password:** Password associated with the user name.
- 5 Click *Login*.
The Confirm Certificate page is displayed.
 - 6 Verify the Certificate information, then click *Accept*.
The Add Search Target page is displayed. It lists the various proxy roles on target server.

Add Search Target

Enter a display name and select the search proxy role. The role search permissions will be used during the search.

Name:*

Search Proxy Role:* (choose from table below)

Note: Showing only roles that have distributed search proxy as role permission.

	Role Name	Description
<input checked="" type="checkbox"/>	Users	This role represents general users on an SLM system

Cancel
OK

7 In the *Name* field, specify a descriptive name that you want to give to the search target.

This helps you to easily identify the target server by a name instead of by its IP address or DNS name.

8 Select a search proxy role that you want to assign to the search initiator.

When the search initiator makes search requests to the target server, the proxy role's security filter is used when performing the search. Only events that pass the proxy role's security filter are returned to the search initiator server.

Only roles that have the `Proxy for Authorized Search Initiators` permission are listed. This permission is required for the target server to accept and process incoming search requests from the search initiator server.

9 Click *OK*.

The server information is listed in the *Search Targets* list.

Search Targets
Authorized Search Initiators

A distributed search is a query for event data contained on one or more search target servers that are not the server initiating the search. A distributed search may include a local search.

Allow this server to search and show results from:

Only this local server

This local server and other search targets

Search Targets

Enabled	Search Target Name	Address		
<input checked="" type="checkbox"/>	SLM Server - Vienna	10.0.0.1	Edit	Delete

Refresh | [Set Opt-in Password](#) | [Add](#)

You can now search events or view event reports from the target server. For more information, see [Section 7.3, "Searching for Events,"](#) on page 117 and [Section 7.6, "Running Reports,"](#) on page 120.

7.2.3 Adding a Search Target Server by Using the Opt-in Password

In organizations where administrative control of Sentinel Log Manager servers is decentralized, it might violate the security policy to share administrator passwords. However, Sentinel Log Manager allows you to share a limited-purpose opt-in password to add target servers, which is more secure than requiring full administrator credentials. If you are not the administrator of the target server, you can set an opt-in password in the search initiator server, then provide the opt-in password to the target server administrators to allow them to opt in to the search initiator server.

When a target server opts in to the search initiator, a message is sent to the search initiator server requesting that it be added to the list of target servers maintained by the search initiator server. The request authorizes the search initiator to access event data on the target server. The search initiator requires an opt-in password to verify that the opt-in request has originated from a valid target server. During the opt-in process, the search initiator and the target server exchange the appropriate password, which allows the target server to authenticate the search requests from the search initiator.

This procedure is similar to adding a target server, but it is done from the target server instead of the search initiator server.

- ♦ [“Setting the Opt-In Password” on page 114](#)
- ♦ [“Authorizing a Search Initiator Server” on page 114](#)

Setting the Opt-In Password

- 1 Log in to the search initiator as an administrator.
- 2 Click *search setup > Search Targets*.
- 3 Select *This local server and other search targets*.
- 4 Click *Set Opt-in Password*.

A search target is a log manager server from which events can be retrieved during a search. If you do not have administrative access to the search target, the opt-in password needs to be shared with the search target administrator to authorize this local server to perform search.

Opt-in Password:

Confirm Password:

[Cancel](#) [Set Password](#)

- 5 Specify the opt-in password, then click *Set Password*.
- 6 Continue with [“Authorizing a Search Initiator Server” on page 114](#) to add the target server to the search initiator.

Authorizing a Search Initiator Server

- 1 Log in to the target server as an administrator.
- 2 Click *search setup > Search Targets*.
- 3 Select the *Authorized Searcher Initiators* tab.

- 4 Check the *Allow these authorized search initiators to search this server as a search target* box.
- 5 Click the *Add* link.

The Add Authorized Search Initiator page is displayed.

Add Authorized Search Initiator

Enter the information to allow this local server to allow searching events from the authorized search initiator.

IP Address/DNS Name:*

Port:*

Opt-in Password:*

CancelOK

- 6 Specify the following information:
 - ♦ **IP Address/DNS Name:** The IP address or the DNS name of the search initiator.
 - ♦ **Port:** Port number of the search initiator. This is the port number on which the search initiator listens for incoming opt-in requests. The default port number is 8443.
 - ♦ **Opt-in Password:** The opt-in password that you configured on the search initiator. You must obtain this password from the administrator of the search initiator.

- 7 Click *OK*.

The Confirm Certificate page is displayed.

- 8 Verify the certificate information, then click *Accept*.

The Add Authorized Search Initiator page is displayed that lists the various proxy roles on the search target servers.

Add Authorized Search Initiator

Enter a display name and select the search proxy role. The role search permissions will be used during the search.

Name:*

Search Proxy Role:*

Note: Showing only roles that have distributed search proxy as role permission.

	Role Name	Description
<input checked="" type="checkbox"/>	Users	This role represents general users on an SLM system

Cancel **OK**

- 9 In the *Name* field, specify a descriptive name that you want to give to the search initiator server. This helps you to easily identify the search initiator server by a name instead of by its IP address or DNS name.
- 10 Select a proxy role that you want to assign to the search initiator.

When the search initiator makes search requests to the target server, the proxy role's security filter is used when performing the search. Only events that pass the proxy role's security filter are returned to the search initiator.

Only roles in the target server that have the *Proxy for Authorized Search Initiators* permission are listed. This permission is required for the target server to accept and process incoming search requests from the search initiator.
- 11 Click OK.

The search initiator is added to Authorized Search Initiators list and is enabled by default.

Search Targets **Authorized Search Initiators**

An authorized search initiator is another server that can access data from this local server.

Allow these authorized search initiators to search this server as a search target.

Authorized Search Initiators Refresh | Add

Enabled	Search Initiator Name	Address	Search Proxy Role	
<input checked="" type="checkbox"/>	SLM Server - Provo	10.0.0.2	Users	Search Activities Edit Delete

NOTE: Also, the target server gets added under the Search Targets list in the search initiator server. Alternatively, you can click the *Refresh* link to see the target server in the Search Targets list.

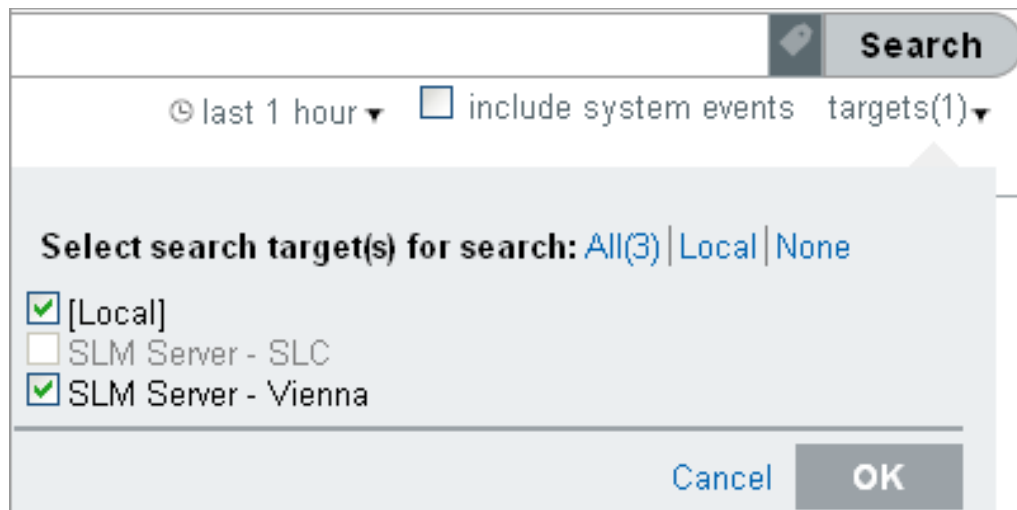
7.3 Searching for Events

Searching for events in a distributed environment is similar to how you perform a search on your local server, except that you perform the search on the selected target servers and can also include your local server.

- 1 Log in to the search initiator server as a user with Search Remote Targets permission.
- 2 Click *New Search*.
- 3 Click the *targets* link on the upper right corner of the page.

A page is displayed that lists the target servers that you have added, including the local server. The target servers that are disabled are also displayed, but they are dimmed.

The targets link appears only if you have added the target servers to your local server. For more information, see [Section 7.2.2, “Adding a Search Target Server by Using the Administrator Credentials,”](#) on page 112.



- 4 Select the check boxes next to the target servers on which you want to perform a search, then click *OK*.
- 5 Specify the search criteria in the search field, then click *Search*.

If you do not specify any search criteria, the search initiator server runs a default search for all events with severity 0 to 5.

The Search Results page displays the events from the selected target servers and the local server (if it selected). The search results are filtered through the combination of the security filter and permissions of the logged-in user and the security filter and permissions of the search proxy role on the target servers. For information on the distributed search results, see [Section 7.4, “Managing the Distributed Search Results,”](#) on page 118.

7.4 Managing the Distributed Search Results

The Search Results page displays the events from the selected target servers and the local server, based on the search criteria you specified. Each event displays the target server information from which the event is being retrieved.

Figure 7-2 Distributed Search Results

The screenshot shows a web interface for search results. At the top, there are buttons for 'export results', 'save as report', 'send results to', and 'all details++'. Below this, a summary bar indicates 'Displaying 25 of 2,169,033 events from 2 targets'. A 'REFINE' section on the left shows field counts for the first 84,020 events, with options to 'clear' or 'add to search'. The main content area lists three 'Syslog Event' entries, each with a date of 6/25/10 at 11:07 AM. The first event has a search target name of '[Local]'. The second and third events have a search target name of 'SLM Server - Vienna'. Each event includes a message snippet and a 'details+' link. The third event also has a 'get raw data' link.

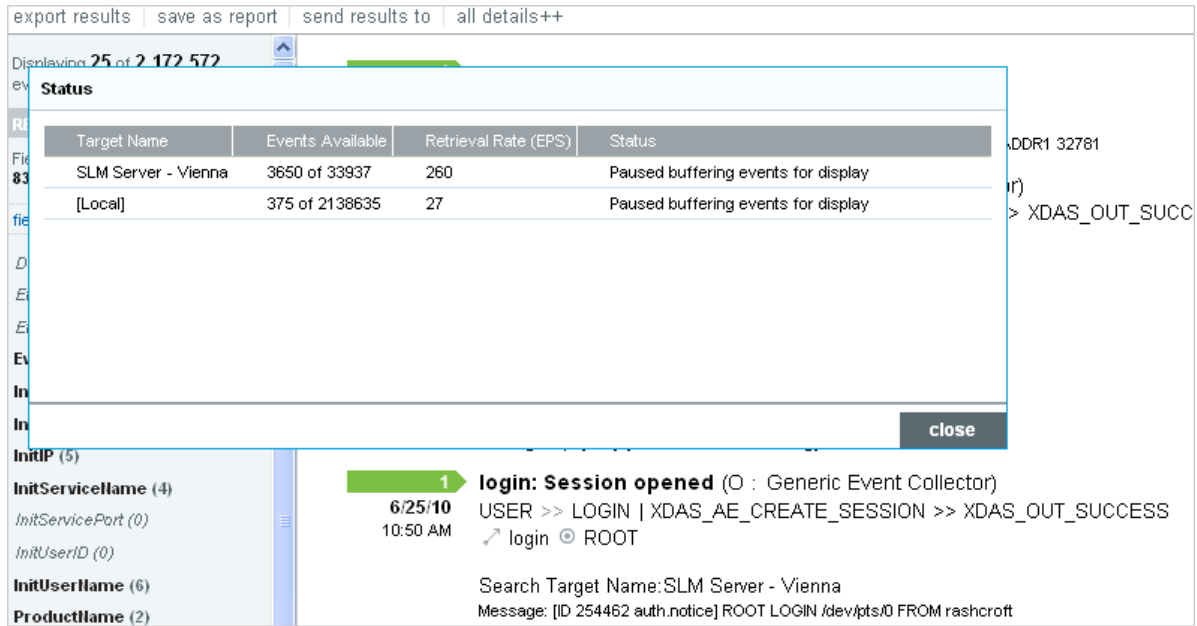
You can expand the event results to see the details by clicking the *details++* link.

For non-internal events, the *get raw data* link is displayed. You can view the raw data only if your role's security filter is set to View all data.

NOTE: For search results that come from the target servers, the role that is used to retrieve raw data is not the role of the logged-in user that is performing the search on the search initiator server, but the role that is assigned to the search initiator server on the target server.

You can view the status of the search in the extended status page while a search is in progress as well as when the search has finished. To access the extended status page, click the *Displaying N of M events from X targets* link that appears at the top of the refinement panel.

Figure 7-3 Extended Status Page



The extended status page displays the following information:

- ◆ **Target Name:** The descriptive name of the target server. If you did not specify a descriptive name for the target server, this field displays the IP address or DNS name of the target server.
- ◆ **Events Available:** Indicates the number of events that have actually been retrieved from the target server. The value is displayed as N of M events available, where N is the number of events that have been retrieved so far and M is the total number of events on the target server that match the search criteria.
- ◆ **Retrieval Rate (EPS):** An approximate rate of how fast the events were retrieved from a specific target server.
- ◆ **Status:** Displays the error messages, if any (generally in red). In addition to error messages, this field also displays the status of the search.
 - ◆ **Running:** Indicates that the search is still running on the search target server.
 - ◆ **Buffering events for display:** Indicates that the search is finished on the target server, but the search initiator server is retrieving events from the target server and buffering them for display.
 - ◆ **Paused buffering events for display:** Indicates that the search is finished on the target server, and the search initiator has paused while retrieving events from the search target. The search initiator reads ahead a few pages from the last page the you scrolled down. When it has buffered enough pages ahead, it pauses so that events are not buffered unnecessarily.
 - ◆ **Searching, paused buffering events for display:** This is similar to pausing and buffering events for display, except that the search is not yet completed on the target server.
 - ◆ **Done buffering:** Indicates that the search is completed on the target server, and all of the results are retrieved by the search initiator and queued for display.

You can further refine the distributed search results and perform various actions based on your requirement. For more information, see [Chapter 5, "Searching Events," on page 77](#).

7.5 Viewing the Search Activities

You can view the search activities that are being done on the target server by the search initiator server. You can see what queries are being done and how frequently they are being done. Based on the search activity, you might want to assign a more/less restrictive proxy role or even disable the access to the target server.

You can also refine the search activity query. For example, you can change the date range to see what queries have been performed today or yesterday or in the last hour, or you can drill down to see the queries that were made by particular users on the search initiator.

- 1 Log in to the target server as an administrator.
- 2 Click *search setup > Search Targets*.
- 3 Select the *Authorized Searcher Initiators* tab.

A list of search initiator servers are displayed under the Authorized Search Initiators list.

- 4 Click the *Search Activities* link for the search initiator server for which you want to view the search activities.

The screenshot shows a search interface with a search bar containing the query: `ext: "EventSearch" AND st: "A" AND dun: "SRCH-SRVR=[326D0840-5D51-102D-87BF-001E0B281DA9]"`. Below the search bar, there are options for 'last 7 days', 'include system events', and 'targets(1)'. The main area displays a list of search events. Two events are visible:

- Event 1:** Date: 6/24/10, Time: 2:39 PM. User: admin. Source IP: 10.0.0.2. Event Type: EventSearch (Sentinel : Internal). Details: XDAS_AE_QUERY_DATA_ITEM_CONTENTS >> XDAS_OUT_UNKNOWN. Message: Search Started: FROM=6/24/10 2:07 AM, TO=6/24/10 3:07 AM, MAX-EVENTS=50,000, QUERY-EXPRESSION=[(sev:[0 TO 5]) NOT st:"" NOT st:"A" NOT st:"P"], SECURITY-FILTER=[<empty>], TAGS-FILTER=[<empt ...]
- Event 2:** Date: 6/22/10, Time: 5:16 PM. User: admin. Source IP: 10.0.0.2. Event Type: EventSearch (Sentinel : Internal). Details: XDAS_AE_QUERY_DATA_ITEM_CONTENTS >> XDAS_OUT_UNKNOWN. Message: Search Started: FROM=6/22/10 12:00 AM, TO=6/22/10 5:44 AM, MAX-EVENTS=1,000,000, QUERY-EXPRESSION=[sev:[0 TO 5]], SECURITY-FILTER=[<empty>], TAGS-FILTER=[<empty>], INTERNAL-EVENT-FILTER=[<emp ...]

The search activities page is displayed that lists the audit events that are retrieved from all of the distributed search requests the target server has received from that particular search initiator.

7.6 Running Reports

Running reports in a distributed environment is similar to running reports on your local server, except that you select the target servers from which you want view the reports while specifying the report parameters.

- 1 Log in to the search initiator as a user with Search Remote Targets permission.
- 2 From the Reports section, select the report you want to run, then click *Run*.

The Run Report page is displayed.

3 Click the link for *Targets*.

A page is displayed that lists the target servers that you have added, including the local server. The target servers that are disabled are also displayed, but they are dimmed.

4 Select the target servers from which you want to view the reports, then click OK.

5 Specify the other parameters for the report.

For more information on these parameters, see [Section 6.1, “Running Reports,” on page 93](#).

6 Click *Run*.

A report results entry is created and listed under the selected report. For more information on managing reports, see [Chapter 6, “Reporting,” on page 93](#).

7.7 Managing the Distributed Setup Configuration

- ♦ [Section 7.7.1, “Editing the Search Target Server Details,” on page 122](#)
- ♦ [Section 7.7.2, “Disabling or Deleting a Search Target Server,” on page 122](#)
- ♦ [Section 7.7.3, “Editing the Search Initiator Server Details,” on page 123](#)
- ♦ [Section 7.7.4, “Disabling or Deleting a Search Initiator Server,” on page 124](#)

7.7.1 Editing the Search Target Server Details

- 1 Log in to the search initiator as an administrator.
- 2 Click *search setup > Search Targets*.
A list of search target servers is displayed under the Search Targets list.
- 3 Click the *Edit* link for the search target server for which you want to modify the details.
- 4 Edit the information.

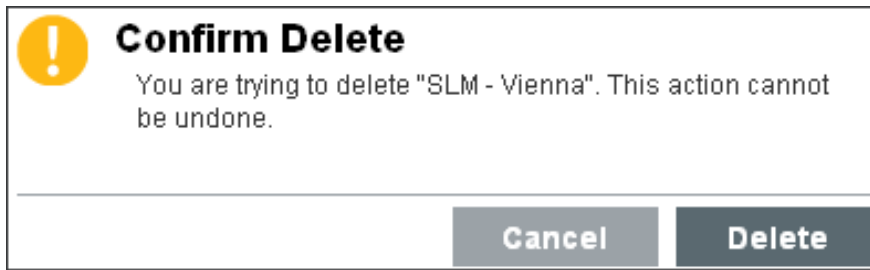
Do not change the IP address unless the IP address of the search target server has actually changed. The *Edit* page is not intended to allow you to change this target server entry to be a different search target server. To add a new target server, see [Section 7.2.2, “Adding a Search Target Server by Using the Administrator Credentials,” on page 112](#). If you accidentally change the IP address or DNS name to a different server, change it back to the correct server, else authentication of search requests will fail.

The screenshot shows a web interface for editing search target server details. At the top, there are two tabs: 'Search Targets' (selected) and 'Authorized Search Initiators'. Below the tabs, the title 'Edit SLM Server - Vienna' is displayed. The form contains four fields: 'Name:*' with the value 'SLM Server - Vienna', 'IP Address/DNS Name:*' with the value '10.0.0.1', 'Port:*' with the value '8443', and 'Search Proxy Role:*' with a blue link 'View/Change'. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

- 5 (Optional) To change the proxy role on the target server as necessary:
 - 5a Click *View/Change*.
 - 5b Log in to the target server.
 - 5c Select a proxy role, then click *OK*.
- 6 Click *Save*.

7.7.2 Disabling or Deleting a Search Target Server

- 1 Log in to the search initiator server as an administrator.
- 2 Click the *search setup > Search Targets*.
A list of target servers is displayed under the Search Targets list.
- 3 To disable searching events on the target server, deselect the *Enabled* check box next to the server you want to disable as a search target.
- 4 To delete a server from the list, click the *Delete* link for the target server that you want to delete.
A message is displayed to confirm whether you want to delete the selected configuration.



- 5 Click *Delete* to confirm deletion.

7.7.3 Editing the Search Initiator Server Details

- 1 Log in to the target server as an administrator.
- 2 Click the *search setup* tab.
- 3 Select the *Authorized Search Initiators* tab.
A list of authorized search initiators is displayed.
- 4 Click the *Edit* link for the target server for which you want to modify the details.
- 5 Edit the information.

Search Targets		Authorized Search Initiators
Edit SLM Server - Provo		
Authorized Search Initiator Name:*	<input type="text" value="SLM Server - Provo"/>	
IP Address/DNS Name:*	<input type="text" value="10.0.0.2"/>	
Port:*	<input type="text" value="8443"/>	
Search Proxy Role:*	Users	
Note: Showing only roles that have distributed search proxy as role permission.		
	Role Name	Description
<input checked="" type="checkbox"/>	Users	This role represents general users on an SLM system
		<input type="button" value="Cancel"/> <input type="button" value="Save"/>

- 6 Click *Save*.

7.7.4 Disabling or Deleting a Search Initiator Server

- 1 Log in to the target server as an administrator.
- 2 Click the *search setup* tab.
- 3 Select the *Authorized Searcher Initiators* tab.
A list of authorized search initiators is displayed.
- 4 Click the *Delete* link for the search initiator that you want to delete.
A message is displayed to confirm whether you want to delete the selected configuration.
- 5 Click *Delete* to confirm deletion.

7.8 Troubleshooting

You can perform some basic troubleshooting to ensure that you have successfully configured the search initiator for distributed search. This section lists the most common issues and the probable causes for these issues.

- ♦ [Section 7.8.1, “Permission Denied,” on page 124](#)
- ♦ [Section 7.8.2, “Connection Down,” on page 124](#)
- ♦ [Section 7.8.3, “Unable to View Raw Data,” on page 125](#)
- ♦ [Section 7.8.4, “Problems Adding Search Target,” on page 125](#)
- ♦ [Section 7.8.5, “Certain Events Are Only Visible from the Local System,” on page 125](#)
- ♦ [Section 7.8.6, “Cannot Run Reports on the Target Servers,” on page 125](#)
- ♦ [Section 7.8.7, “Different Users Might Get Different Results,” on page 125](#)
- ♦ [Section 7.8.8, “Cannot Set the Admin Role as the Search Proxy Role,” on page 125](#)
- ♦ [Section 7.8.9, “Error Logs,” on page 125](#)

7.8.1 Permission Denied

After doing a distributed search, check the extended status page to view the search status. If the search is not successful, check the following possible causes:

- ♦ The target server administrator might have disabled distributed searching on the target server. To enable distributed search on the target server, see [Step 4 in “Authorizing a Search Initiator Server” on page 114](#).
- ♦ The target server administrator might have disabled the search initiator server for distributed searching. Ensure that the search initiator server is enabled in the target server. For more information, see [“Authorizing a Search Initiator Server” on page 114](#).
- ♦ The role that you used for connecting might not have the `Search Remote Targets` permission.

7.8.2 Connection Down

- ♦ Network issues in your organization.
- ♦ Sentinel Log Manager servers or Sentinel Log Manager services might be down.
- ♦ Connection time-out.
- ♦ The IP address or the port number of the target server has changed, but the search initiator configuration might not be updated.

7.8.3 Unable to View Raw Data

The Proxy group that is assigned to the search initiator might not have the `view all events` permission to view the raw data.

7.8.4 Problems Adding Search Target

The search initiator server and target server might not be communicating with each other. Ensure that the firewall and NAT are set up properly to allow communication in both directions. Ping both ways to test.

7.8.5 Certain Events Are Only Visible from the Local System

You might not be able to view the events from the target servers for one of the following reasons:

- ♦ The trial license might be expired. You must purchase an enterprise license to reactivate this feature to view the events from the target servers.
- ♦ The user who has logged in to the search initiator has one set of permissions on the local data such as `view all data`, `view system events`, `security filter settings`, and so on. The search proxy group has another set of permissions, possibly more restrictive. Therefore, certain types of data, such as raw data, system events, and PCI events might only be returned from the local system and not the target server.

7.8.6 Cannot Run Reports on the Target Servers

The trial license might be expired. You must purchase an enterprise license to reactivate this feature to run the reports from the target servers.

7.8.7 Different Users Might Get Different Results

Different users might have different security filters or other permissions and therefore get different results from a distributed search.

7.8.8 Cannot Set the Admin Role as the Search Proxy Role

This is by design, for security reasons. Because the data viewing rights for the admin are unrestricted, it is not desirable to allow the admin role as the search proxy role.

7.8.9 Error Logs

You can also determine the cause of the search failure by examining the log files on the search initiator server, particularly in the `tomcat0.0` log file. For example, one of the following messages might have been logged:

```
Invalid console host name 10.0.0.1
Error sending target request to console host 10.0.0.1
Error getting certificate for console host 10.0.0.1
Authentication credentials in request to opt-in to console 10.0.0.2 were rejected
Request to opt-in to console 10.0.0.2 was not authorized
```

Error sending target request to console host 10.0.0.1

8 Configuring Tags

The Tags feature of Sentinel Log Manager allows you to tag all data collection objects such as event sources, event source servers, Collector Managers, Collector plug-ins, report templates, and report results. This feature is useful because tags help you to filter object lists for the data collection objects and also to augment incoming data. Tags are user defined values, that can be used to logically group data collection objects within the Sentinel Log Manager system. You can search for events, report templates and report definitions based on tags.

- ♦ [Section 8.1, “Overview,” on page 127](#)
- ♦ [Section 8.2, “Creating a Tag,” on page 129](#)
- ♦ [Section 8.3, “Managing Tags,” on page 129](#)
- ♦ [Section 8.4, “Performing Text Refined Searches,” on page 131](#)
- ♦ [Section 8.5, “Deleting Tags,” on page 132](#)
- ♦ [Section 8.6, “Associating Tags with Different Objects,” on page 133](#)
- ♦ [Section 8.7, “Searching Tagged Events,” on page 136](#)

8.1 Overview

You can create and delete tags and associate them with different objects in the system. Each tag may be associated with one or more data collection objects. Tags can be added as field to all incoming data and can be used to filter data.

You can associate more than one object with a tag. Similarly, an object can also be associated with more than one tags. You can, for example, create tags related to regulations (PCI) or compromised systems or network infrastructure such as routers, switches, and firewalls. Some organizations have to define data retention or data viewing policies based on the geographic location, so tags can be used to tag event sources based on different locations.

The Tags UI provides you with options to add and remove tags, maintain a list of favorites, and search tagged events. You can perform text-refined searches to find the tags that you are looking for. Sentinel Log Manager also allows you to search for events, report definitions and report templates that are tagged with a particular tag.

When ESM objects such as event sources, event servers, Collector Managers, or Collector plug-ins are tagged, all the events from those ESM objects are tagged with that value. The tag value is placed in a reserved variable `rv145`. However, event generated before tagging of the ESM objects are not tagged. Sentinel Log Manager does not perform retroactive tagging of data that is already stored because it is not an accepted practice to modify the events that are already stored.

Sentinel Log Manager comes with some default tags. For more information on default tags, see [Table 8-1 on page 128](#). You can either use default tags or create new tags, based on your requirements. For more information on creating new tags, see [Section 8.2, “Creating a Tag,” on page 129](#).

Table 8-1 *Default Tags*

Tag Name	Description
APP	Tag for general application or service not in other category.
AV	Tag for data related to the antivirus.
CreatedDuringEval	Tag to identify report results that do not include event details that exceed 25 EPS on systems running with the free license.
CM	Tag for configuration management related data.
DB	Tag for data related to database.
FISMA	Tag for data related to the Federal Information Security Management Act (FISMA) regulation.
FW	Tag for data related to network firewall.
GLBA	Tag for data related to the Gramm Leach Bliley Act (GLBA) regulation.
HIPAA	Tag for data related to the The Health Insurance Portability and Accountability Act (HIPAA) regulation.
IDM	Tag for data related to identity management.
IDS	Tag for data related to Intrusion Detection/Prevention System.
ISO/IEC_27002:2005	Tag for data related to the ISO/IEC_27002:2005 regulation.
JSOX	Tag for data related to the JSOX (the Financial Instruments Exchange Law, commonly referred to as JSOX, which is applicable to companies that are publicly registered on the Japanese stock exchanges) regulation.
NERC	Tag for data related to the North American Electric Reliability Corporation (NERC) regulation.
NETD	Tag for data related to network router/switch.
Network	Tag for network infrastructure related data, such as that obtained from routers, switches, and virtual private network (VPN).
Network Security	Tag for network security infrastructure data, such as that obtained from firewalls, IDSs, and Web proxies.
NISPOM	Tag for data related to the National Industrial Security Program Operating Manual (NISPOM) regulation.
O	Tag for event sources not in the other category.
OS	Tag for data related to the operating system.
OverEPSLimit	Tag for events that are received when the system running on free license averages more than 25 EPS. This is a system tag and cannot be deleted.
PCI	Tag for data related to the PCI regulation.
SentinelLogManager	Tag for Sentinel Log Manager system related data. This is a system tag and cannot be deleted.
SOX	Tag for data related to the Sarbanes–Oxley Act (SOX) regulation.
VPN	Tag for data related to virtual private network.
Windows	Tag for Windows related data

8.2 Creating a Tag

- 1 Log in to Sentinel Log Manager.
- 2 Select *Tags* in the left-hand pane.

The Tag display panel is displayed.



- 3 Click *Create* to add a tag.

The Create Tag window is displayed.



- 4 Specify a name for the tag. This is a mandatory field.

Tags have the following naming conventions and you are warned if the name you are specifying does not comply with these conventions:

- ♦ Tag names should not be more than 20 characters.
- ♦ There should not be any white space as part of the tag name.
- ♦ Tag name is case-insensitive. You cannot create two tags with identical names except for capitalization. For example, you cannot have two tag names IDM and idm, because both are perceived as same names.
- ♦ Articles such as a and the cannot be tag names.

- 5 Specify a description for the tag. This is an optional field.

If the tag name is available, a message is displayed.

If a tag with the same name already exists, then you are informed of the same so that you can create a tag with a different name.

- 6 Click *Save*.

8.3 Managing Tags



You can sort, search, or find tags by using the UI. This section has the following information:

- ♦ [Section 8.3.1, “Using the Tag Selector Widget,” on page 130](#)
- ♦ [Section 8.3.2, “Sorting Tags,” on page 130](#)

- ♦ [Section 8.3.3, “Adding and Removing Tags from Favorites,”](#) on page 130
- ♦ [Section 8.3.4, “Viewing and Modifying Tag Description,”](#) on page 130

8.3.1 Using the Tag Selector Widget

The tag widgets are an useful feature, which allows you to quickly add tags to data collection, object, reports and report templates or search for events with a particular tag.

- ♦ To tag reports and report templates with a particular tag, click the  icon, then select the name of the tag from the dialog box that opens.
- ♦ To search events with a particular tag, click the  icon next to the Search field, then select the tags from the dialog box that opens.

8.3.2 Sorting Tags

You can sort tags either based on their names or based on the number of objects associated with the tags. To sort tags:

- 1 Log in to Sentinel Log Manager.
- 2 Select *Tags* in the left-pane.
- 3 Select *Sort by Name* in the drop-down list, to sort the tags in the alphabetical order, based on the tag name,
- 4 Select *Sort by Count* in the *More* drop-down list, to sort based on the number of objects associated with them.
- 5 Click *OK*.

8.3.3 Adding and Removing Tags from Favorites

You can add the frequently used tags to the Favorites section so that it is easier to locate them and associate them with objects. When a tag is added to the Favorite section, it is removed from the Other section.

To add a tag to the Favorites section:

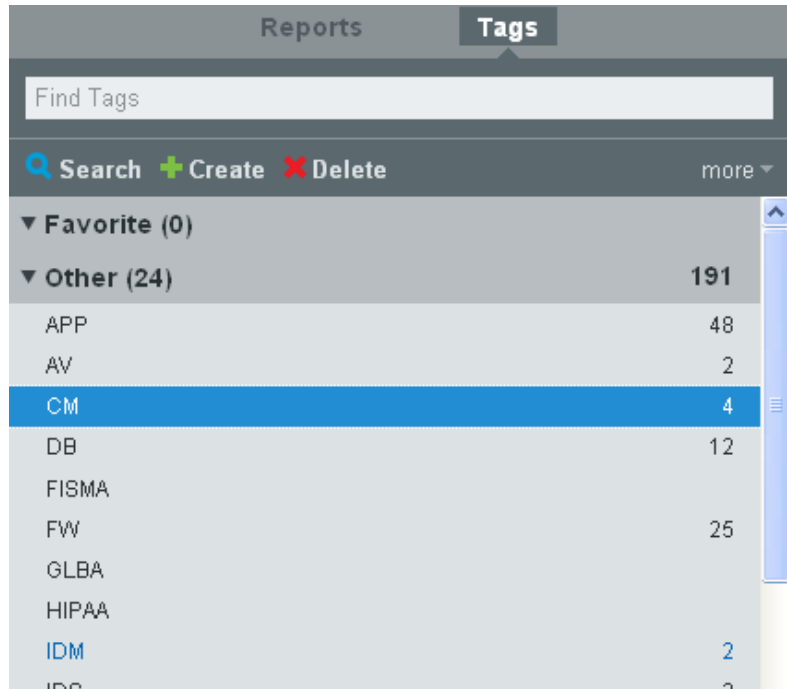
- 1 Log in to Sentinel Log Manager.
- 2 Select *Tags* in the left-hand pane.
- 3 To add a tag to the Favorites section, select the tag, then select *Add to Favorites* from the *More* drop-down list.
The selected tag is displayed in the Favorites section.
- 4 To delete a tag from the Favorites section, select the tag, then select *Remove From Favorites* from the *More* drop-down list.

8.3.4 Viewing and Modifying Tag Description

You can modify the description of a tag that is already created and tagged to data collection objects.

- 1 Log in to Sentinel Log Manager.
- 2 Select *Tags* in the left-hand pane.

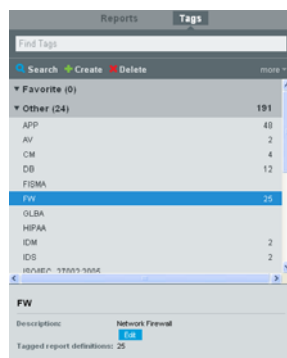
All the available tags are displayed.



The number against each tag indicates the number of data collection objects, reports and report templates associated with the tag.

- 3 Select the tag whose description you want to view or modify.

The tag details are displayed.



- 4 Click *Edit*.
- 5 Modify the description, then click *Save*.

8.4 Performing Text Refined Searches

This option is useful when there are more than one tag and you want to look for a particular tag.

- 1 Log in to Sentinel Log Manager.
- 2 Select *Tags* in the left pane.

- 3 To search for a particular tag, specify the name or description of the tag or a keyword.
The tag that matches the keyword is displayed.

8.5 Deleting Tags

- ♦ [Section 8.5.1, “Deleting a Tag,” on page 132](#)
- ♦ [Section 8.5.2, “Deleting Multiple Tags,” on page 132](#)

8.5.1 Deleting a Tag

- 1 Log in to Sentinel Log Manager.
- 2 Select *Tags* in the left-hand pane.
- 3 Select the tag that you want to delete.
- 4 Click *Delete*.
- 5 Click *Delete* when prompted to confirm deletion.

8.5.2 Deleting Multiple Tags

- 1 Log in to Sentinel Log Manager.
- 2 Select *Tags* in the left-hand pane.
- 3 Select *Multiple Tags* in the *More* drop-down list.



- 4 To select all the tags to be deleted, click *Select All*. To select individual tags, select the check box next to the tags to be delete.
- 5 Click *Delete*.
- 6 Click *Delete* when prompted to confirm deletion.

8.6 Associating Tags with Different Objects

You can associate tags with event sources, event source servers, Collector Managers, Collector Plug-ins, and reports and report templates. You can add more than one tag to a data collection object. However, the `rv145` field, which stores the tag value, can hold a maximum of 256 characters. Therefore, the maximum number of tags that you can associate with an object depends on the length of the tag name.

This section has the following information:

- ◆ Section 8.6.1, “Associating Tags with Event Sources,” on page 133
- ◆ Section 8.6.2, “Associating Tags with Event Sources Servers,” on page 133
- ◆ Section 8.6.3, “Associating Tags with Collector Managers,” on page 134
- ◆ Section 8.6.4, “Associating Tags with Collector Plug-ins,” on page 135
- ◆ Section 8.6.5, “Associating Tags with Reports Results and Report Definition,” on page 135

8.6.1 Associating Tags with Event Sources

- 1 Log in to Sentinel Log Manager.
- 2 Select *Collection*.
- 3 Select *Event Sources*.
- 4 Select one or more of the Event Sources that you want to associate with the tag.



- 5 Select the Configure icon.
- 6 Click *Tags*.

The Set Tag to Event Source dialog box is displayed.

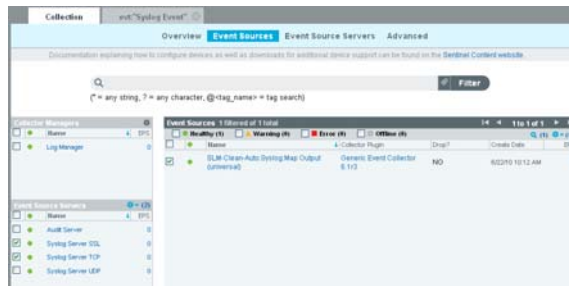


- 7 Select one or more of the tags that you want the selected event source to be associated with.
- 8 Click *Set*.

8.6.2 Associating Tags with Event Sources Servers

- 1 Log in to Sentinel Log Manager.
- 2 Select *Collection*.
- 3 Select *Event Source Servers*.

- From the Event Source Server section, select one or more of the Event Source servers that you want to associate with the tag.



- Select the Configure icon.
- Select *Tags*.
The Set Tag to Event Source Servers dialog box is displayed.
- Select one or more of the tags that you want the selected event source to be associated with.
- Click *Set*.

8.6.3 Associating Tags with Collector Managers

- Log in to Sentinel Log Manager.
- Select *Collection*.
- Select *Event Sources*.
- From the Collector Managers section, select one or more of the Collector Managers that you want to associate with the tag.



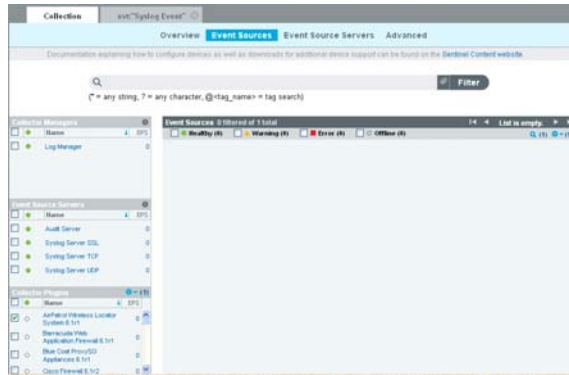
- Select the Configure icon.



- Select *Tags*.
The Set Tag to Collector Managers dialog box is displayed.
- Select one or more of the tags that you want the selected Collector Managers to be associated with.
- Click *Set*.

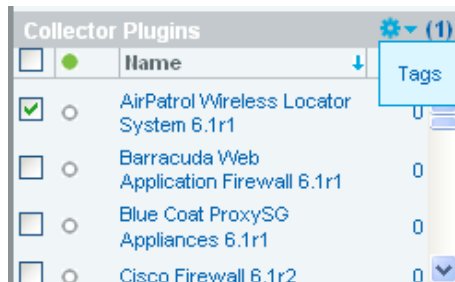
8.6.4 Associating Tags with Collector Plug-ins

- 1 Log in to Sentinel Log Manager.
- 2 Select *Collection*.
- 3 Select *Event Sources*.
- 4 From the Collector Plugins section, select one or more of the Collector plug-ins that you want to associate with the tag.



- 5 Select the Configure icon.
- 6 Select *Tags*.

The Set Tag to Collector Plugins dialog box is displayed.



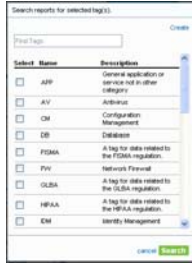
- 7 Select one or more of the tags that you want the selected Collector plug-ins to be associated with.
- 8 Click *Set*.

8.6.5 Associating Tags with Reports Results and Report Definition

NOTE: When a tag is set on a report definition, the report results under the report definition inherit the tag by default. Inherited tags for a report result appear disabled in the Tag selector dialog box.

- 1 Log in to Sentinel Log Manager.
- 2 Make sure you are in the *Reports* tab in the left pane.
- 3 Select the report result or the report definition that you want to associate with a tag.
- 4 Do one of the following:
 - ♦ Select *Tags* from the *more* drop-down list.
 - ♦ Click *Edit* at the bottom left pane.

The Tag selector dialog box is displayed.

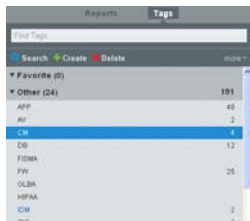



- 5 Select one or more of the tags that you want the selected report to be associated.
- 6 Select one or more of tags from the Tags section.
- 7 Click *Set*.

8.7 Searching Tagged Events

Sentinel Log Manager allows you to search for events that are tagged with a particular tag. You can search for tags by using any of the following methods, after logging in to the Sentinel Log Manager Web UI.

- ◆ Click *Tags*, then select a tag. Click *Search* to view all the data collection objects, reports and templates that are tagged with the selected tag.



- ◆ To find events tagged with a particular tag, click the  icon, then specify the name of the tag.
- ◆ To find events tagged with a particular tag specify `rv145:<tagname>` or `@<tagname>` as the search criteria, then click *Search*.

9 Configuring Rules and Actions

You can configure rules to evaluate and filter all incoming events and deliver selected events to designated output actions. For example, each severity 5 event can be e-mailed to a security analyst distribution list or to an administrator.

NOTE: This feature is a licensed feature. If the system is running with the free license, rules and actions do not get executed. For more information, see [Section 13.1, “Understanding the Licenses,”](#) on page 171.

This section describes the actions and rules that can be used to send events from Novell Sentinel Log Manager to another system.

- ♦ [Section 9.1, “Configuring Rules,”](#) on page 137
- ♦ [Section 9.2, “Configuring Actions,”](#) on page 140
- ♦ [Section 9.3, “Handling Auto-Created Event Sources without a Time Zone,”](#) on page 148
- ♦ [Section 9.4, “Forwarding the Events to Another Sentinel System,”](#) on page 150

9.1 Configuring Rules

You can configure rules to filter events based on one or more of the searchable fields. Each rule can be associated with one or more of the configured actions.

The rules are evaluated on a first-match basis in top-down order and the first matched rule is applied to the events that matches the filter criteria.

- ♦ [Section 9.1.1, “Adding a Rule,”](#) on page 137
- ♦ [Section 9.1.2, “Editing a Rule,”](#) on page 138
- ♦ [Section 9.1.3, “Ordering Rules,”](#) on page 138
- ♦ [Section 9.1.4, “Deleting a Rule,”](#) on page 139
- ♦ [Section 9.1.5, “Activating or Deactivating a Rule,”](#) on page 139

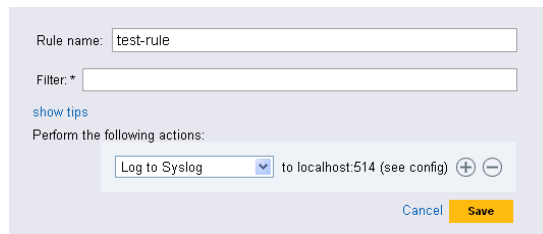
9.1.1 Adding a Rule

You can add a filter-based rule and then assign one or more configured actions that get executed to handle or output the events that meet the rule criteria.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *rules* in the upper left corner of the page.
The *Rules* tab is displayed on the right pane of the page.
- 3 Click *Add Rule*.
- 4 Specify a name for the rule.

- 5 Specify a filter value. The filter value can be the same value required to perform a search. The available operators depend on the data type of the event field. For example, match subnet is available for IP addresses, and match regex is available for text fields.



Click the *show tips* link to use the tag names defined in the table for defining rule filter. For example, to define a rule that applies to all events with a severity of 3 or 5 use *sev:[3 TO 5]*.



- 6 Select an action to be performed on every event that meets the filter criteria. The list of available actions in the drop-down list is determined by the defined actions. Actions are created and configured individually.

For more information about how to add, modify, and delete actions, see [“Configuring Actions” on page 140](#).

For each selected action, information is displayed to indicate where this action will send events. The information comes from the configuration details for the action.

- 7 Click  icon to select additional actions to be performed.
- 8 Click  to remove the selected action for this rule.
- 9 Click *Save* to save the rule.

The newly created rule appears at the end of rule list under the *Rules* tab. By default, this new rule is active.

9.1.2 Editing a Rule

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *rules* in the upper left corner of the page.
- 3 The *Rules* tab is displayed on the right pane of the page.
The created rules appear on the page.
- 4 Click the *edit* link next to the rule to change a rule definition.
- 5 Click *Save* to save the settings.

If the rules settings are changed, a *Successfully Saved Rule* message is displayed.

9.1.3 Ordering Rules

When there is more than one rule, the rules can be reordered by using drag-and-drop. Events are evaluated by rules in the specified order until a match is made, so you should order rules accordingly. More narrowly defined rules and more important rules should be placed at the beginning of the list.

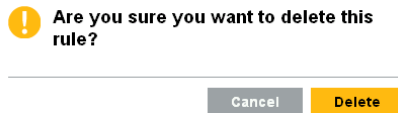
- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *rules* in the upper left corner of the page.
- 3 The *Rules* tab is displayed on the right pane of the page.

Existing rules appear on the page.

- 4 Mouse over the icon to the left of the rule numbering to enable drag-and-drop. The cursor changes.
- 5 Drag and drop the rule to the correct place in the ordered list.
If the rules are ordered, a `Successfully Moved Rule` message is displayed.
If the rules are not ordered, a `Reordering rules failed` message is displayed.

9.1.4 Deleting a Rule

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *rules* in the upper left corner of the page.
- 3 The *Rules* tab is displayed on the right pane of the page.
Existing rules appear on the page.
- 4 Click the *remove* link next to the rule to delete a rule definition.
- 5 The following confirmation message is displayed:



- 6 Click *Delete* to delete the selected rule.
If the rule is deleted, a `Successfully Deleted Rule` message is displayed.

9.1.5 Activating or Deactivating a Rule

New rules are activated by default. If you deactivate a rule, incoming events are no longer evaluated according to that rule. If there are already events in queue for one or more actions, it might take some time to clear the queue after the rule is deactivated. If the *On* check box beside the rule is selected, it indicates that the rule is activated. If the *On* check box is not selected, then it indicates that the rule is deactivated.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *rules* in the upper left corner of the page.
- 3 The *Rules* tab is displayed on the right pane of the page.
Existing rules appear on the page.
- 4 To activate the rule, select the check box next to each rule, in a column headed *On*.
If the rule is activated, a `Successfully activated the rule` message is displayed.
- 5 To deactivate the rule, select the check box next to each rule, in a column headed *On*.
If the rule is deactivated, a `Successfully deactivated the rule` message is displayed.

9.2 Configuring Actions

You can configure actions to deliver an event to one or more actions when it meets the criteria specified by one of the rules. An incoming event is evaluated against each filtering rule in the specified order until a match is found, then the delivery actions associated with that rule are executed. Actions are added, deleted, and modified independent of the rules that use them. However, an action that is associated with one or more rules cannot be deleted.

NOTE: Events are processed by the associated actions one at a time. You should therefore consider performance implications when selecting the output action to which events are sent. For example, the Log to File action is the least resource-intensive, so it can be used to test rule criteria to determine the data volume before sending a flood of events to e-mail or syslog.

Also, when you set up the Send to e-mail action, you should consider how many events the recipient can effectively handle, and adjust the filtering on the rule accordingly.

Event output is in JavaScript Object Notation (JSON) format, which is a lightweight data exchange format. Events consist of field names (such as `evt` for Event Name) followed by a colon and a value (such as "Start"), separated by commas.

For example:

```
{ "st": "I", "evt": "Start", "sev": "1", "sres": "Collector", "res": "CollectorManager", "rv99": "0", "rv1": "0", "repassetid": "0", "rv77": "0", "agent": "Novell SecureLogin", "obsassetid": "0", "vul": "0", "port": "Novell SecureLogin", "msg": "Processing started for Collector Novell SecureLogin (ID D892E9F0-3CA7-102B-B5A1-005056C00005).", "dt": "1224204655689", "id": "751D97B0-7E13-112B-B933-000C29E8CEDE", "src": "D892E9F0-3CA7-102B-B5A2-005056C00004" }
```

You can add multiple actions and then associate these actions to the rules. The *Rules* column under the *Actions* tab displays the number of rules associated with each action.

You can configure one of the following action types:

Execute a Script: This action executes the specified command line executable on the Sentinel Log Manager server. The events are passed to it as a JSON encoded argument.

Log to File: This action writes the event to a specified file on a Sentinel Log Manager server.

Log to Syslog: This action forwards the event to a configured syslog server.

Send an E-mail This action sends the event to one or more user by using a configured SMTP relay. For example, a Send to Email action can be used to escalate specific events to notify a system administrator or Tier 2 analyst. It can also be used to forward events to an incident response system that accepts e-mail input.

Send SNMP Trap: This action sends the SNMP traps.

Send to Sentinel Link: This action uses Sentinel Link to forward events to another Sentinel Log Manager, Sentinel, or Sentinel RD system.

- ◆ [Section 9.2.1, “Executing a Script,” on page 141](#)
- ◆ [Section 9.2.2, “Logging the Events to a File,” on page 141](#)
- ◆ [Section 9.2.3, “Sending the Events to Syslog,” on page 142](#)
- ◆ [Section 9.2.4, “Sending the Events by an E-Mail,” on page 143](#)
- ◆ [Section 9.2.5, “Sending the SNMP Traps,” on page 144](#)
- ◆ [Section 9.2.6, “Sending the Events to a Sentinel Link,” on page 144](#)

- Section 9.2.7, “Modifying an Action,” on page 147
- Section 9.2.8, “Deleting an Action,” on page 148

9.2.1 Executing a Script

All Sentinel Log Manager events that meet the filter criteria for which the Execute a Script action is defined are passed as argument to the same script.

To configure the Execute a Script action, you need to specify the path of the script that will be executed. The script must already exist and the novell user must have permissions to execute it.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Select *rules > Actions*, then click *Add Action*.

Name	Rules	Actions
Execute Script	2	ec
Log to File	0	ec
Log to Syslog	0	ec
Send an email	1	ec
Send Events via Sentinel Link	1	ec
Send SNMP trap	0	ec

- 3 Select *Execute a Script*.
- 4 Specify an action name. Make sure that the action name is unique.

Execute Script

Action name:

Path:

- 5 Specify the path to the script that you want to be executed. Specify either an absolute path or a relative path, where the working directory is under the data directory of the application `$ESEC_DATA_HOME/data/`. For example, `/var/opt/novell/sentinel_log_mgr/data/`.
If required, click *Test* to test if script exists and novell user has the required permissions.
- 6 Click *Save*. If the action is configured, a *Successfully Added Action* message is displayed.

9.2.2 Logging the Events to a File

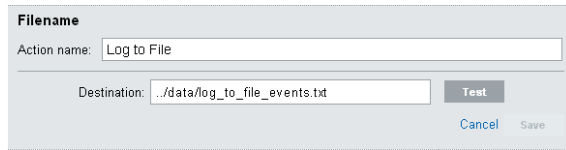
All Sentinel Log Manager events that meet the filter criteria for which the *Log to File* action is defined are written to the specified file.

To configure the *Log to File* action, you must know the name and path of the file onto which the events must be written. The directory should already exist and the novell user must have permissions to write to it. If the file does not already exist, Sentinel Log Manager creates it.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Select *rules > Actions*, then click *Add Action*.

3 Select *Log to File*.

The *Filename* dialog box appears.



4 Specify the following information:

- ◆ **Action Name:** Specify a name for the action. Make sure that the action name is unique.
- ◆ **Destination:** Specify the path to the file to which you want the events to be written. Specify either an absolute path or a relative path, where the working directory is under the data directory of the application `$ESEC_DATA_HOME/data/`. For example, `/var/opt/novell/sentinel_log_mgr/data/`.
- ◆ **Test:** (Optional) Click *Test* to test permissions and create a zero-byte file to hold the data

5 Click *Save*. If the action is configured, a `Successfully Added Action` message is displayed.

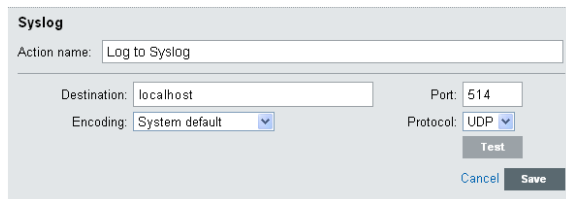
9.2.3 Sending the Events to Syslog

All Sentinel Log Manager events that meet the filter criteria for which the *Send to Syslog* action is defined are sent to the specified syslog server.

To configure the *Send to Syslog* action, you need the IP address and port number of the syslog server.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Select *rules > Actions*, then click *Add Action*.
- 3 Select the *Log to Syslog* action type.

The *Syslog* screen appears.



4 Specify the following information:

- ◆ **Action Name:** Specify an action name. Make sure that the action name is unique.
- ◆ **Destination:** Specify the hostname or IP address of the Syslog server.
- ◆ **Protocol:** Select the protocol used to connect to the Syslog server.
- ◆ **Port:** Specify the port number.
- ◆ **Encoding:** Select the encoding standard that the Syslog Integrator should use.
- ◆ **Test:** (Optional) Click *Test* to test if the destination server and port are specified correctly.

5 Click *Save*. If the action is configured, a `Successfully Added Action` message is displayed.

9.2.4 Sending the Events by an E-Mail

All Sentinel Log Manager events that meet the filter criteria for which the *Send an E-mail* action is defined are sent to the associated SMTP relay and e-mail addresses.

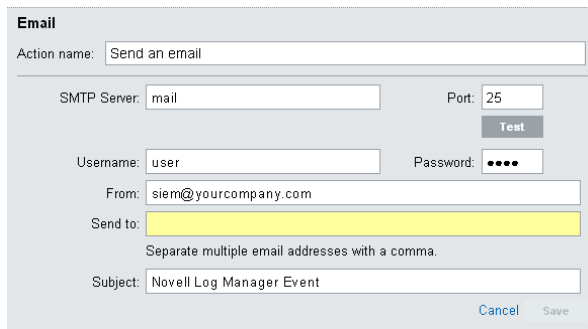
To configure the Send to e-mail action, you need the IP address and port number of an SMTP relay, and the To and From e-mail addresses. To send events to more than one e-mail addresses, use a comma-separated list.

NOTE: To avoid overwhelming your SMTP relay or e-mail recipients, this action should only be used with rules that generate a low volume of events.

This SMTP relay configuration is also used to deliver reports to users.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Select *rules > Actions*, then click *Add Action*.
- 3 Select the *Send an Email* action type.

The *Email* screen appears.



The screenshot shows the 'Email' configuration form. The 'Action name' field contains 'Send an email'. The 'SMTP Server' field contains 'mail' and the 'Port' field contains '25'. There is a 'Test' button next to the port field. The 'Username' field contains 'user' and the 'Password' field contains four dots. The 'From' field contains 'siem@yourcompany.com'. The 'Send to' field is highlighted in yellow and contains a yellowed-out address. Below the 'Send to' field is the text 'Separate multiple email addresses with a comma.' The 'Subject' field contains 'Novell Log Manager Event'. At the bottom right are 'Cancel' and 'Save' buttons.

- 4 Specify the following information:
 - ♦ **Action Name:** Specify an action name. Make sure that the action name is unique.
 - ♦ **SMTP Server:** Specify the hostname or IP address of an available SMTP server.
 - ♦ **Port:** Specify the port number of an available SMTP server.
 - ♦ **Port:** (Optional) Click *Test* to validate the hostname or IP address, port, username, and password fields.
 - ♦ **Username:** If the SMTP server requires authentication, specify a username.
 - ♦ **Password:** Specify the password for SMTP server.
 - ♦ **Send To:** Specify one or more e-mail addresses for recipients, separated by commas.
 - ♦ **From:** Specify an address from where the e-mail messages are sent.
 - ♦ **Subject:** Specify the subject line for the e-mail.
- 5 Click *Save*. If the action is configured, a *Successfully Added Action* message is displayed.

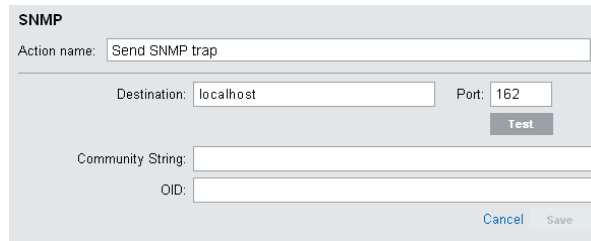
9.2.5 Sending the SNMP Traps

All Sentinel Log Manager events that meet the filter criteria for which the Send SNMP Traps action is defined are sent to the specified SNMP addresses.

To configure the Send SNMP Traps action, you need the connection information for an SNMP server, including the IP address and the port number.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Select *rules > Actions*, then click *Add Action*.
- 3 Select the Send SNMP Trap action type.

The *SNMP* screen appears.



- 4 Specify the following information:
 - ♦ **Action Name:** Specify an action name. Make sure that the action name is unique.
 - ♦ **Destination:** Specify the IP address or hostname of the SNMP server you want to send the trap.
 - ♦ **Port:** Specify the port number for the SNMP server. The default port is 162.
 - ♦ **Test:** (Optional) Click *Test* to validate the hostname or IP address and port number.
 - ♦ **Community String:** Specify the community string (password) to access the SNMP management system. If no community string is specified, the Integrator sets the default value to public.
 - ♦ **OID:** Specify the desired asnl object ID you want to associate with this message. If no Object ID is specified, the Novell Audit internal OID is used (2.16.840.1.113719.1.347.3.1).
- 5 Click *Save*. If the action is configured, a *Successfully Added Action* message is displayed.

9.2.6 Sending the Events to a Sentinel Link

Sentinel Link provides the ability to hierarchically link multiple Sentinel systems, including Sentinel Log Manager and the two Sentinel SIEM (Security Information Event Management) systems, Novell Sentinel and Novell Sentinel Rapid Deployment (RD) systems. Sentinel Link provides several benefits:

- ♦ Several Sentinel Log Managers can be linked in a hierarchical manner. Regional or distributed Sentinel Log Manager servers can manage a large volume of data, retaining raw data and event data locally, while also forwarding important events to a central Log Manager for consolidation.

- ♦ One or more Sentinel Log Managers can forward important data to either Sentinel or Sentinel RD, which are SIEM (Security Information Event Management) systems. These systems provide real-time visualization of data, advanced correlation and actions, workflow management, and integration with identity management systems.
- ♦ Sentinel Link must be configured in two locations: on the Sentinel Log Manager system that sends the data and on the Sentinel Log Manager, Sentinel, or Sentinel RD system that receives the data.

The following instructions describe how to configure the system sending the data:

- 1 Set up the Sentinel Link connection to receive messages from another Sentinel or Sentinel Log Management system.

For more information about configuring Sentinel systems for receiving events, see [Sentinel Link Solution Guide \(http://support.novell.com/products/sentinel/zip/utilities/Sentinel-Link_Solution.pdf\)](http://support.novell.com/products/sentinel/zip/utilities/Sentinel-Link_Solution.pdf).

- 2 Log in to the Sentinel Log Manager as an administrator.
- 3 Select *rules > Actions*, then click *Add Action*.
- 4 Select the Send to Sentinel Link action type.

The *Sentinel Link* screen appears.

- 5 Specify an action name. Make sure that the action name is unique.
- 6 Specify the IP address or hostname of the destination Sentinel system where a Sentinel Link Connector is configured.
- 7 Specify the port number for the sentinel system. The default port is 1290.
If required, click *Test* to validate the hostname or IP address and port fields.

8 Select one of the following:

- ◆ **Not Encrypted (HTTP):** Establish an unsecured connection.
- ◆ **Encrypted (HTTPS):** Establish a secured connection. If you select the encrypted (HTTPS) option, you are optionally allowed to specify a Server validation mode and an Integrator key pair.

Field	Description
<i>Server Validation Mode</i>	Select one of the following: <ul style="list-style-type: none">◆ None- no server certificate required: The Integrator does not validate the receiver's certificate.◆ Strict - server certificate required: The Integrator always verifies the receiver's certificate when connecting to the receiver. If this option is selected, the Integrator immediately attempt to retrieve the receiver's certificate over the network and validate that it is issued by an authorized CA. If the certificate is not validated for some reason, it is still presented to the user to accept or reject. The certificate is considered to be valid if the user accepts it. When a validated certificate is acquired, it is stored in the Integrator's configuration. Henceforth, the Integrator allows communication only with a receiver that provides that certificate during the initial connection setup.
<i>Integrator Key Pair</i>	Select one of the following: <ul style="list-style-type: none">◆ None - server does not require client certificate: The receiver system does not validate the sender certificates. Select this option if the receiver's client authentication type is configured to <i>Open</i>.◆ Custom - server validates (strict) client certificate: The receiver system validates the sender certificates. Select this option if the receiver's client authentication type is configured to <i>Strict</i>. If the receiver system performs a strict validation, it imports a trust store, which contains all the sender certificates that it trusts. After selecting this option, click the <i>Import Key Pair</i> button to import a key pair. The key pair you import must match one of the certificates that is included in the trust store, which is imported by the receiver system.

9 Select the *Send alerts if no events are received in specified time period* option to allow the sentinel link to generate alerts (internal events) that can be monitored by a system administrator.

These alerts are generated when the sentinel link has not received any events for a specified time period. The internal event type for this alert is `NoEventsReceived`.

If the *Send alerts if no events are received in specified time period* option is enabled, the user is allowed to specify the following two parameters:

- ◆ **Time period (minutes):** The time period is the number of minutes that must elapse without receiving an event before the sentinel link generates the `NoEventsReceived` alert.
 - ◆ **Repeat alerts interval (minutes):** The repeat alert interval is the number of minutes between repeating the `NoEventsReceived` alert. The alert is sent repeatedly at this interval until sentinel link starts receiving the events again.
- 10 In the *Maximum Event Queue Size (MB)* field, specify the maximum event queue size value in megabytes. The value must be between 0 and 2147483647.

The following options are enabled only when you specify a value in the *Maximum Event Queue Size (MB)* field.

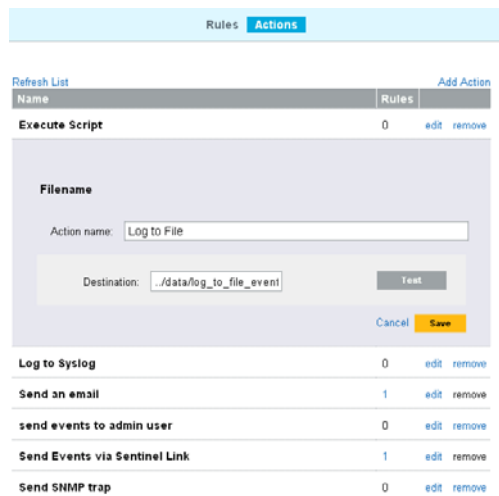
Drop OLDEST event when queue is full: Select this option to drop the oldest events in the event queue when the value specified in the *Maximum Event Queue Size (MB)* field exceeds the limit.

Drop NEWEST event when queue is full: Select this option to drop the newest events when the value specified in the *Maximum Event Queue Size (MB)* field exceeds the limit.

- 11 Select the *Send alerts if events are dropped* option to generate the alerts when the sentinel link drops the received events because its queue is full. The internal event type for this alert is `DroppedEvents`.
- 12 Specify the maximum data rate value in kilobytes per second. The value must be between 0 and 2147483647.
- 13 Select one of the following options to specify the Event Forwarding Mode:
 - Forward Events Immediately:** Select this option to forward the events immediately to the Sentinel system.
 - Scheduled Event Forwarding:** Select this option to schedule event forwarding. You can specify the *Time Of Day* and *Duration* (in minutes) for each day of the week. The valid format for the Time Of Day is *hh:[mm] [am | pm]*. The duration must be between 1 and 1440 minutes.
If you do not specify a time or the duration for any of the days of the week, the schedule is considered to be 24 hours a day, seven days a week. It would be equivalent to the *Forward Events Immediately* option.
 - Queue Events Only (do not forward):** Select this *option* to stop forwarding events to the destination Sentinel system. However, the integrator stores the events it receives in its queue unless the queue has a size limit and has reached its maximum capacity.
This mode is useful if the destination Sentinel is down for maintenance or any network problems persist in communicating with the Sentinel system that might not be fixed immediately. In such situations, rather than continually trying to forward events, you can select the *Queue Events Only (do not forward)* option to temporarily stop forwarding messages. After the problems are resolved, you can re-enable event forwarding by selecting the *Forward Events Immediately* or *Scheduled Events Forwarding* options.
- 14 Click *Save*. If the action is configured, a `Successfully Added Action` message is displayed.

9.2.7 Modifying an Action

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *rules* in the upper left corner of the page.
- 3 The *Rules > Actions*.
- 4 To change the action settings, click *edit* next to the action.



- 5 Edit the parameter values for the action.
- 6 Click *Save* to save the settings.

If the action settings are changed, a `Successfully Saved Action` message is displayed.

9.2.8 Deleting an Action

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *rules* in the upper left corner of the page.
- 3 The *Rules* tab is displayed on the right pane of the page.
- 4 Select the *Actions* tab.
- 5 To delete the selected action, click the *remove* link next to the action

NOTE: The *remove* link is only enabled if an action is not associated with a rule.

The following confirmation message is displayed.



- 6 Click *Delete* to delete the action.

If the action is deleted, a `Successfully Deleted Action` message is displayed.

The selected action is deleted from the configured action list.

9.3 Handling Auto-Created Event Sources without a Time Zone

When event sources are auto-created without a time zone, it is recommended that an administrator receives a notification so that a time zone can be manually assigned to the event sources, if necessary.

By default, Sentinel Log Manager is installed with a rule that sends an e-mail message when an event source is auto-created without a timezone. The rule is called `Event Source Created With Unspecified Timezone`.

This rule is triggered by the following conditions:

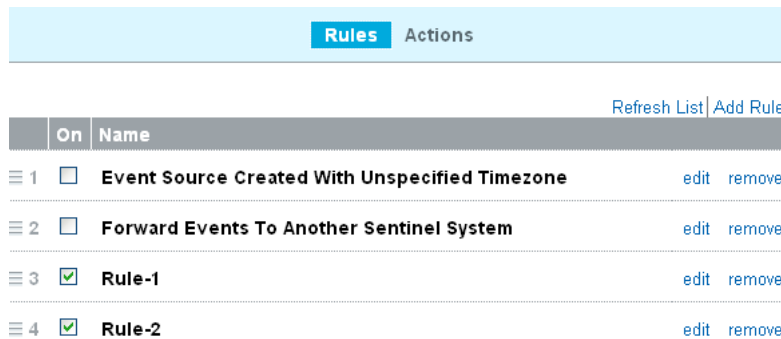
- ◆ EventName = CreateEventSource AND
- ◆ Message match regex .*EMPTYTZ\$

The Event Name is `CreateEventSource`. The Event Message indicates the name and universally unique identifier (UUID) of the newly created event source. If a new event source group or a new Collector is also created, their respective names and UUIDs are also indicated in the message. The message also indicates if any timezone was assigned to the event source when it was created. If the event source was created without a time zone, it shows the text `EMPTYTZ` at the end of the message.

When the defined conditions are met, an e-mail is sent to the configured e-mail address. The Event Source Created With Unspecified Timezone is already preconfigured to perform the Send E-Mail action. To send an e-mail, the rule must be activated, and the e-mail notification settings for *Send an email* action must be configured as follows:

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *rules*.
- 3 The *Rules* tab is displayed on the right pane of the page.

The Event Source Created With Unspecified Timezone rule is displayed under the *Rules* tab.



- 4 To activate the Event Source Created With Unspecified Timezone rule, select the check box next to the rule.

If the rule is activated a `Successfully activated the rule` message is displayed.

- 5 To modify the Send an email action to send an email for event sources created with unspecified time zone, click *Actions*.
- 6 Select the Send an Email action.

The *Email* screen appears.

Email

Action name:

SMTP Server: Port:

Username: Password:

From:

Send to:
Separate multiple email addresses with a comma.

Subject:

- 7 Specify the values for each field. For more information, see [Section 9.2.4, “Sending the Events by an E-Mail,”](#) on page 143.

9.4 Forwarding the Events to Another Sentinel System

Sentinel Log Manager is installed with a rule that forwards events to another Sentinel system. The rule is called Forward Events To Another Sentinel System. By default, the Forward Events To Another Sentinel System rule is configured to filter out internal system events and events with a severity that is less than four. This rule filters out the following three types of system events:

- ◆ Audit (A)
- ◆ Performance (P)
- ◆ Internal (I)

You can also change the conditions of the rule to filter more events or remove conditions to filter fewer events.

Novell recommends that you configure the rule to forward only those events that you want to store on the Sentinel system for more in-depth reporting and analysis.

The Forward Events To Another Sentinel System rule is installed with Log Manager, but it is in the inactive (off) state. To forward the system events to another Sentinel system, the rule must be activated, and the Sentinel Link Integrator settings must be configured. The Send to Sentinel Link settings configures the Sentinel Link Integrator instance that is pre-installed on Sentinel Log Manager, which must be configured.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *rules* in the upper left corner of the page.
- 3 The *Rules* tab is displayed on the right pane of the page.
The Forward Events To Another Sentinel System rule is displayed under the *Rules* tab.
- 4 To activate the Forward Events To Another Sentinel System rule, select the check box next to the rule.
If the rule is activated, a `Successfully activated the rule` message is displayed.
- 5 To configure the Sentinel Link Integrator settings, click *Actions*.
- 6 To configure the Send to Sentinel Link settings, refer to [“Sending the Events to a Sentinel Link” on page 144](#).

10 Configuring Users and Roles

This section describes the user and role administration feature of Sentinel Log Manager. You can add, edit and delete roles. You can also grant different permissions at the role level. You can edit the details of user and role profiles.

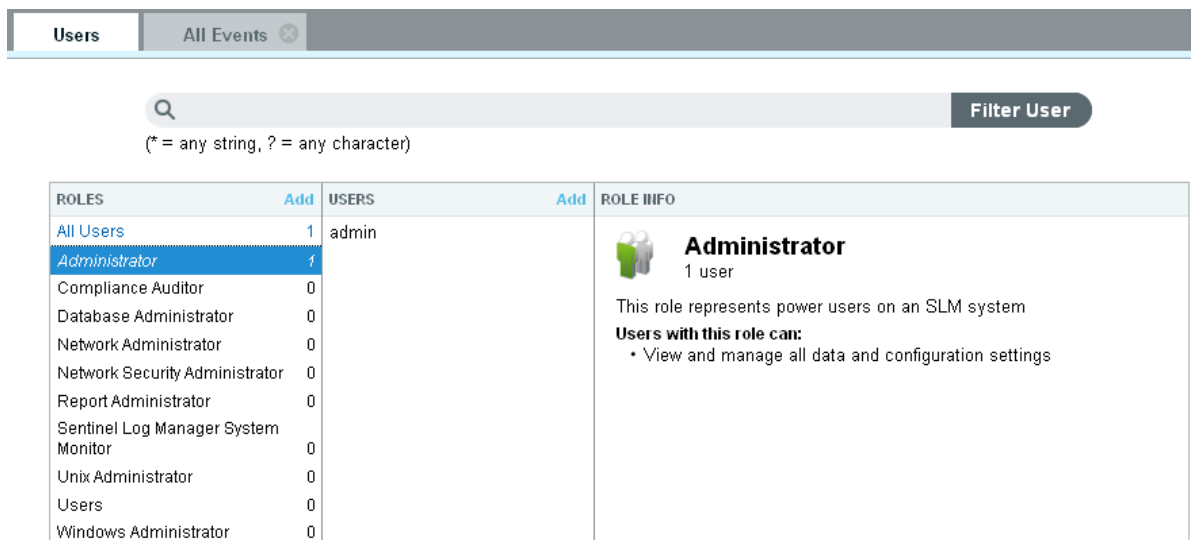
You can create roles, which can contain any number of users. Each role can be assigned a different set of permissions and the users of the role inherit the permissions of the role they are in.

- [Section 10.1, “Overview,” on page 151](#)
- [Section 10.2, “Creating Roles and Users,” on page 154](#)
- [Section 10.3, “Viewing Roles and User Details,” on page 156](#)
- [Section 10.4, “Viewing All Users,” on page 157](#)
- [Section 10.5, “Modifying Roles and Users,” on page 157](#)
- [Section 10.6, “Moving Users to Another Role,” on page 159](#)
- [Section 10.7, “Deleting Roles and Users,” on page 159](#)


10.1 Overview

You can create different users roles and assign them different permissions depending on their role. Each role can contain any number of users. Users belonging to a same role inherit the permissions of the role they belong to. You can set multiple permissions for a role.

Figure 10-1 Users and Roles configuration page



The screenshot displays the 'Users and Roles configuration page'. At the top, there are tabs for 'Users' and 'All Events'. Below the tabs is a search bar with a magnifying glass icon and a 'Filter User' button. The search bar contains the text '(* = any string, ? = any character)'. Below the search bar is a table with three columns: 'ROLES', 'USERS', and 'ROLE INFO'. The 'ROLES' column lists various roles, and the 'USERS' column shows the number of users for each role. The 'Administrator' role is highlighted in blue. The 'ROLE INFO' column provides details for the selected role, including a description and a list of permissions.

ROLES	Add	USERS	Add	ROLE INFO
All Users	1	admin		
Administrator	1			 Administrator 1 user This role represents power users on an SLM system Users with this role can: <ul style="list-style-type: none">• View and manage all data and configuration settings
Compliance Auditor	0			
Database Administrator	0			
Network Administrator	0			
Network Security Administrator	0			
Report Administrator	0			
Sentinel Log Manager System Monitor	0			
Unix Administrator	0			
Users	0			
Windows Administrator	0			

This section has the following information:

- ♦ [Section 10.1.1, “Default Roles,” on page 152](#)
- ♦ [Section 10.1.2, “Filtering Data,” on page 153](#)
- ♦ [Section 10.1.3, “Setting Permissions,” on page 153](#)

10.1.1 Default Roles

The Novell Sentinel Log Manager has the following roles by default:

Administrator: A user in this role has administrative rights in the Sentinel Log Manager system. You cannot delete the default admin user, but you can delete other users added to the Administrator role. Administrative rights include the ability to perform the user administration, data collection, data storage, rules and report management, search operations and license management.

You cannot modify or delete the Administrator role.

Compliance Auditor: A user in this role has access to view events that are tagged with at least one of the regulation related tags such as PCI, SOX, HIPAA, NERC, FISMA, GLBA, NISPOM, JSOX, and ISO/IEC_27002:2005, view system events, view the Sentinel Log Manager configuration data, and search remote targets.

Database Administrator: A user in this role has access to events coming from database event sources. The type of the event source (DB) is determined by the collector parsing the data from the event source. A user with this role can view data that matches filter `rv32 : "DB"` and search remote targets.

Network Administrator: A user in this role can administer network infrastructure devices, such as routers, switches, VPN, etc. A users in this role has access to events coming from devices in the category `NETD` or `VPN` (as determined by the Collector parsing the data) or from event sources with the `Network` tag. Set the `Network` tag on network infrastructure related event sources to allow users in this role to view the events. A users with this role can view data that matches filter `rv32 : "NETD" OR rv32 : "VPN" OR rv145 : "Network"` and search remote targets.

Network Security Administrator: A user in this role can administer network security infrastructure devices, such as firewalls, IDSs, and web proxies. A user in this role has access to events coming devices in the category `AV`, `FW`, or `IDS` (as determined by the Collector parsing the data) or from event sources with the `NetworkSecurity` tag. Set the `NetworkSecurity` tag on network infrastructure related event sources to allow users in this role to view the events. A user with this role can view data that matches filter `rv32 : "AV" OR rv32 : "FW" OR rv32 : "IDS" OR rv145 : "NetworkSecurity"` and search remote targets

Report Administrator: A user in this role has the ability to run reports, view, rename and delete report results, add and delete report templates and report results, run reports on configuration database, export all reports and save search result as report. A Report Administrator can also tag report templates and report results. The Report Administrator can search report templates and report results based on these tags.

Sentinel Log Manager System Monitor: A user in this role has the ability to monitor the Sentinel Log Manager system for errors or outages. A user in this role has access only to events coming from Sentinel Log Manager systems. A user in this role can also access data coming from event sources that the Sentinel Log Manager is dependent on. For example, you can tag operating systems on which the Sentinel Log Managers and Collector Managers are running on with a `SentinelLogManager` event source tag so that the users in this role can monitor problems with operating systems. A user with this role can view data that matches filter `rv145 : "SentinelLogManager"`, view system events and search remote targets.

Unix Administrator: A users in this role has access to events from operating system event sources that are not Windows machines. The type of the event source is determined by verifying the Collector parsing data and also by verifying if a Windows tag is present. A user in this role can view data that matches filter (rv32:"OS" NOT (("Microsoft?Active?Directory*" NOT msg:"Microsoft?Active?Directory*") OR ("Microsoft?Windows*" NOT msg:"Microsoft?Windows*"))) NOT rv145:"Windows" and search remote targets.

User: A user with this role has the ability to run reports, view, rename, and delete report results.

Windows Administrator: A user with this role can administer Windows machines. A users in this role has access to data generated by Windows event sources. The type of the event source is determined by verifying the Collector parsing the data. If data from a Windows event source is not being processed by the Active Directory or Windows collector, then add the Windows tag to event sources to indicate that Windows data is being collected from the event source. This enables the Windows Administrator to access the data. A user in this role can view data that matches filter (rv32:"OS" AND (("Microsoft?Active?Directory*" NOT msg:"Microsoft?Active?Directory*") OR ("Microsoft?Windows*" NOT msg:"Microsoft?Windows*"))) OR rv145:"Windows" and search remote targets.

10.1.2 Filtering Data

You can either allow a user to view all the events or view only the selected events:

- ◆ To allow a user to view all the events select the *View all Data* radio button.
- ◆ To allow users to view only selected data, then select the *View the following Data* radio button, the select one or more of the following options:
 - ◆ To allow a user to view events that match a filter, specify the Lucene search query in the text box. You can click the *Tips* link to understand how to construct valid Lucene search query. For example, if you set the filter value to `sev:5`, the user can view only events of severity five in a search.
 - ◆ To allow a user to view the Sentinel Log Manager configuration data, select *View Sentinel Log Manager configuration data*.
 - ◆ To allow a user to view system events, select *View System Events*.

10.1.3 Setting Permissions

You can assign the following permissions to the role:

- ◆ **Manage Reports:** When this permission is set on a role, all members of that role can run reports, view, rename and delete report results, add and delete report templates and results. For more information on reports, see [Chapter 6, "Reporting," on page 93](#).
- ◆ **Manage Tags:** When this permission is set on a role, all members of that role can create, delete and modify tags, and associate tags to different event sources. For more information on tags, see [Chapter 8, "Configuring Tags," on page 127](#).
- ◆ **Search Remote Targets:** When this permission is set on a role, all members of that role can perform searches on event sources that are in a distributed location. For more information on distributed searching and reporting, see [Chapter 7, "Searching and Reporting Events in a Distributed Environment," on page 109](#).
- ◆ **Proxy for Authorized Search Initiators:** When this permission is set on a role, the members of this role can accept searches from remote targets.


10.2 Creating Roles and Users

- [Section 10.2.1, “Creating Roles,”](#) on page 154
- [Section 10.2.2, “Creating Users,”](#) on page 155

10.2.1 Creating Roles

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click the *users* link in the upper left corner of the page.
The *Users* tab is displayed in the right pane of the page.
- 3 Click *Add* in the *Roles* section to create a new role.
The New Role creation form is displayed.

New Role Cancel Save

 Role Name

Description:

Users with this role can:

View all data

View the following data:

Only events matching the filter:

Tips

View Sentinel Log Manager configuration data

View System Events

Manage Reports

Manage Tags

Search Remote Targets

Proxy for Authorized Search Initiators

- 4 Specify a name for the role and a brief description about the role. A role name can not exceed 40 characters.
- 5 Specify the values to filter events that a user can view. For more information on filters, see [Section 10.1.2, “Filtering Data,”](#) on page 153.
- 6 Select the permissions that you want to set for the users of the role. For more information, see [Section 10.1.3, “Setting Permissions,”](#) on page 153.
- 7 Click *Save*.
- 8 To create users for this role, continue with [Section 10.2.2, “Creating Users,”](#) on page 155.

10.2.2 Creating Users

Adding a user in the Sentinel Log Manager system creates an application user who can then log in to the Sentinel Log Manager application.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click the *users* link in the upper left corner of the page.
The *Users* tab is displayed in the right pane of the page.
- 3 Click *Add*. in the *Users* section.
The new user creation form is displayed.

ROLES	Add	USERS	Add
All Users	1	admin	
Administrator	1		
Compliance Auditor	0		
Database Administrator	0		
Network Administrator	0		
Network Security Administrator	0		
Report Administrator	0		
Sentinel Log Manager System Monitor	0		
Unix Administrator	0		
Users	0		
Windows Administrator	0		

NEW USER Cancel Save

Provide the name and email address of the user:

First Name:

Last Name:

Email:

Role: Administrator

Authentication Type: Local Directory

Choose a username and password for this user:

Username: *

Password: *

Verify: *

The following information is optional, but could be useful if someone needs to contact the user directly.

Title:

Office #:

Ext.

Mobile #:

Fax #:

- 4 Specify the name and e-mail address of the user. The e-mail address format is validated.
The fields with an asterisk (*) are mandatory, and the username must be unique. If the username already exists with the specified name, a Username taken message is displayed.
A user name:
 - ♦ must begin with a letter or an underscore (_).
 - ♦ cannot exceed 30 characters.
 - ♦ can only contain letters, digits and special characters (! @ # \$ % ^ & * () _ - = , < > ?)
 - ♦ supports extended characters.
- 5 Select a role to which the user must be assigned.
- 6 Select the authentication type:
Local: Select this option for the server to authenticate the user login against the Sentinel Log Manager database. By default, the *Local* option is selected.
Directory: The *Directory* option is enabled only if you have configured the Sentinel Log Manager server for LDAP authentication. Select this option for the server to authenticate the user login against an LDAP directory.
- 7 Specify a user name in the *Username* field.
 - ♦ **Local:** Specify any user name and move to [Step 8](#).

◆ **Directory:**

Username: *	<input type="text" value="ldap_user"/>	✔ Username available
LDAP User DN: *	<input type="text" value="cn=ldap_user,o=novell"/>	

When you configured the LDAP settings:

- ◆ **If you selected Yes for Anonymous Search:** User name must be the same as the LDAP directory username.
- ◆ **If you selected No for Anonymous Search and did not specify the Domain Name:** Username need not be the same as the LDAP directory username.
You must also specify the *LDAP User DN*. If Base DN was set, the Base DN is appended to the relative user DN to construct the absolute user DN.
For example, if the Base DN was set to `o=novell` and the absolute user DN is `cn=sentinel_ldap_user,o=novell` only the relative user DN i.e `cn=sentinel_ldap_user` can be specified.
- ◆ **If you selected No for Anonymous Search and specified the Domain Name:** User name must be the same as the LDAP directory username.

For more information on configuring LDAP settings, see [Chapter 11, “LDAP Authentication,”](#) on page 161.


Move to [Step 10](#).

- 8 Specify a password in the *Password* field.
- 9 Re-enter the password in the *Verify* field.
- 10 The *Title*, *Office #*, *Ext*, *Mobile #*, and *Fax*. fields are optional. The phone number fields allow any format. Make sure you have entered a valid phone number so that the user can be contacted directly.
- 11 Click *Save*.

10.3 Viewing Roles and User Details

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *user* in the upper left corner of the page.
The *Users* tab is displayed in the right pane.
- 3 Do one of the following:
 - ◆ To view information of a role, select the role. The detailed information of that role is displayed in the right-hand side.

ROLE INFO

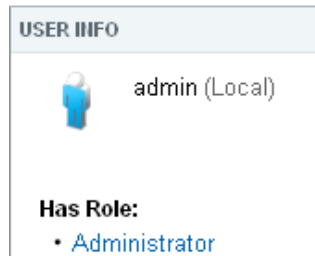
 **Administrator**
1 user

This role represents power users on an SLM system

Users with this role can:

- View and manage all data and configuration settings

- ♦ To view information of a role, select the user. The information of that user is displayed in the right-hand side. Click the link in *Has Role* list to get more information on the respective role.



10.4 Viewing All Users

- 1 Log in to the Sentinel Log Manager as an Administrator.
- 2 Click *user* in the upper left corner of the page.
The *Users* tab is displayed in the right pane.
- 3 To view all users at the same time, click *All Users* under *Roles* section.
All the users are displayed under the *Users* section.

10.5 Modifying Roles and Users

- ♦ [Section 10.5.1, “Modifying Roles,” on page 157](#)
- ♦ [Section 10.5.2, “Modifying User Details,” on page 158](#)

10.5.1 Modifying Roles

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click the *users* link in the upper left corner of the page.
The *Users* tab is displayed in the right pane of the page.
- 3 Select the role that you want to modify from the *Roles* section.
- 4 Click *Edit* in the *Role Info* section.
The Edit Role form is displayed.

EDIT ROLE
Cancel Save

Description:

The role for users that administer databases. Users in this role will only have access to events coming from database event sources. The type of the event source (DB) is determined by the collector parsing the data from the event source.

Users with this role can:

View all data

View the following data:

Only events matching the filter:

Tips

View Sentinel Log Manager configuration data
 View System Events

Manage Reports
 Manage Tags
 Search Remote Targets
 Proxy for Authorized Search Initiators

- 5 Modify the information in the field that you want to change.
- 6 Click *Save*.

10.5.2 Modifying User Details

Administrators can edit user information for a user in the system. Users can edit their own profiles except for the username and administrative privileges.

- ♦ [“Modifying Your Own Profile” on page 158](#)
- ♦ [“Modifying Your Own Password” on page 159](#)
- ♦ [“Modifying Another User’s Profile \(admin only\)” on page 159](#)

Modifying Your Own Profile

To edit your own profile:

- 1 Click the logged in user name in the upper left corner of the page.
The *Users Info* tab is displayed on the right pane of the page.
- 2 Modify the information in the *Edit User* pane.
- 3 Click *Save*.

Modifying Your Own Password

To change the password:

- 1 Click the logged in user name in the upper left corner of the page.
The *User Info* tab is displayed on the right pane of the page.
- 2 Specify your current password.
- 3 Specify your new password.
- 4 Confirm your new password.
- 5 Click *Save*.

Modifying Another User's Profile (admin only)

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *users* in the upper left corner of the page.
The *Users* tab is displayed in the right pane.
- 3 Select the User whose profile you want to change.
- 4 Click *Edit* in the *User Info* section.
- 5 Modify the information.

NOTE: You cannot modify the name of a user.

- 6 Click *Save*.

10.6 Moving Users to Another Role

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *user* in the upper left corner of the page.
The *Users* tab is displayed in the right pane.
- 3 Select the user that you want to move to another role.
- 4 Click *Edit*.
- 5 From *Role* drop-down list, select the role that you want to move the user to.
- 6 Click *Save*.

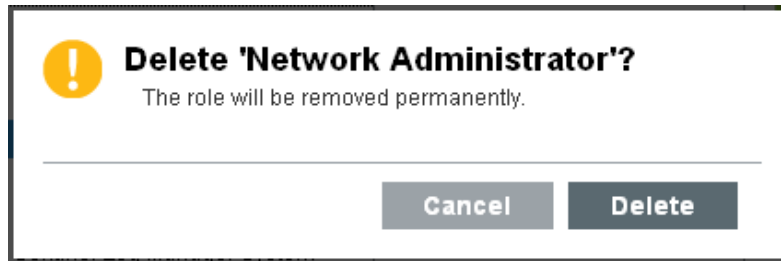
10.7 Deleting Roles and Users

- ♦ [Section 10.7.1, "Deleting a Role," on page 159](#)
- ♦ [Section 10.7.2, "Deleting a User," on page 160](#)

10.7.1 Deleting a Role

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *users* in the upper left corner of the page.
The *Users* tab is displayed in the right pane.

- 3 Select the role that you want to delete.
- 4 Select *Delete* from the *Role Info* section.
You are prompted to confirm deletion.



- 5 Click *Delete* to confirm deletion.

NOTE: If you attempt to delete a role with one or more users, you are prompted the confirm deletion. If you proceed with deletion, the role and the users belonging to that role are permanently deleted.

10.7.2 Deleting a User

If you delete users who are already logged in, the users can continue to use Sentinel Log Manager until they log out.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click *user* in the upper left corner of the page.
The *Users* tab is displayed in the right pane.
- 3 Select the user that you want to delete.
- 4 Click *Delete* in the upper right corner of the *User Info* section.
You are prompted to confirm deletion.
- 5 Click *Delete* to confirm deletion.

11 LDAP Authentication

Sentinel Log Manager supports LDAP authentication in addition to database authentication. You can configure a Sentinel Log Manager server for LDAP authentication to enable users to log in to Sentinel Log Manager with their LDAP directory credentials.

NOTE: Sentinel Log Manager LDAP authentication is tested with Novell eDirectory and Microsoft Active Directory. Other LDAP compliant directories might be used, but are not tested. If an issue is encountered when using a directory that has not been tested, support will be provided to the extent that the issue can be reproduced on one of the tested directories.

- ♦ [Section 11.1, “Overview,” on page 161](#)
- ♦ [Section 11.2, “Prerequisites,” on page 162](#)
- ♦ [Section 11.3, “Setting Up LDAP Authentication,” on page 162](#)
- ♦ [Section 11.4, “Creating an LDAP User Account,” on page 166](#)
- ♦ [Section 11.5, “Configuring Multiple LDAP Servers for Failover,” on page 166](#)

11.1 Overview

LDAP authentication can be performed either using an SSL connection or an unencrypted connection to the LDAP server.

You can configure the Sentinel Log Manager server for LDAP authentication either using or without using anonymous searches on the LDAP directory.

NOTE: If anonymous search is disabled on the LDAP directory, you must not configure the Sentinel Log Manager server to use anonymous search.

- ♦ **Anonymous:** While creating Sentinel Log Manager LDAP user accounts, the directory username must be specified and the user distinguished name (DN) need not be specified.

When the LDAP user logs in to Sentinel Log Manager, the Sentinel Log Manager server performs an *anonymous search* on the LDAP directory based on the specified username, finds the corresponding DN, then authenticates the user login against the LDAP directory by using the DN.

- ♦ **Non Anonymous:** While creating Sentinel Log Manager LDAP user accounts, the user DN must also be specified along with the username.

When the LDAP user logs in to the Sentinel Log Manager, the Sentinel Log Manager server authenticates the user login against the LDAP directory by using the specified user DN and does not perform any anonymous search on the LDAP directory.

There is an additional approach applicable only for Active Directory. For more information, see [“Domain Name” on page 164](#).

11.2 Prerequisites

- ♦ Section 11.2.1, “Exporting the LDAP Server CA Certificate,” on page 162
- ♦ Section 11.2.2, “Enabling Anonymous Search in the LDAP Directory,” on page 162

11.2.1 Exporting the LDAP Server CA Certificate

If you want to connect to the LDAP server by using an SSL connection and the LDAP server certificate is not signed by a well-known CA, you must export the LDAP server CA certificate to a Base64-encoded file.

- ♦ **eDirectory:** See [Exporting an Organizational CA's Self-Signed Certificate \(http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html\)](http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html).

To export an eDirectory CA certificate in iManager, the Novell Certificate Server plug-ins for iManager must be installed.

- ♦ **Active Directory:** See [How to enable LDAP over SSL with a third-party certification authority \(http://support.microsoft.com/kb/321051\)](http://support.microsoft.com/kb/321051).

11.2.2 Enabling Anonymous Search in the LDAP Directory

To perform LDAP authentication using anonymous search, you must enable anonymous search in the LDAP directory. By default, anonymous search is enabled in eDirectory and is disabled in Active Directory.

- ♦ **eDirectory:** See `ldapBindRestrictions` in section [Attributes on the LDAP Server Object \(http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html\)](http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html).
- ♦ **Active Directory:** Enabling anonymous binds for Active Directory requires two steps. These steps are the same for both Windows 2003 and Windows 2008 Active Directory.
 - ♦ **Enable Anonymous LDAP Operations:** By default, anonymous LDAP operations are disabled in Active Directory. You must enable anonymous LDAP operations in Active Directory by setting the `dsHeuristics` attribute to an appropriate value.
For more information, see [Enabling anonymous LDAP operations \(http://www.petri.co.il/anonymous_ldap_operations_in_windows_2003_ad.htm\)](http://www.petri.co.il/anonymous_ldap_operations_in_windows_2003_ad.htm).
 - ♦ **Assign Permissions to the ANONYMOUS LOGON User:** The Read and List Contents permissions must be assigned to the ANONYMOUS LOGON user.
For more information, see [Granting anonymous read access \(http://www.petri.co.il/anonymous_ldap_operations_in_windows_2003_ad.htm\)](http://www.petri.co.il/anonymous_ldap_operations_in_windows_2003_ad.htm).

11.3 Setting Up LDAP Authentication

- 1 Log in to Sentinel Log Manager as the administrator user.
- 2 Click the *users* link on the top left corner of the page.
- 3 On the Users page, click *LDAP Settings*.
The LDAP Settings page is displayed.

Provide the LDAP server details:

Host:*

SSL:

Port:*

The default SSL port is 636 and the default non-SSL port is 389.

Certificate File Path:

The path to the LDAP server's certificate. This only needs to be set if the LDAP server's certificate is not signed by a well known CA and, therefore, is not trusted by default.

Provide the LDAP user search details:

Anonymous Search: Yes No

Base DN:

The root node in the LDAP directory under which to search for users, optional for eDirectory, mandatory for Active Directory. For example, cn=users,dc=example,dc=com.

Search Attribute:*

The attribute in LDAP holding the user login name, which is used to search for users. For example, uid for eDirectory, sAMAccountName for Active Directory.

Test Connection

Reset

Save

4 Specify the following:

Field	Description/Action
<i>Host</i>	The hostname or the IP address of the LDAP server.
<i>SSL</i>	Select this option if you want to connect to the LDAP server by using a Secure Socket Layer connection.
<i>Port</i>	The port number for the LDAP connection. The default SSL port number is 636 and the default non-SSL port number is 389.
<i>Certificate File Path</i>	Path of the LDAP server CA certificate file. This field must be set only if you selected the SSL option and if the LDAP server certificate is not signed by a well-known CA and, therefore, is not trusted by default.
<i>Anonymous Search</i>	Select <i>Yes</i> to perform anonymous searches or select <i>No</i> if you do not want perform anonymous searches on the LDAP directory.

Field	Description/Action
<i>Base DN</i>	<ul style="list-style-type: none"> ◆ If Anonymous Search is Yes: The root node in the LDAP directory under which to search for users. This is optional for eDirectory, and mandatory for Active Directory. For eDirectory, if the Base DN is not specified, the entire directory is searched to locate the users. ◆ If Anonymous Search is No: The root node in the LDAP directory that contains the users. This is mandatory if you are using Active Directory and if you set a domain name. For all other cases, this is optional. <p>The following are examples for specifying the Base DN:</p> <ul style="list-style-type: none"> ◆ eDirectory: <code>o=novell</code> ◆ Active Directory: <code>cn=users,dc=example,dc=com</code>
<i>Search Attribute</i>	<p>The attribute in LDAP holding the user login name, which is used to search for users.</p> <p>For example:</p> <ul style="list-style-type: none"> ◆ eDirectory: <code>uid</code> ◆ Active Directory: <code>sAMAccountName</code> <p>This field is available only if you had selected <i>Yes</i> for Anonymous Search.</p>
<i>Domain Name</i>	<p>The name of the Active Directory domain.</p> <p>There is an additional approach applicable only for Active Directory for performing LDAP authentication without using Anonymous search:</p> <p>When you specify the Domain Name, <code>username@domainname</code> (<code>userPrincipalName</code>) is used to authenticate the user before searching for the LDAP user object.</p> <p>For example, <code>test.example.com</code></p> <p>This field is applicable only for ActiveDirectory and is available only if you selected <i>No</i> for Anonymous Search.</p>

NOTE: If *Base DN* is set and *Domain Name* is not set, the *Base DN* is appended to the relative user DN to construct the absolute user DN.

For example, if the Base DN is set to `o=novell` and the absolute user DN is `cn=sentinel_ldap_user,o=novell` while creating LDAP user accounts, only the relative user DN i.e `cn=sentinel_ldap_user` can be specified.

- 5 Click *Test Connection* to test whether the LDAP connection is successful.

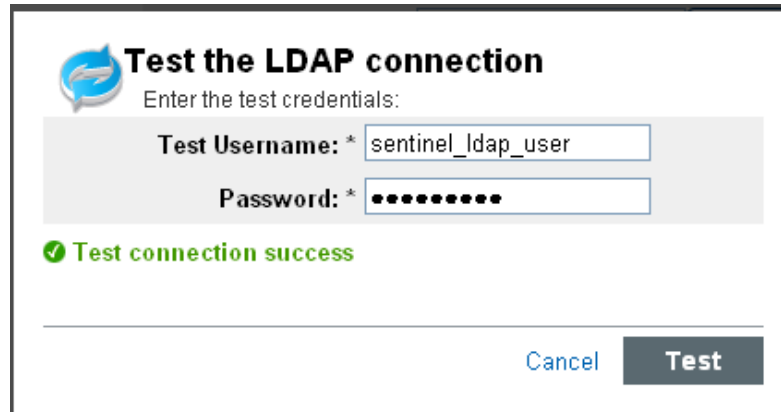
The Test the LDAP Connection page is displayed.

5a Specify the test credentials to connect to the LDAP server:

- ♦ **If Anonymous Search is Yes:** Specify the username and password.
- ♦ **If Anonymous Search is No:** Specify the user DN and password. The user DN can be relative to the Base DN.

5b Click *Test* to test the LDAP connection.

A message is displayed that indicates whether the connection is successful.



If there is any error, review the configuration details you provided and test the connection again. You can determine the cause of the failure by examining the `/var/opt/novell/sentinel_log_mgr/log/server0.0.log` file. You must ensure that the test connection is successful before saving the LDAP settings.

6 Click *Save* to save the LDAP settings.

On successful configuration:

- ♦ The `LdapLogin` section of the `/etc/opt/novell/sentinel_log_mgr/config/auth.login` file is updated. For example:

```
LdapLogin {
    com.sun.security.auth.module.LdapLoginModule required
    java.naming.ldap.factory.socket="com.esecurity.common.communication.ProxyL
dapSSLSocketFactory"
    userProvider="ldap://10.0.0.1:636/o=novell"
    userFilter="(uid={USERNAME}) (objectclass=user)"
    useSSL=true;
};
```

- ♦ The LDAP server CA certificate, if provided, is added to a keystore named `/etc/opt/novell/sentinel_log_mgr/config/.activemqkeystore.jks`

After saving the LDAP settings successfully, you can create LDAP user accounts to enable users to log in to Sentinel Log Manager by using their LDAP directory credentials.

NOTE: You can also configure the Sentinel Log Manager server for LDAP authentication by running the `ldap_auth_config.sh` script in the `/opt/novell/sentinel_log_mgr/setup` directory.

The script also supports command line options. To view the command line options, run the script as follows:

```
/opt/novell/sentinel_log_mgr/setup/ldap_auth_config.sh --help
```

11.4 Creating an LDAP User Account

For information on creating LDAP user accounts, see [Section 10.2, “Creating Roles and Users,”](#) on page 154.

11.5 Configuring Multiple LDAP Servers for Failover

To configure one or more LDAP servers as failover servers for LDAP authentication:

- 1 Log in to the Sentinel Log Manager server as root user.
- 2 Switch to novell user.

```
su - novell
```

- 3 Change to the `/etc/opt/novell/sentinel_log_mgr/config` directory:

```
cd /etc/opt/novell/sentinel_log_mgr/config/
```

- 4 Open the `auth.login` file for editing.

```
vi auth.login
```

- 5 Update the `userProvider` in the `LdapLogin` section to specify multiple LDAP URLs. Separate each URL by a blank space.

For example:

```
userProvider="ldap://primary_server_IP:port/BaseDN ldap://  
failover_server_IP:port/BaseDN"
```

NOTE: For Active Directory, ensure that the BaseDN in the LDAP URL is not blank.

For more information on specifying multiple LDAP URLs, see the description of the `userProvider` option in [Class LdapLogin Module](http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html) (<http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html>).

- 6 Save the changes.

If you are using an SSL connection to the LDAP server and if the LDAP server certificate is not signed by a well-known CA, you must perform the following additional steps:

- 1 Export the certificate of each failover LDAP server and copy the certificate file to the `/etc/opt/novell/sentinel_log_mgr/config` directory on the Sentinel Log Manager server.

For more information, see [Section 11.2.1, “Exporting the LDAP Server CA Certificate,”](#) on page 162.

- 2 Ensure that you set the necessary ownership and permissions of the certificate file for each LDAP sever.

```
chown novell:novell /etc/opt/novell/sentinel_log_mgr/config/<cert-file>
```

```
chmod 600 /etc/opt/novell/sentinel_log_mgr/config/<cert-file>
```

- 3 Add each LDAP server certificate to the keystore named `activemqkeystore.jks`.

```
/opt/novell/sentinel_log_mgr/jre/bin/keytool -importcert -noprompt -  
trustcacerts -file <certificate-file> -alias <alias_name> -keystore /etc/opt/  
novell/sentinel_log_mgr/config/.activemqkeystore.jks -storepass password
```

where `<certificate-file>` is the LDAP certificate filename and `<alias_name>` is the alias name for the certificate to be added.

IMPORTANT: Ensure that you specify the alias. If no alias is specified, the keytool takes mykey as the alias by default. When you import multiple certificates into the keystore without specifying an alias, the keytool reports an error that the alias already exists.

You have now successfully configured LDAP servers for failover.

12 Implementing High Availability and Disaster Recovery

Sentinel Log Manager has been tested and certified to work in a high availability environment and supports disaster recovery architectures. Novell Consulting and Novell partners can help you implement Sentinel Log Manager high availability and disaster recovery.

This section has the following information:

- ♦ [Section 12.1, “High Availability,” on page 169](#)
- ♦ [Section 12.2, “Disaster Recovery,” on page 170](#)

12.1 High Availability

To enable the Sentinel Log Manager servers for high availability, you require the following:

- ♦ Redundant, clustered Sentinel Log Manager nodes.
- ♦ Access to shared data storage.
- ♦ Virtual IP addresses that can be used to transparently shift from a failed node to another node.
- ♦ Scripts to start, stop, and monitor the application based on policies defined in the cluster solutions. You can use cluster solutions such as Cluster Resource Agents or LSB init scripts on Linux Enterprise High Availability systems.

There are many packages in the market that enable high availability, testing for Sentinel Log Manager was performed with *SUSE Linux Enterprise High Availability (HA) Extension* (<http://www.novell.com/products/highavailability/>), shared storage RAID drives, and custom scripts. This architecture can be replicated across data centers to ensure availability of everything from the Sentinel Log Manager server to the Collector Managers and Collectors.

If the environment includes Windows-based Collector Managers, high availability for the Windows Collector Managers may be setup using the Microsoft Windows Clustering approach by using the [Microsoft Windows Clustering approach](http://www.microsoft.com/windowsserver2003/enterprise/clustering.mspx) (<http://www.microsoft.com/windowsserver2003/enterprise/clustering.mspx>) Other clustering solutions (for example, Veritas Clustering Services) may be used, but Novell has not tested these at this time. For information on using any of these clustering services, please refer to the respective vendor documentation.

High availability for the event sources should also be considered on a case by case basis because of the wide variety of devices.

12.2 Disaster Recovery

Disaster recovery is enabled by using out-of-the-box full backup and restoration capabilities. Frequent backups of the Sentinel Log Manager can be taken while the server is running, with zero down time.

These backups can be copied to a safe location and be used at any time to fully restore the original Sentinel Log Manager or a redundant Sentinel Log Manager to the state of the most recent backup. For more information about the out-of-the-box backup and restore, see [Appendix C, “Backing Up and Restoring Data,”](#) on page 193.

13 License Information

This section describes the various Sentinel Log Manager licenses and also provides information on how you can manage the licenses.

- ♦ [Section 13.1, “Understanding the Licenses,” on page 171](#)
- ♦ [Section 13.2, “Managing the Licenses,” on page 173](#)

13.1 Understanding the Licenses

Sentinel Log Manager has several licenses that you can use. By default, Sentinel Log Manager comes with the trial license.

- ♦ [Section 13.1.1, “Trial License,” on page 171](#)
- ♦ [Section 13.1.2, “Free License,” on page 172](#)
- ♦ [Section 13.1.3, “Enterprise Licenses,” on page 172](#)

13.1.1 Trial License

The Sentinel Log Manager default licensing allows you to use all the enterprise features of Sentinel Log Manager except for the Data Restoration feature, with an unrestricted events per second (EPS) for 60 days. After the trial license expires the system runs with a base license key that enables a limited set of features and a limited event rate of 25 EPS. The base license is also known as the free license.

During the 60-day trial period, you can use the following features:

- ♦ **Rules:** Enables you to configure rules that allow you to evaluate and filter all incoming events and deliver selected events to designated output actions. For more information, see [Chapter 9, “Configuring Rules and Actions,” on page 137](#).
- ♦ **Actions:** Enables you to configure actions that get executed when one or more events meet the criteria specified by a rule. For more information, see [Section 9.2, “Configuring Actions,” on page 140](#).
- ♦ **Distributed Search:** Enables you to search events and report event data not only on your local Sentinel Log Manager server, but also on other Sentinel Log Manager servers distributed across the globe. For more information, see [Chapter 7, “Searching and Reporting Events in a Distributed Environment,” on page 109](#).
- ♦ **Sentinel Link:** Provides the ability to hierarchically link multiple Sentinel systems, including Sentinel Log Manager and the two Sentinel Security Information Event Management (SIEM) systems, Novell Sentinel and Novell Sentinel Rapid Deployment systems. For more information, see [Section 9.2.6, “Sending the Events to a Sentinel Link,” on page 144](#).
- ♦ **Event Store:** Enables you to view the details of all the events regardless of the EPS rate.

13.1.2 Free License

Sentinel Log Manager comes with a free license that allows you to use a limited set of features with a limited event rate of 25 EPS. The free license does not expire.

NOTE: Novell does not provide technical support and product updates for the free version of Sentinel Log Manager.

The free version of Sentinel Log Manager includes the following features:

- ♦ **Collector:** Allows you to use any Collector without any restriction.
- ♦ **Embedded Database:** Stores the Sentinel Log Manager configuration data.
- ♦ **EPS Limited Event Store:** Provides the ability to persist with the event flow even if the event view is restricted because of the expired or not licensed Event Store feature.

The following features can still be accessed with limited functionality:

- ♦ **Distributed Search and Report:** You can add, modify, and delete the search target configurations. However, only the local event store is used for searches and reports while you are using an expired license. This applies to all distributed searches and reports, even if they were scheduled before the license expired.
- ♦ **Actions and Rules:** You can add, modify, and delete actions and rules. However, the actions and rules will not be executed.
- ♦ **Sentinel Link:** The Sentinel Link ESM node and actions are disabled after 60 days. Therefore, events cannot be sent or received by using Sentinel Link.
- ♦ **Event Store:** The authorized event rate after the license expires is 25 EPS. Any events received while the system averages more than 25 EPS are stored, but the details of those events are not displayed in the search results or reports. These events are tagged with the OverEPSLimit tag. For more information, see [“Events View in Free Versions of Sentinel Log Manager” on page 82](#).

All the functionality, including Data Restoration and the ability to view all events, can be restored by upgrading the system to an enterprise license. To prevent any interruption in the functionality, you must upgrade the system with the enterprise license before the expiration date.

13.1.3 Enterprise Licenses

Enterprise licenses are paid licenses that allow you to use all the Sentinel Log Manager features. The licenses are generated based on EPS: 500 EPS, 2500 EPS, and 7500 EPS.

NOTE: To purchase an enterprise license or to upgrade to a higher event rate, contact [Novell Support \(http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup\)](#) or see [How to Buy \(http://www.novell.com/products/sentinel-log-manager/howtobuy.html\)](#). To add the license key to the system, see [Section 13.2.1, “Adding a License Key,” on page 173](#).

13.2 Managing the Licenses

NOTE: To add, view, or delete a license, you must have admin rights.

- ◆ [Section 13.2.1, “Adding a License Key,” on page 173](#)
- ◆ [Section 13.2.2, “Viewing the License Details,” on page 175](#)
- ◆ [Section 13.2.3, “Deleting a License Key,” on page 175](#)

13.2.1 Adding a License Key

This section describes the procedure to add a license key either by using the Web UI or through the command line.

- ◆ [“Adding a License Key By Using the Web UI” on page 173](#)
- ◆ [“Adding a License Key Through Command Line” on page 174](#)

Adding a License Key By Using the Web UI

- 1 Log in to Sentinel Log Manager as an administrator.
- 2 Click the *About* link in the upper left corner of the page.
- 3 Click the *Licenses* tab.
- 4 In the Licenses section, click *Add License*.

The screenshot shows the 'About' tab selected in the top navigation bar. Below it is a table with the following data:

Distributed Search	Apr 9, 2011
Event Store	Apr 9, 2011
Rules	Apr 9, 2011
Sentinel Link	Apr 9, 2011
COLLECTOR	Never
EPS Limited Event Store	Never
Embedded Database	Never

* Note : Hover the mouse on expiry date to see the exact local time.

The 'licenses' section is visible below, containing a form with the following fields and values:

Key: Dr50YeYu348

Features: Actions, Distributed Search, Event Store, Rules, Sentinel Link

Hostname: 29c503fc Serial: 05022006

EPS: Unlimited

Expires: 4/9/11

Key: Dr50YeYu348

Features: COLLECTOR, EPS Limited Event Store, Embedded Database

Hostname: All Serial: 05022006

EPS: 25

Expires: Never

Add License

- 5 Specify the license key in the *Key* field. After you specify the license, the following information is displayed in the Preview section:

The screenshot displays a software interface for managing license keys. At the top, there are tabs for 'About' and 'All Events'. Below this, there are three license key entries, each with a 'Key' field and a list of 'Features'. The first entry has features: Actions, Distributed Search, Event Store, Rules, Sentinel Link; Hostname: 29c503fc; Serial: 05022006; EPS: Unlimited; Expires: 4/9/11. The second entry has features: COLLECTOR, EPS Limited Event Store, Embedded Database; Hostname: All; Serial: 05022006; EPS: 25; Expires: Never. The third entry is a preview of a license key with features: Actions, COLLECTOR, Data Restoration, Distributed Search, Embedded Database, Event Store, Rules, Sentinel Link, Sentinel Log Manager; Hostname: All; Serial: 05022006; EPS: 500; Expires: Never. At the bottom right, there are 'Cancel' and 'Save' buttons.

Features: The features that are available with the license.

Hostname: This field is for internal Novell use only.

Serial: This field is for internal Novell use only.

EPS: Maximum licensed event rate for the Sentinel Log Manager instance. During event spikes, the system continues to collect data even though it is out of compliance.

Expires: Expiry date of the license. You must specify a valid license key before the expiry date to prevent an interruption in functionality.

6 Click *Save*.

Adding a License Key Through Command Line

You can add the license through the command line by using the `softwarekey.sh` script.

- 1 Log in to the Novell Sentinel Log Manager server as root.
- 2 Change to the `/opt/novell/sentinel_log_mgr/bin` directory.
- 3 Enter the following command to change to novell user:


```
su novell
```
- 4 Specify the following command to run the `softwarekey.sh` script.


```
./softwarekey.sh
```
- 5 Enter 1 to enter the license key.
- 6 Specify the license key, then press enter.

13.2.2 Viewing the License Details

You can view the license information either through the Web UI, or through the command line by using the `softwarekey.sh` script. For information on running the `softwarekey.sh` script, see [“Adding a License Key Through Command Line” on page 174](#). The following procedure describes the steps to view the license key by using the Web UI:

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click the *About* link in the upper left corner of the page.
- 3 Click the *Licenses* tab.

The *Licenses* section specifies the features, hostname, serial number, and expiry date of the added licenses.

- ♦ The *Max EPS* shows the maximum number of EPS value among the various licenses.
For example, if Sentinel Log Manager contains EPS licenses with values of 500, 2500, and 7500, the 7500 EPS value is displayed in the *Max EPS* field.
- ♦ The *Licensed Features* section lists the features and expiry date of the license key.

13.2.3 Deleting a License Key

NOTE: You can only delete an expired license. The *delete license* link is displayed only when a license expires.

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Click the *About* link in the upper left corner of the page.
- 3 Click the *Licenses* tab.
The expired date is displayed inside a red box with the *Expired on <mm/dd/yy>* text. The *delete license* link is displayed next to the expiry date box.
- 4 Click the *delete license* link. A confirmation message is displayed.
- 5 Click *Delete*.

14 Command Line Utilities

The command line utilities included with Novell Sentinel Log Manager are useful for managing and configuring many lower level functions of the system.

- ♦ [Section 14.1, “Managing the Sentinel Log Manager Services,” on page 177](#)
- ♦ [Section 14.2, “Running the Report Development Utility,” on page 178](#)
- ♦ [Section 14.3, “Getting the .jar Version Information,” on page 178](#)
- ♦ [Section 14.4, “Reconfiguring Database Connection Properties,” on page 179](#)
- ♦ [Section 14.5, “Sentinel Scripts,” on page 179](#)

14.1 Managing the Sentinel Log Manager Services

The command line utilities included with Novell Sentinel Log Manager are useful for managing and configuring many lower level functions of the system.

Table 14-1 Useful commands

Services	command
Starting Sentinel Log Manager Service	<code>/opt/novell/sentinel_log_mgr/bin/./server.sh start</code>
Stopping Sentinel Log Manager Service	<code>/opt/novell/sentinel_log_mgr/bin/./server.sh stop</code>
Verifying the status of Sentinel Log Manager Service	<code>/opt/novell/sentinel_log_mgr/bin/./server.sh status</code>
Verifying the version of Sentinel Log Manager	<code>/opt/novell/sentinel_log_mgr/bin/./server.sh version</code>
Restarting the Sentinel Log Manager	<code>/opt/novell/sentinel_log_mgr/bin/./server.sh restart</code>
Starting the database	<code>/opt/novell/sentinel_log_mgr/bin/./server.sh start db</code>
Stopping the database	<code>/opt/novell/sentinel_log_mgr/bin/./server.sh stopdb</code>
Restart the Sentinel Log Manager service if it is running	<code>/opt/novell/sentinel_log_mgr/bin/./server.sh try-restart</code>
Forces the Sentinel Log Manager service to reload configuration.	<code>/opt/novell/sentinel_log_mgr/bin/./server.sh force-reload</code>

14.2 Running the Report Development Utility

You can use the `/opt/novell/sentinel_log_mgr/bin/report_dev_setup.sh` utility to set up the report development environment. This utility does the following:

- ♦ Opens the PostgreSQL database port so that other servers can connect to the Sentinel Log Manager database.
- ♦ Updates the firewall to allow connection on the database port.
- ♦ Modifies the database configuration files (`postgresql.conf` and `pg_hba`) so that other applications can connect to the Sentinel Log Manager database. The database configuration files are located at `$ESEC_DATA_HOME/3rdparty/postgresql/data`.
- ♦ Changes the `rptuser` password, if required and saves it in an encoded format in the `obj-component.JasperReportingComponent.properties` file. This password can be changed in the database as well.
- ♦ Collects the required Sentinel Log Manager jar files, xml and keystore file for report development and creates a tar file `sentineljarsforireport.tar`, in the `/opt/novell/sentinel_log_mgr/bin` directory.

To run this utility:

- 1 Specify the following command:

```
./report_dev_setup.sh
```

A warning message is displayed indicating that the Sentinel Log Manager server gets restarted after the script is executed.

- 2 To continue running the script, press 1.
- 3 Specify the `root` password when prompted.

The script opens the database port, updates the firewall configuration files, modifies the configuration files and database files.

- 4 When prompted to change the `rptuser` password, do one of the following:
 - 4a Specify a password for `rptuser` when prompted. Specify a password and reconfirm the password when prompted.
 - 4b Continue without changing the password.

NOTE: The `rptuser` password is randomly generated during the installation of Sentinel Log Manager. It is a recommended practice to change it here.

The Sentinel Log Manager Server restarts.

If you require any information or help on the usage of commands, specify the following command:

```
./report_dev_setup.sh -h
```

14.3 Getting the .jar Version Information

The following procedure describes how to gather the version information of Sentinel Log Manager jar files for troubleshooting purposes:

- 1 Log in to the Sentinel Log Manager server by using Sentinel Log Manager's Administrator Operating System user (by default `novell`).
- 2 Go to the `/opt/novell/sentinel_log_mgr/bin` directory.

- 3 At the command line, specify the `./versionreader.sh <path/jar file name>`.
Running the script without any arguments gives the version of the installed Sentinel Log Manager server. For more information on the arguments that can be used, specify the `--help` command.

14.4 Reconfiguring Database Connection Properties

The primary settings in the configuration files that can be configured using the `dbconfig` utility are related to the database connection, including:

- ♦ username
- ♦ password
- ♦ hostname
- ♦ port number
- ♦ database (database name)
- ♦ server (PostgreSQL)

WARNING: Do not manually edit the database connection properties. Use the `dbconfig` utility to change any database connection values within the files.

To Reconfigure Database Connection Properties

- 1 Log in to the Novell Sentinel Log Manager server as `novell` user on UNIX.
- 2 Go to the `/opt/novell/sentinel_log_mgr/bin` directory.
- 3 Enter the following command:

```
dbconfig -a /etc/opt/novell/sentinel_log_mgr/config [-u username] [-p password]
[-h hostname] [-t portnum] [-d database] [-s server] [-help] [-version]
```

For example,

```
dbconfig -a /etc/opt/novell/sentinel_log_mgr/config [-u username] [-p password]
[-h hostname] [-t portnum] [-d database] [-s server] [-help] [-version]
```

Changing these settings might affect database performance and should be done with caution.

14.5 Sentinel Scripts

The `/opt/novell/sentinel_log_mgr/bin` directory contains some or all of the scripts mentioned below. The operational scripts are appropriate for use during normal operations of Sentinel Log Manager.

For most scripts that require arguments, running the scripts without arguments provides details about the arguments and usage of the script.

The scripts below can be used during the normal operation of Sentinel Log Manager.

Table 14-2 Operational Scripts

Script File:	Description:
dbconfig	You can use this to configure the database connection settings. For more information, see “Reconfiguring Database Connection Properties” on page 179.
config_firewall.sh	For more information, see “Listening on Ports Below 1024” on page 59.
softwarekey.sh	You can use this to add and view license key through the command line. For more information, see Chapter 13, “License Information,” on page 171.
report_dev_setup.sh	You can use this utility to set up the report development environment. For more information, see Section 14.2, “Running the Report Development Utility,” on page 178.
backup_util.sh	You can use this script to back up and restore Sentinel Log Manager event data and configuration Data. For more information, see Appendix C, “Backing Up and Restoring Data,” on page 193.
updateServerLocale.sh	<p>This utility provides an option to change the language of Sentinel Log Manager server process. The Sentinel Log Manager server messages displayed in the user interface appear in the language you select.</p> <p>If the appliance language is changed through WebYast, you can use this script to change the language of the Sentinel Log Manager process in the server.</p>

A Search Query Syntax

Sentinel Log Manager uses the Lucene query language for searching events. This section provides an overview of how to use the Lucene query language to perform searches in Sentinel Log Manager. For more advanced features, see [Apache Lucene - Query Parser Syntax \(http://lucene.apache.org/java/3_2_0/queryparsersyntax.html\)](http://lucene.apache.org/java/3_2_0/queryparsersyntax.html).

For information on the event fields in Sentinel Log Manager, click *search tips* on the top right corner in the Sentinel Log Manager Web interface. A table is displayed that lists the event names and their IDs.

- ♦ [Section A.1, “Basic Search Query,” on page 181](#)
- ♦ [Section A.2, “Wildcards in Search Queries,” on page 186](#)
- ♦ [Section A.3, “The notnull Query,” on page 188](#)
- ♦ [Section A.4, “Tags in Search Queries,” on page 188](#)
- ♦ [Section A.5, “Range Queries,” on page 189](#)
- ♦ [Section A.6, “IP Addresses Query,” on page 189](#)

A.1 Basic Search Query

A basic query is a search for a value on a field. The syntax is as follows:

```
msg:<value>
```

The field name (msg) is separated from the value by a colon.

For example, to search for a phrase that includes the word “authentication,” you can specify the search query as follows:

```
msg:authentication
```

Or, to search for events of severity 5, you can specify the search query as follows:

```
sev:5
```

If the value has spaces or other delimiters in it, you should use quotation marks. For example:

```
msg:"value with spaces"
```

Sentinel Log Manager classifies event fields as either tokenized fields or non-tokenized fields. A tokenized field is indexed and is searched differently than a non-tokenized field.

- ♦ [Section A.1.1, “Case Insensitivity,” on page 182](#)
- ♦ [Section A.1.2, “Special Characters,” on page 182](#)
- ♦ [Section A.1.3, “Operators,” on page 182](#)
- ♦ [Section A.1.4, “The Default Search Field,” on page 183](#)

- ♦ [Section A.1.5, “Tokenized Fields,” on page 184](#)
- ♦ [Section A.1.6, “Non-Tokenized Fields,” on page 186](#)

A.1.1 Case Insensitivity

Indexing and searching in Sentinel Log Manager is not case-sensitive. For example, the following queries are all equivalent:

```
msg:AdMin
msg:admin
msg:ADMIN
```

A.1.2 Special Characters

If you include special characters as part of a search, the special characters must be escaped. These characters are as follows:

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
```

Use “\” before the character you want to escape. For example, to search for ISO/IEC_27002:2005 in the rv145 (Tag) field, use the following query:

```
rv145:ISO/IEC_27002\:2005
```

You can also use quotation marks around the query:

```
rv145:"ISO/IEC_27002:2005"
```

If the value contains quotation marks, you must escape it by using the “\” character instead of quotation marks. For example, to search for “system “mail” service” in the `initiatorservicename` field, you must specify the query as follows:

```
sp:"system \"mail\" service"
```

For more information on quoting wildcard characters, see [Section A.2.2, “Quoted Wildcards,” on page 187](#).

A.1.3 Operators

Lucene supports AND, OR, and NOT Boolean operators, which allow words to be combined. Boolean operators must be always capitalized.

- ♦ [“OR Operator” on page 182](#)
- ♦ [“AND Operator” on page 183](#)
- ♦ [“NOT Operator” on page 183](#)
- ♦ [“Operator Precedence” on page 183](#)

OR Operator

The OR operator is the default conjunction operator. If there is no Boolean operator between two clauses, the OR operator is used. The OR operator links two clauses and finds a matching event if either of the clauses is satisfied. The symbol `||` can be used in place of the word OR. For example, consider the following query:

```
sun:admin OR dun:admin
```

This query finds events whose initiator username or target username is “admin.” The following query produces the same result because OR is used by default:

```
sun:admin dun:admin
```

AND Operator

The AND operator links two clauses and finds a matching event only if both clauses are satisfied. The symbol && can be used in place of the word AND. For example, consider the following query:

```
sun:admin AND dun:tester
```

This query finds events whose initiator username is admin and the target username is tester.

NOT Operator

The NOT operator excludes events that match the clause after the NOT. The symbol ! can be used in place of the word NOT. For example, consider the following query:

```
sev:[0 TO 5] NOT st:I NOT st:A NOT st:P
```

This query matches all events whose severity is between 0 and 5, but excludes those whose sensor type is I (internal), A (audit), or P (performance); that is, it excludes Sentinel Log Manager internal events.

The NOT operator cannot be used by itself because it is a way to exclude events from a set that has been found by other search terms. For example, consider the following query:

```
NOT st:I NOT st:A NOT st:P
```

This query might seem like it should return all events where the sensor type is not I, A, or P. However, it is an invalid query because a query cannot begin with the NOT operator.

Operator Precedence

Parentheses can be used in the usual way to change operator precedence. They can be nested to any depth, as shown in the following examples:

```
(sun:admin OR dun:admin) AND (sip:10.0.0.1 OR sip:10.0.0.2)
((sun:admin OR dun:admin) AND (sip:10.0.0.1 OR sip:10.0.0.2)) OR (msg:user AND
evt:authentication)
```

A.1.4 The Default Search Field

Lucene uses a default search field, which is the field that is searched if no field is specified. In Sentinel Log Manager, `_data` is the default search field. This field is a concatenation of all non-empty fields in the event. It is indexed and searched as a tokenized field. The result is that you can search for words that might appear in any event field.

For example, suppose you have two non-tokenized fields in an event, `sun` (initiatorusername) and `dun` (targetusername). The `sun` field has the following value:

```
report-administrator
```

The `dun` field has the following value:

```
system-tester
```

The `_data` field contains the concatenation of these fields separated by a single space character:

```
report-administrator system-tester
```

Because the `_data` field is a tokenized field, the words “report,” “administrator,” “system,” and “tester” are indexed and searchable. The following queries would find this event:

```
report
```

```
_data:report
```

```
report-administrator
```

```
_data:report-administrator
```

```
report tester
```

In addition, the following queries also find this event:

```
sun:report-administrator
```

```
dun:system-tester
```

A.1.5 Tokenized Fields

Fields that are classified as tokenized fields are parsed into individual words for indexing. Therefore, a search occurs only on words within the field value. Characters that are considered to be word delimiters are not searchable, nor are words that are considered to be stop words. Lucene removes extremely common words to save disk space and speed up searching. These words are ignored in search filters. Currently, the following stop words are removed:

- ◆ a
- ◆ an
- ◆ and
- ◆ are
- ◆ as
- ◆ at
- ◆ be
- ◆ but
- ◆ by
- ◆ for
- ◆ if
- ◆ in
- ◆ into
- ◆ is
- ◆ it
- ◆ no
- ◆ not
- ◆ of
- ◆ on
- ◆ or
- ◆ such

- ♦ that
- ♦ the
- ♦ their
- ♦ then
- ♦ there
- ♦ these
- ♦ they
- ♦ this
- ♦ to
- ♦ was
- ♦ will
- ♦ with

When it does a search, Lucene examines all of the words in a field and tries to match words in the search value. For example, suppose that you specify a search for messages containing the following value:

```
msg:"user-authentication failed on the server"
```

The words that are parsed within this value are “user,” “authentication,” “failed,” and “server.” These are the only search words that would match this value. “On” and “the” are omitted because they are stop words.

The value has the hyphen character (-) between some words. Hyphens are treated as word delimiters, so Lucene does not search for hyphens. Consider, the following query:

```
msg:"user-authentication"
```

The results might not be exactly what you expect. The query search value matches the value, but not because it is matching the hyphen. It matches because Lucene first parses the words in the search value and identifies the words “user” and “authentication.” Lucene then matches those words against values that have the words “user” and “authentication” with no intervening words in between. This query would also match the following value, even though there is no hyphen between “user” and “authentication”:

```
user authentication has failed on the server
```

Consider the following query:

```
msg:"failed on server"
```

This query has the stop word, “on,” which is ignored. However, the stop word does affect the relative positioning that is expected to be between words when evaluating a value to see if it matches. The “failed on server” search matches any phrase where the words “failed” and “server” are separated by exactly one word. It does not matter what the word is because the separating word is a stop word and is ignored. Thus, the above query would match all of the following:

```
failed on server
```

```
failed-on server
```

```
failed a server
```

```
failed-a-server
```

Proximity indicators created by using the ~ character followed by a value, make this more complicated. The query dictates an expected distance between words. In the “failed on server” query, the expected distance between “failed” and “server” is one word. The proximity indicator specifies how much variance there can be from the expected distance. For example, consider the following query, where a proximity indicator of one (~1) is specified:

```
msg:"failed on server"~1
```

This query indicates that the distance between “failed” and “server” could be plus or minus one from the expected distance, which is one because of the stop word “on.” Thus, the distance could be 1, 1-1 (0), or 1+1 (2). Thus, all of the following would match:

```
failed on server
```

```
failed on the server
```

```
failed finance server
```

As of Lucene version 3.1, word parsing is done according to word break rules outlined in the Unicode Text Segmentation algorithm. For more information, see [Unicode Text Segmentation \(http://www.unicode.org/reports/tr29/\)](http://www.unicode.org/reports/tr29/).

For information on tokenized fields in Sentinel Log Manager, in the Sentinel Log Manager Web interface *Tsearch tips* on the top right corner of the Sentinel Log Manager Web interface. A table is displayed that lists all the event fields and whether an event field is searchable or not.

A.1.6 Non-Tokenized Fields

Fields that are classified as non-tokenized fields are parsed fully for indexing. Thus, a search occurs on full field values. For example, to search events whose initiatoruserfullname (iufname) field has the value “Bob White”, you must specify the query as follows:

```
iufname:"Bob White"
```

A.2 Wildcards in Search Queries

Lucene supports wildcards in search values but not in regular expressions:

- ♦ The asterisk (*) matches zero or more characters.
- ♦ The questions mark (?) matches any one character.

For example:

- ♦ **adm*test**: Matches admtest, ADMTEST, admintest, adMINtEst (note the lack of case sensitivity).
- ♦ **adm?test**: Matches adm1test and AdMatest. Does not match admtest or ADMINTEST because it must have exactly one character between "adm" and "test."
- ♦ [Section A.2.1, “Wildcards in Tokenized Fields,” on page 187](#)
- ♦ [Section A.2.2, “Quoted Wildcards,” on page 187](#)
- ♦ [Section A.2.3, “Leading Wildcards,” on page 187](#)

A.2.1 Wildcards in Tokenized Fields

Wildcards are applied differently to tokenized fields and non-tokenized fields. Wildcards for tokenized fields match only words that were parsed from the value and not the entire value. For example, if you specify the search query `msg:authentication*failed` to search for the message `The user authentication has failed on the server`, it does not return the events with this message. This is because `*` does not match anything between `authentication` and `failed`. However, it matches any words that begin with `authentication` and end with `failed`. For example, it returns results if any of the following words are used: `authenticationhasfailed`, `authenticationuserfailed`, and `authenticationserverfailed`. For tokenized fields, all matching that uses wildcard searches is done on the words within the value and not on the full value.

A.2.2 Quoted Wildcards

- ♦ [“Tokenized Fields” on page 187](#)
- ♦ [“Non-Tokenized Fields” on page 187](#)

Tokenized Fields

When wildcards are quoted, they are not treated as wildcards, but as word delimiters. For example, consider the following query:

```
msg:"user* fail*"
```

The search value `"user* fail*"` is parsed into two words, `"user"` and `"fail"`. The semantic is "find any event where the `msg` field contains `"user"` AND `"fail"` words in that order, and there are no intervening words between them." Thus, it does not match the following value:

```
The user authentication has failed on the server.
```

This is because the wildcard is not treated as a wildcard but as a word delimiter.

Non-Tokenized Fields

When wildcards are quoted, they are treated as literal characters to search. For example, if the query is: `sun:"adm*,"` it returns the following values:

```
adm*
```

```
ADM* (case-insensitive)
```

The query does not return the following values:

```
admin
```

```
ADMIN
```

A.2.3 Leading Wildcards

Leading wildcards are not valid in searches because Lucene does not allow the `*` or `?` characters to be the first character of a search value. For example, the following queries are invalid:

- ♦ `sun:*adm*` The semantic is "find any event whose initiator username value contains the letters a, d, and m in sequence."
- ♦ `sun:*tester` The semantic is "find any event whose initiator username value ends with `"tester."`"

- ♦ **sun:*** The semantic is “find any event whose initiator username field is non-empty.”
Because this is an important type of query, Sentinel Log Manager provides an alternative way to accomplish this. For more information, see [Section A.3, “The notnull Query,”](#) on page 188.

A.3 The notnull Query

You might need to find events where some field is present, or non-empty. For example, to find all events that have a value in the sun field, you can specify the query as `sun: *`

The query does not return the expected results because Lucene does not support wildcards to be the first character of a search value. However, Sentinel Log Manager provides an alternate solution. For every event, Sentinel Log Manager creates a special field called `notnull`. The `notnull` field is a list of all fields in the event that are not null (not empty). For example, if there is an event that has values in the `evt`, `msg`, `sun`, and `xdasid` fields, the `notnull` field contains the following value:

```
evt msg sun xdasid
```

The `notnull` field is a tokenized field, so the following kinds of queries are possible:

- ♦ **notnull:sun** Finds all events whose sun field has a value.
- ♦ **notnull:xdas*** Finds all events where any field beginning with the name "xdas" has a value.

When a `notnull` field is added in Lucene, creating, indexing, and storing this field adds a cost to processing each event as CPU needs to create and index the field and it also requires additional storage space. If you want to disable storing the list of non-empty fields in the `notnull` field, set the following property in the `/etc/opt/novell/sentinel_log_mgr/config/configuration.properties` file:

```
indexedlog.storenotnull=false
```

Save the file and restart the Sentinel Log Manager server. All events received after this property was set do not have a `notnullfield` associated.

NOTE: If you disable the `notnull` field, do not use the `notnull` field in search filters, rule filters, or policy filters because the results might be incorrect and unpredictable.

A.4 Tags in Search Queries

The Tag field (`rv145`) is a tokenized field that has special parsing rules for words. The parsing rules enable you to search on tags that include non-alphanumeric characters. However, the only word delimiters are white space characters such as the blank and the tab. This is because tags do not include white space in their names. For example, the following queries find the event if the event is tagged with the `ISO/IEC_27002:2005` tag and the `NIST_800-53` tag:

```
rv145:"ISO/IEC_27002:2005"
```

```
rv145:"iso/iec_27002:2005"
```

```
rv145:ISO/IEC_27002*
```

```
rv145:nist_*
```

The slash (/), hyphen (-), and colon (:) characters are significant in the search value because, unlike other tokenized fields, the parsing rules for `rv145` do not treat them as a word delimiter. Also, the search is not case sensitive.

The following queries would not find the event:

```
rv145:"ISO IEC_27002 2005"
```

```
rv145:"iso *"
```

A.5 Range Queries

Range queries allow you to find events where a field value is between a lower bound and an upper bound. Range queries can be inclusive or exclusive of the upper and lower bounds. Whether a particular value falls in the specified range is based on lexicographic character sorting. Inclusive ranges are denoted by square brackets []. Exclusive ranges are denoted by curly brackets {}.

For example, consider the following query:

```
sun:[admin TO tester]
```

This query finds events whose sun field has values between admin and tester, inclusive. Note that "TO" is capitalized.

However, if you change the query as follows:

```
sun:{admin TO tester}
```

The query now finds all events whose sun field is between admin and tester, not including admin and tester.

Some event fields such as sev and xdasid are numeric. In Sentinel Log Manager, range queries on numeric fields are based on numeric sorting and not on lexicographic character sorting. For example, consider the following query:

```
xdasid:[1 TO 7]
```

This query returns events whose xdasid value is 1, 2, 3, 4, 5, 6, or 7. If the range evaluation was based on lexicographic sorting, it would incorrectly match 10, 101, 100001, 200, and so on.

A.6 IP Addresses Query

There are several extensions that Sentinel Log Manager has implemented for searching on IP addresses. Specifically, there are a number of convenient ways to specify IP address ranges. These are explained in the following sections:

- ♦ [Section A.6.1, "CIDR Notation," on page 189](#)
- ♦ [Section A.6.2, "Wildcards in IP Addresses," on page 190](#)

A.6.1 CIDR Notation

Sentinel Log Manager supports the Classless Inter-Domain Routing (CIDR) notation as a search value for IP address fields such as sip (initiator IP) and dip (target IP) for specifying an IP address range. The notation uses a combination of an IP address and a mask, as follows:

```
xxx.xxx.xxx.xxx/n
```

In this notation, n is the number of high order bits in the value to match. For example, consider the following query:

```
sip:10.0.0.0/24
```

This query returns events whose sip field is an IPv4 address ranging from 10.0.0.0 to 10.0.0.255.

A.6.2 Wildcards in IP Addresses

You can use only the asterisk character (*) in the IP address search values to specify ranges of IP addresses. You cannot use the question mark (?) character.

In IPv4 addresses, an asterisk (*) can be used at any of the positions in the quad format. For example, all of the following queries are valid on the sip field:

```
sip:10.*.80.16
```

```
sip:10.02.*.*
```

```
sip:10.*.80.*
```

If an asterisk (*) is used in one of the quad positions in an IPv4 address, it cannot be combined with other digits. For example, all of the following queries are invalid:

```
sip:10.*7.80.16
```

```
sip:10.10*.80.16
```

Because the question mark (?) is not allowed, the following queries are invalid:

```
sip:10.10?.80.16
```

```
sip:10.?.80.16
```

B Managing Data

- ♦ [Section B.1, “Moving Event Data Storage to a Large Partition,”](#) on page 191
- ♦ [Section B.2, “Directory Structure,”](#) on page 192
- ♦ [Section B.3, “Data Expiration Policy,”](#) on page 192

B.1 Moving Event Data Storage to a Large Partition

Use the YaST tool to add partitions in the appliance to increase the size available for the event data storage.

- 1 Log in to Sentinel Manager as root.
- 2 Run the following command to stop the Sentinel Log Manager on the appliance:

```
/etc/init.d/sentinel_log_manager stop
```
- 3 Specify the following command to change to novell user:

```
su -novell
```
- 4 Move the contents of the directory at `/var/opt/novell/sentinel_log_mgr/data` to a temporary location.
- 5 Change to root user.
- 6 Enter the following command to access the YaST2 Control Center:

```
yast
```
- 7 Select *System > Partitioner*.
- 8 Read the warning and select *Yes* to add the new unused partition.
- 9 Mount the new partition at `/var/opt/novell/sentinel_log_mgr/data`.
- 10 Specify the following command to change to novell user:

```
su -novell
```
- 11 Move the contents of the data directory from the temporary location (where it was saved in [Step 4](#)) back to `/var/opt/novell/sentinel_log_mgr/data`.
- 12 Change to root user.
- 13 Run the following command to restart the Sentinel Log Manager appliance:

```
/etc/init.d/sentinel_log_manager start
```

B.2 Directory Structure

By default, the data directories are in the following locations:

- ♦ The data files are in `/var/opt/novell/sentinel/data` and `/var/opt/novell/sentinel/3rdparty` directories.
- ♦ Executables and libraries are stored in the following directories:
 - ♦ `/opt/novell/sentinel/bin`
 - ♦ `/opt/novell/sentinel/setup`
 - ♦ `/opt/novell/sentinel/3rdparty`
- ♦ Log files are in the directory `/var/opt/novell/sentinel_log_mgr/log`
- ♦ Data is in the directory `/var/opt/novell/sentinel_log_mgr`
- ♦ Configuration files are in the directory `/etc/opt/novell/sentinel_log_mgr`
- ♦ The process ID (PID) file is in the directory `/var/run/sentinel_log_mgr/server.pid`.
Using the PID, administrators can identify the parent process of Sentinel Log Manager server and monitor or terminate the process.

B.3 Data Expiration Policy

This section lists the order in which Sentinel Log Manager chooses to delete data from the networked storage or from the local storage locations. Sentinel Log Manager deletes the data types in their listed order until the required space is available.

Data is deleted in the following order:

1. All partitions (both local storage and networked storage) are deleted as soon as the *keep at most* time limit of their retention policy completes.
2. Partitions that are successfully moved to networked storage (oldest first until none-left or the desired amount of space is available).
3. Partitions that are not yet moved to networked storage, but completed their retention policy's *keep at most* time limit (ordered by the largest amount of time completed the *keep at most* limit, until none left or the desired amount of space is available).
If at least half of the desired space is not yet been freed, then partitions are deleted prematurely, considering that the incoming data is more important than any old data.
4. Partitions that are not moved to networked storage and completed their policy's *keep at most* time limit (ordered by the shortest amount of time before the *keep at most* limit, until none left or at least half of the desired amount of space is available, but the current UTC day partitions are not deleted).

C Backing Up and Restoring Data

Novell Sentinel Log Manager provides a utility to backup and restore the data on the Sentinel Log Manager server. The backup and restore utility performs a back up of the system data and also restores the data at any given point in time without a considerable amount of effort. However, this utility cannot be used for backing up a Collector Manager or the appliance operating system.

You can back up the following data:

- ◆ **Configuration data:** Data stored in the `config`, `data`, `3rdparty/postgresql`, and `3rdparty/tomcat` directories, and the data in the Sentinel Log Manager database. This data includes configuration files, property files, and keystore files. The Sentinel database contains various configuration information related to users, plug-ins, Collectors, Connectors, and filters.

NOTE: The configuration data can be critical and you should always include the configuration data in the backup.

- ◆ **Event data:** Dynamic event data and raw event data stored in the `data/eventdata` and `data/rawdata` directories.
- ◆ **Networked storage data:** The closed event data files that have been moved to the networked storage.
- ◆ **Runtime data:** Dynamic file-based queues used by plug-ins, Sentinel Link, and other Sentinel Log Manager components. This includes the data in the `data/plugindata` and the `data/sentinel_link.queues` directories.

The backup and restore utility is a script that is controlled by various command line parameters as described in [Table C-1](#).

- ◆ [Section C.1, “Parameters for the Backup and Restore Utility Script,”](#) on page 193
- ◆ [Section C.2, “Running the Backup and Restore Utility Script,”](#) on page 195

C.1 Parameters for the Backup and Restore Utility Script

The following table lists the various command line parameters that you can use with the `backup_util.sh` script:

Table C-1 Backup and Restore Script Parameters

Parameters	Description
<code>-m backup</code>	Takes a backup of the specified data.

Parameters	Description
-m restore	<p>Restores the specified data. The restore mode of the script is interactive and allows you to specify the data to be restored from the backup file.</p> <p>The restore parameter can be used in the following scenarios:</p> <ul style="list-style-type: none"> ♦ System Failure: In the event of a system failure, you must first reinstall Sentinel Log Manager and then use the <code>backup_util.sh</code> script with the restore parameter to restore the most recent data that you had backed up. ♦ Data Loss: In the event of data loss, use the <code>backup_util.sh</code> script with the restore parameter to restore the most recent data that you had backed up. <p>You must restart the Sentinel Log Manager server after you restore any data because the script might make several modifications to the database.</p> <p>NOTE: The restore parameter is not backward compatible for local storage and networked storage data. Therefore, the local storage data and networked storage data can be restored only on the same or a later version of Sentinel Log Manager, and cannot be restored on an older version of Sentinel Log Manager.</p>
-m info	Displays the information for the specified backup file.
-m simple_event_backup	Specifies to back up events located in a specified directory.
-m simple_event_restore	Specifies to restore events into a specified directory.
-c	Takes a backup of the configuration data.
-e	Takes a backup of the local storage event data. If the backup is performed on the Sentinel Log Manager server, the current local storage partition is not backed up unless you shut down the Sentinel Log Manager server.
-dN	<p>Takes a backup of the event data for the specified number of days. The -dN option specifies to include the local storage event data from up to N days ago in the backup. Based on the current data retention policy settings, many days of events might be stored on the system. Backing up all of the event data might not always be necessary and might not be desirable. This option allows the specification of how many days to go back when backing up the event data. Example: -d7 includes only the event data from the last week in the backup.</p> <p>NOTE: If you specify only -d, event data will not be backed up. You must specify this parameter along with the -e parameter. For example:</p> <pre>backup_util.sh -m backup -e -d5 -f /var/opt/novell/sentinel_log_mgr/data/<events_5days_backup.tar.gz></pre>
-f	Enables you to specify the location and name of the backup file.
-l	Includes the log files in the backup. By default, the log files are not backed up unless you specify this option.
-r	Includes the runtime data in the backup. Runtime data can only be backed up if the Sentinel Log Manager server is shut down because the data is dynamic. This means that this flag can only be used in combination with the -s option (described below). If -s is not specified, this flag will be ignored.
-s	Shuts down the Sentinel Log Manager server before performing the backup. Shutting down the server is necessary to backup certain dynamic data such as the Runtime data and the current local storage partitions. By default, the server is not shut down before performing the backup. If this option is used, the server restarts automatically after the backup is complete.

Parameters	Description
-w	Specifies to include the raw event data in the backup.
-z	Only available with the <code>simple_event_backup</code> and <code>simple_event_restore</code> options. Specifies the location of the event data directory like where the event data is collected during a <code>simple_event_backup</code> and where the event data is placed during a <code>simple_event_restore</code> .

C.2 Running the Backup and Restore Utility Script

- 1 Open a console, and navigate to the `/opt/novell/sentinel_log_mgr/bin` directory as the novell user.
- 2 Enter `backup_util.sh`, along with the necessary parameters for the data that you want to back up or restore.

For more information on the different parameters, see [Table C-1](#). The following table lists examples of how to specify the parameters:

Syntax	Action
<code>backup_util.sh -m backup -c -e -l -s -f /var/opt/novell/sentinel_log_mgr/data/full_backup.tar.gz</code>	Shuts down the Sentinel Log Manager server and takes a backup of the complete system data. NOTE: If you have taken a full backup, the data can be restored only on same versions of Sentinel Log Manager.
<code>backup_util.sh -m backup -c -f /var/opt/novell/sentinel_log_mgr/data/config_backup.tar.gz</code>	Performs a local backup of the configuration data. This is a minimal backup of the system without any event data.
<code>backup_util.sh -m backup -e -f /var/opt/novell/sentinel_log_mgr/data/events_backup.tar.gz</code>	Performs a local backup of the event data. This is a minimal backup of the local storage event data.
<code>backup_util.sh -m backup -e -d5 -f /var/opt/novell/sentinel_log_mgr/data/events_5days_backup.tar.gz</code>	Performs a local backup of the event data from the last 5 days. This is a minimal backup of the local storage event data from the last five days.
<code>backup_util.sh -m info -f /var/opt/novell/sentinel_log_mgr/data/config_backup.tar.gz</code>	Displays the backup information for the specified backup file.
<code>backup_util.sh -m simple_event_backup -e -z /opt/archives/archive_dir -f /opt/archives/archive_backup.tar.gz</code>	Performs a backup of event data on the machine where the networked storage directory is located. You must manually copy the <code>backup_util.sh</code> script to the machine where the networked storage is located.
<code>backup_util.sh -m restore -f /var/opt/novell/sentinel_log_mgr/data/config_backup.tar.gz</code>	Restores the data from the specified filename.
<code>backup_util.sh -m simple_event_restore -z /opt/archives/archivedir -f /opt/archives/archive_backup.tar.gz</code>	Performs a restore of backed up networked storage data.

Syntax	Action
<code>backup_util.sh -m backup -c -e -l -r -s -w -f /var/opt/novell/sentinel_log_mgr/ data/<backupfilename></code>	Takes a full back up of the data and configuration. Stores the back up data in the specified back up filename.

- 3** (Conditional) If you have restored any data, restart the server because the script might make several modifications to the database.

Use the Data Restoration feature to restore the extracted partitions. For more information, see [Section 3.7.6, "Restoring Data," on page 51](#).

D Syslog Collector Package Policy

Event sources, Connectors, and Collectors can be auto-created based on policy information contained in installed Syslog Collector packages. These policies are specified in special properties of the connection modes in a SYSLOG connection method. A connection mode might contain an Applications, UniqueMatchingRule, or UniversalSyslogCollector property. These are described below:

NOTE: Only one of these properties should be specified.

Applications: This property contains a list of comma-separated application names for the syslog messages the Collector and connection mode can handle. Each application name in the list should be unique for all Collectors and connection modes. If multiple Collector plug-ins contain the same application name, only the first one spotted is used as authoritative. The log appliance logs a message stating that an application name is defined in multiple Collectors or connection modes, and also states, which one it selected as authoritative.

UniqueMatchingRule: This property contains a regular expression that can be used to find a matching syslog message. A device that generates a matching syslog message is assigned to this Collector and connection mode.

It is important that matching rules from different Collectors should never match the same message, to avoid ambiguity about which Collector/connection mode the device that generated the matching message should be assigned to.

UniversalSyslogCollector: This property should have a value of true. It specifies that the Collector/connection mode with this property is used for messages whose Collector/connection mode cannot be determined. It is the catch-all Collector and connection mode. There should be only one Collector/connection mode with this property. If more than one Collector and connection mode exists with this property, the log appliances logs an error and indicates which one it is using.

For the Collector and connection mode, only one of the above properties should be specified. If more than one property is specified, the log appliance logs a message and indicates which among the three properties it uses. It chooses the properties in the following order: 1) Applications, 2) UniqueMatchingRule, and 3) UniversalSyslogCollector

E Event Fields

Each event has its own fields. Based on the type of event, some fields in an event might not be populated. The values for these event fields can be viewed by using a search or running a report. Each field has a short name that is used in advanced searches. The values for most of these fields are visible in the detailed event view; other values are visible in the basic event view.

NOTE: The taxonomy values that you can search for the TaxonomyLevel* and XDAS* fields are documented at the [Sentinel Taxonomy Web page \(http://developer.novell.com/wiki/index.php/Sentinel_Taxonomy\)](http://developer.novell.com/wiki/index.php/Sentinel_Taxonomy).

Some fields are tokenized. Tokenizing also makes it possible to search for an individual word in the field without a wildcard. The fields are tokenized based on spaces and other special characters. For these fields, articles such as “a” or “the” is removed from the search index.

Tokenized fields are marked in the following table and these fields are not case-sensitive while performing a search.

NOTE: In addition to the below mentioned tokenized field, if you do a search without specifying a field name (full text search), that search will be performed tokenized (not case-sensitive).

Table E-1 *Event Fields*

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
Collector	port	Name of the Collector that generated this event.			
CollectorId	rv22	Unique identifier for the Collector which generated this event.			
CollectorManagerId	rv21	Unique identifier for the Collector Manager which generated this event.			
CollectorScript	agent	The name of the Collector Script used by the Collector to generate this event.	Y		Y
ConnectorId	rv23	Unique identifier for the Connector which generated this event.			
ControlMonitor	rv27	Control categorization - level 2	Y		
ControlPack	rv26	Control categorization - level 1	Y		

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
CorrelatedEventUuids	ceu	List of event UUIDs associated with this correlated event. Only relevant for correlated events.			
Criticality	crt	The criticality of the asset identified in this event.			
Ct1	ct1	Reserved for use by customers for customer-specific data. (String)			
Ct2	ct2	Reserved for use by customers for customer-specific data. (String)			
Ct3	ct3	Reserved for use by customers for customer-specific data. (Number)			
CustomerHierarchyId	rv1	Customer Hierarchy Id			
CustomerHierarchyLevel1	rv49	Customer Hierarchy Level 1	Y		
CustomerHierarchyLevel2	rv54	Customer Hierarchy Level 2			
CustomerHierarchyLevel3	rv55	Customer Hierarchy Level 3			
CustomerHierarchyLevel4	rv100	Customer Hierarchy Level 4			
CustomerVar1-CustomerVar10	cv1-10	Reserved for use by customers for customer-specific data. (Number)	Y		Y
CustomerVar100	cv100	Reserved for use by customers for customer-specific data. (String)			
CustomerVar101-CustomerVar130	cv101-130	Reserved for use by customers for customer-specific data. (Integer; Stored in DB)			
CustomerVar11-CustomerVar20	cv11-20	Reserved for use by customers for customer-specific data. (Date)	Y		
CustomerVar131-140	cv131-140	Reserved for use by customers for customer-specific data. (IPv4; Stored in DB)	Y		
CustomerVar141-150	cv141-150	Reserved for use by customers for customer-specific data. (String; Stored in DB)	Y		
CustomerVar151-160	cv151-160	Reserved for use by customers for customer-specific data. (Integer; Not stored in DB)	Y		

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
CustomerVar161-170	cv161-170	Reserved for use by customers for customer-specific data. (Date; Not stored in DB)	Y		
CustomerVar171-180	cv171-180	Reserved for use by customers for customer-specific data. (UUID; Not stored in DB)	Y		
CustomerVar181-190	cv181-190	Reserved for use by customers for customer-specific data. (IPv4; Not stored in DB)	Y		
CustomerVar191-200	cv191-200	Reserved for use by customers for customer-specific data. (String; Not stored in DB)	Y		
CustomerVar21-99	cv21-99	Reserved for use by customers for customer-specific data. (String)	Y		
DataCotext	rv36	Container for the FileName data object (for example, a directory for a file or a database instance for a database table)	Y		Y
DataTagId	rv3	An Id for user-defined event tagging.			
DataValue43	rv43	Data Value. (String)	Y		
DeviceCategory	rv32	Device category (FW, IDS, AV, OS, DB).			
DeviceName	rv31	The name of the device generating the event. If this device is supported by Advisor, the name should match the name known by Advisor. (String)	Y	Y	
EffectiveUserDomain	eudom	The domain (namespace) in which the effective user account exists.			Y
EffectiveUserID	euid	Numerical ID of the user that the InitUser is impersonating (<code>root</code> using <code>su</code> , for example), based on the raw data reported by the device.			Y
EffectiveUserName	euname	The name of the account that is effectively being used.			Y
EventContext	rv33	Event context (threat level).	Y		
EventGroupID	evtgrpid	A source-specific identifier to group multiple related events together.			Y

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
EventMetric	rv2	An event-dependent numeric value.			Y
EventMetricClass	rv28	The class of the event-dependent numeric value.			
EventName	evt	The descriptive name of the event as reported (or given) by the sensor. Example Port Scan.	Y	Y	Y
EventSourceId	rv24	Unique identifier for the Event Source which generated this event.			Y
ExtendedInformation	ei	Stores additional Collector processed information. Values within this variable are separated by semi-colons (;).	Y		Y
FISMA	cv93	Set to 1 if the asset is governed by the Federal Information Security Management Act (FISMA) regulation via an asset map. (String)			
GLBA	cv92	Set to 1 if the asset is governed by the Gramm-Leach Bliley Act regulation via an asset map. (String)			
HIPAA	cv91	Set to 1 if the asset is governed by the Health Insurance Portability and Accountability Act regulation via an asset map. (String)			
InitFunction	rv37	Initiator function.	Y		
InitHostDomain	rv42	The domain portion of the initiating system's fully-qualified hostname.		Y	Y
InitHostName	shn	The unqualified host name of the initiating system.		Y	Y
InitIP	sip	The IPv4 address of the initiating system.			Y
InitIPCountry	rv29	The country where the IPv4 address of the initiating system is located.	Y		
InitOperationalContext	rv38	Initiator operational context.	Y		
InitServiceComp	isvcc	The subcomponent of the initiating service that caused this event.	Y		

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
InitServiceName	sp	The name of the initiating service that caused this event.			Y
InitServicePort	spint	The port used by the service/application that initiated the connection.			Y
InitThreatLevel	rv34	Initiator threat level.			
InitUserDepartment	iudep	The department of the identity associated with the initiating account.	Y		
InitUserDomain	rv35	The domain (namespace) in which the initiating account exists.		Y	
InitUserFullName	iufname	The full name of the identity associated with the initiating account.	Y	Y	Y
InitUserID	iuid	The initiating account's source-specific identifier as determined by the Collector based on raw device data.			Y
InitUserIdentity	iuident	The internal UUID of the identity associated with the initiating account.			
InitUserName	sun	The initiating user's account name (SourceUsername).		Y	Y
Message	msg	Free-form message text for the event.		Y	Y
MSSPCustomerName	rv39	Name of the MSSP customer.			
NISPOM	cv94	Set to 1 if the asset is governed by National Industrial Security Program Operating Manual (NISPOM) regulation via an asset map. (String)			
ObserverChannel	rv150	The channel on which the observer delivered the event, for multi-channel protocols. An example would be the syslog facility. (String; Stored in DB)			Y
ObserverHostDomain	obsdom	The domain portion of the observer's (sensor) fully qualified hostname.			Y
ObserverHostName	sn	The unqualified hostname of the observer of the event (SensorName).			Y

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
ObserverIP	obsip	The IP address of the observer (sensor) that detected the event.			Y
ProductName	pn	Indicates the type, vendor and product code name of the sensor from which the event was generated.	Y	Y	Y
Protocol	prot	The protocol used between the initiating and target services.			Y
RepeatCount	rc	The number of times the same event occurred if multiple occurrences were consolidated.			Y
ReporterHostDomain	repdom	The domain portion of the reporter's fully qualified hostname.			Y
ReporterHostName	rn	The unqualified hostname of the reporter of the event (ReporterName).			Y
ReporterIP	repip	The IP address of the reporter, i.e. the system that delivered the event to this server.			Y
Resource	res	The resource name.			
RetentionPolicyConflict	rv101	Set to 1 (true) if more than one retention policy matched this event but only one was chosen. (Integer; Stored in DB)			Y
SARBOX	cv90	Set to 1 if the asset is governed by Sarbanes-Oxley via an asset map. (String)			
SensorType	st	The single character designator for the sensor type (N, H, O, V, C, W, A, I).			
SentinelServiceID	src	Unique identifier for the Sentinel service which generated this event.			
Severity	sev	The normalized severity of the event (0-5).		Y	Y
SubResource	sres	The sub-resource name.	Y		
Tags	rv145	A comma separated list of tags (such as PCI) applied to the event.	Y		Y
TargetDataName	fn	The name of the data object (file, database table, directory object, etc) that was affected by this event.			Y

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
TargetFunction	rv47	Target function.	Y		
TargetHostDomain	rv41	The domain portion of the target system's fully-qualified hostname.		Y	Y
TargetHostName	dhn	The unqualified hostname of the target system.		Y	Y
TargetIP	dip	The IPv4 address of the target system.			Y
TargetIPCountry	rv30	The country where the IPv4 address of the target system is located.	Y		
TargetOperationalContext	rv48	Target operational context.	Y		
TargetServiceComponent	tsvcc	The subcomponent of the target service affected by this event.	Y		
TargetServiceName	dp	The name of the target service affected by this event.			Y
TargetServicePort	dpint	The network port accessed on the target.			Y
TargetThreatLevel	rv44	Target threat level.			
TargetTrustDomain	ttd	The domain (namespace) within which the target trust exists.			
TargetTrustID	ttid	The source-specific identifier of the trust (group, role, profile, etc) affected.			
TargetTrustName	ttn	The name of the trust (group, role, profile, etc) affected.			
TargetUserDepartment	tudep	The department of the identity associated with the target account.	Y		
TargetUserDomain	rv45	The domain (namespace) in which the target account exists.			Y
TargetUserFullName	tufname	The full name of the identity associated with the target account.	Y		
TargetUserID	tuid	The target account's source-specific identifier as determined by the Collector based on raw device data.			Y
TargetUserIdentity	tuident	The internal UUID of the identity associated with the target account.			

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
TargetUserName	dun	The target user's account name (DestinationUsername).		Y	Y
TaxonomyLevel1	rv50	Event code categorization - level 1. Displayed under the event name in the format: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	Y	Y	Y
TaxonomyLevel2	rv51	Event code categorization - level 2. Displayed under the event name in the format: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	Y	Y	Y
TaxonomyLevel3	rv52	Event code categorization - level 3. Displayed under the event name in the format: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	Y	Y	Y
TaxonomyLevel4	rv53	Event code categorization - level 4. Displayed under the event name in the format: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	Y	Y	Y
VendorEventCode	rv40	Event code reported by device vendor. (String)			
VirusStatus	rv46	Virus status.			
Vulnerability	vul	The vulnerability of the asset identified in this event.			
XDASClass	xdasclass	The XDAS Event Class ID; refer to XDAS specification.			
XDASDetail	xdasdetail	The XDAS outcome detail; refer to XDAS specification.			
XDASIdentifier	xdasid	The XDAS Event Identifier; refer to XDAS specification.			
XDASOutcome	xdasoutcome	The XDAS major outcome; success, failure, or denial.			

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
XDASOutcomeName	xdasoutcomename	Human-readable XDAS outcome.	Y	Y	
XDASProvider	xdasprov	The XDAS Provider ID; refer to XDAS specification.			
XDASRegistry	xdasreg	The XDAS Registry ID; refer to XDAS specification.			
XDASTaxonomyName	xdastaxname	Human-readable XDAS event taxonomy string.	Y	Y	

F Troubleshooting

This section contains some of the common error messages reported in Sentinel Log Manager, along with the probable troubleshooting measures.

F.1 Data Retention Policies are not Displayed when there is Large Data in the Networked Storage

Sentinel Log Manager does not display the data retention policies if there is huge data in the networked storage. The `du` command runs for a longer time to find the disk usage and a message is displayed in the Web user interface indicating that refreshing retention policies timed out.

Workaround: Increase the time out period so that Sentinel Log Manager does not time out before retrieving the disk usage space.

1. Log in to Sentinel Log Manager as `novell` user.
2. Open the `/etc/opt/novell/sentinel_log_mgr/config/server.xml` file in an editor.
3. Modify the `taskTimeoutPeriod` and `diskStatsCheckInterval` properties in the `DiskStatisticsCache` component such that the `taskTimeoutPeriod` is lesser than or equal to `diskStatsCheckInterval`. These value are in milliseconds.

```
<obj-component id="DiskStatisticsCache">
<class>esecurity.ccs.comp.diskstatistics.DiskStatisticsCache</class>
<property name="emaSmoothingFactor">0.2</property>
<property name="diskStatsCheckInterval">400000</property>
<property name="taskTimeoutPeriod">300000</property>
</obj-component>
```

4. Restart Sentinel Log Manager.

F.2 Unable to Log In to the Web Interface when the System runs out of Local Disk Storage Space

When the system runs out of local disk storage space, the `Invalid username/password` message is displayed when you log in to the web interface. The following exceptions are logged in the `server_wrapper` logs:

```
SEVERE | IndexedLogComponent.LoggerThread | Unknown.unknown
    Unable to log event.; Exception Lock obtain timed out:
NativeFSLock@/var/opt/novell/sentinel_log_mgr/data/eventdata/20111122_408E7E50-
C02E-4325-B7C5-2B9FE4853476/index/write.lock;
org.apache.lucene.store.LockObtainFailedException;
```

```
SEVERE|IndexedLogComponent.LoggerThread|Unknown.unknown
    Unable to log event.; Exception No space left on device;
java.io.IOException;
SEVERE|IndexedLogComponent.LoggerThread|Unknown.unknown
    java.io.IOException: No space left on device
    at java.io.RandomAccessFile.writeBytes(Native Method)
    at java.io.RandomAccessFile.write(Unknown Source)
```

Workaround: Restart the Sentinel Log Manager server. To avoid this issue, configure the local disk storage space per system requirements. For more information, see “[Hardware Requirements](#)” in the *Sentinel Log Manager 1.2.2 Installation Guide*.

G Internal Audit Events

This section lists the various internal events that are generated by the various components in Sentinel Log Manager such as Event Source Management, User Management, Report definitions and report results, and so on. The events are grouped component wise.

- ◆ [Section G.1, “Authentication Events,” on page 211](#)
- ◆ [Section G.2, “User Management,” on page 213](#)
- ◆ [Section G.3, “Event Router,” on page 217](#)
- ◆ [Section G.4, “Event Source Management - General,” on page 218](#)
- ◆ [Section G.5, “Event Source Management - Event Sources,” on page 227](#)
- ◆ [Section G.6, “Event Source Management - Collectors,” on page 229](#)
- ◆ [Section G.7, “Event Source Management - Event Source Servers,” on page 230](#)
- ◆ [Section G.8, “Event Source Management - Connectors,” on page 231](#)
- ◆ [Section G.9, “Data Objects,” on page 235](#)
- ◆ [Section G.10, “Search,” on page 235](#)
- ◆ [Section G.11, “Data Retention Policy,” on page 235](#)
- ◆ [Section G.12, “Disk Usage Configuration,” on page 237](#)
- ◆ [Section G.13, “Report Definitions and Report Results,” on page 237](#)
- ◆ [Section G.14, “General,” on page 238](#)

G.1 Authentication Events

- ◆ [Section G.1.1, “Authentication,” on page 211](#)
- ◆ [Section G.1.2, “Failed Authentication,” on page 212](#)
- ◆ [Section G.1.3, “Web User Interface Login,” on page 212](#)
- ◆ [Section G.1.4, “Web User Interface Login Failed,” on page 212](#)
- ◆ [Section G.1.5, “User Logged In,” on page 213](#)
- ◆ [Section G.1.6, “User Logged Out,” on page 213](#)

G.1.1 Authentication

Table G-1 Authentication Events - Authentication

Tag	Value
Severity	1

Tag	Value
Event Name	Authentication
Resource	UserAuthentication
SubResource	Authenticate
Message	User <username> has passed authentication to Sentinel/Wizard

G.1.2 Failed Authentication

Table G-2 Authentication Events - Failed Authentication

Tag	Value
Severity	4
Event Name	AuthenticationFailed
Resource	UserAuthentication
SubResource	Authenticate
Message	Authentication of user <username> with OS name <domUser> from <IP> failed

G.1.3 Web User Interface Login

Table G-3 Authentication Events - Web UI Login

Tag	Value
Severity	1
Event Name	LoginUser
Resource	SessionServices
SubResource	SessionServices
Message	Logging in user:<username>

G.1.4 Web User Interface Login Failed

Table G-4 Authentication Events - Web UI Login Failed

Tag	Value
Severity	4
Event Name	LoginUser-*-Failed
Resource	SessionServices

Tag	Value
SubResource	SessionServices
Message	Logging in user:<username>

G.1.5 User Logged In

Table G-5 Authentication Events - User Logged In

Tag	Value
Severity	1
Event Name	UserLoggedIn
Resource	UserSessionManager
SubResource	User
Message	User <username> with OS name <osName> at <IP> logged in; currently <number> active users

G.1.6 User Logged Out

Table G-6 Authentication Events - User Logged Out

Tag	Value
Severity	1
Event Name	UserLoggedOut
Resource	UserSessionManager
SubResource	User
Message	Closing session for <username> OS name <osName> from <IP> was on since <date>; currently <number> active users

G.2 User Management

- ♦ [Section G.2.1, "Create User," on page 214](#)
- ♦ [Section G.2.2, "Create User Role," on page 214](#)
- ♦ [Section G.2.3, "Add User To Role," on page 214](#)
- ♦ [Section G.2.4, "Removing User From a Role," on page 215](#)
- ♦ [Section G.2.5, "Updating User," on page 215](#)
- ♦ [Section G.2.6, "Updating User Role," on page 215](#)
- ♦ [Section G.2.7, "Delete User," on page 216](#)

- ♦ [Section G.2.8, “Delete User Role,”](#) on page 216
- ♦ [Section G.2.9, “Resetting User Password,”](#) on page 216

G.2.1 Create User

Table G-7 *User Management - Create User*

Tag	Value
Severity	1
EventName	CreateUser
Resource	Config
SubResource	UserManagementService
Message	Creating user account <username> with Last name: <lastname>, First name: <firstname>

G.2.2 Create User Role

Table G-8 *User Management - Create User Role*

Tag	Value
Severity	1
Event Name	CreateUserRole
Resource	Core
SubResource	UserGroupsPermissionService
Message	Creating role <role_name>, users with this role can: <permissions>

G.2.3 Add User To Role

Table G-9 *User Management - Add User To Role*

Tag	Value
Severity	1
Event Name	AddUserToRole
Resource	Core
SubResource	UserGroupsPermissionService
Message	Adding User: <username> to Role: <role_name>

G.2.4 Removing User From a Role

Table G-10 User Management - Removing User From a Role

Tag	Value
Severity	1
Event Name	RemoveUserFromRole
Resource	Core
SubResource	UserGroupsPermissionService
Message	Removing User: <username> from Role: <username>

G.2.5 Updating User

Table G-11 User Management - Updating User

Tag	Value
Severity	1
Event Name	UpdateUser
Resource	Config
SubResource	UserManagementService
Message	Updating User: <username>

G.2.6 Updating User Role

Table G-12 User Management - Updating User Role

Tag	Value
Severity	1
Event Name	UpdateUserRole
Resource	Core
SubResource	UserGroupPermissionService
Message	Updating role: <rolename>, users with this role can now: <rolepermission>

G.2.7 Delete User

Table G-13 User Management - Delete User

Tag	Value
Severity	1
Event Name	DeleteUser
Resource	Config
SubResource	UserManagementService
Message	Deleting User Account: <username>

G.2.8 Delete User Role

Table G-14 User Management - Delete User Role

Tag	Value
Severity	1
Event Name	DeleteUserRole
Resource	Core
SubResource	UserGroupsPermissionService
Message	Deleting User Role: <username>

G.2.9 Resetting User Password

Table G-15 Resetting User Password

Tag	Value
Severity	1
Event Name	ResettingUserPassword
Resource	Config
SubResource	UserManagementService
Message	Resetting password for User Account <username>

G.3 Event Router

Event router is the main component of the Collector Manager. The event router performs the maps, applies global filters, and publishes events.

- ♦ [Section G.3.1, “Event Router is Initializing,” on page 217](#)
- ♦ [Section G.3.2, “Event Router is Running,” on page 217](#)
- ♦ [Section G.3.3, “Event Router is Stopping,” on page 218](#)
- ♦ [Section G.3.4, “Event Router is Terminating,” on page 218](#)

G.3.1 Event Router is Initializing

This event is sent when an event router starts its initialization. The event router starts initializing when it has established a connection with the backend (DAS Query).

Table G-16 *Event Router - Event Router is Initializing*

Tag	Value
Severity	1
Event Name	EventRouterInitializing
Resource	CollectorManager
SubResource	EventRouter
Message	Event router is initializing in standalone mode; reqId(1EEAD430-E790-1029-93AC-000C296FC5D4)

G.3.2 Event Router is Running

This internal event is sent when the event router is ready during initialization. When the Collector Manager is restarted, another event is sent when it is ready.

This event is not sent until the event router successfully loaded all the global filters and map information.

Table G-17 *Event Router - Event Router is Running*

Tag	Value
Severity	1
Event Name	EventRouterIsRunning
Resource	CollectorManager
SubResource	
Message	

G.3.3 Event Router is Stopping

This event is sent when a request is received by the event router to stop during shutdown.

Table G-18 *Event Router - Event Router is Stopping*

Tag	Value
Severity	2
Event Name	EventRouterStopping
Resource	CollectorManager
SubResource	EventRouter
Message	Event router is stopping; reqId(B408EC15-F4D2-1029-A795-000C296FC5D4)

G.3.4 Event Router is Terminating

This event is sent when a request is received by the event router to stop during shutdown.

Table G-19 *Event Router - Event Router is Terminating*

Tag	Value
Severity	2
Event Name	EventRouterTerminating
Resource	CollectorManager
SubResource	EventRouter
Message	Event router is terminating; reqId(B408EC15-F4D2-1029-A797-000C296FC5D4)

G.4 Event Source Management - General

- ◆ [Section G.4.1, “Collector Manager Initialized,” on page 219](#)
- ◆ [Section G.4.2, “Collector Manager Is Down,” on page 219](#)
- ◆ [Section G.4.3, “Collector Manager Started,” on page 220](#)
- ◆ [Section G.4.4, “Collector Manager Stopped,” on page 220](#)
- ◆ [Section G.4.5, “Collector Service Callback,” on page 220](#)
- ◆ [Section G.4.6, “Event Source Manager Callback,” on page 221](#)
- ◆ [Section G.4.7, “Initializing Collector Manager,” on page 221](#)
- ◆ [Section G.4.8, “Update Collector Manager,” on page 221](#)
- ◆ [Section G.4.9, “Lost Contact With Collector Manager,” on page 222](#)
- ◆ [Section G.4.10, “No Data Alert,” on page 222](#)
- ◆ [Section G.4.11, “Persistent Process Died,” on page 222](#)

- ♦ Section G.4.12, “Persistent Process Restarted,” on page 223
- ♦ Section G.4.13, “Port Start,” on page 223
- ♦ Section G.4.14, “Port Stop,” on page 223
- ♦ Section G.4.15, “Reestablished Contact With Collector Manager,” on page 224
- ♦ Section G.4.16, “Restart Plugin Deployments,” on page 224
- ♦ Section G.4.17, “Restarting Collector Manager (Cold Restart),” on page 224
- ♦ Section G.4.18, “Restarting Collector Manager (Warm Restart),” on page 225
- ♦ Section G.4.19, “Start Event Source Group,” on page 225
- ♦ Section G.4.20, “Start Event Source Manager,” on page 225
- ♦ Section G.4.21, “Starting Collector Manager,” on page 226
- ♦ Section G.4.22, “Stop Event Source Group,” on page 226
- ♦ Section G.4.23, “Stop Event Source Manager,” on page 226
- ♦ Section G.4.24, “Stopping Collector Manager,” on page 227

G.4.1 Collector Manager Initialized

Table G-20 Event Source Management (General) - Collector Manager Initialized

Tag	Value
Severity	1
Event Name	CollectorManagerInitialized
Resource	CollectorManager
SubResource	Internal
Message	Initialized Collector Manager...

G.4.2 Collector Manager Is Down

Table G-21 Event Source Management (General) - Collector Manager Is Down

Tag	Value
Severity	
Event Name	CollectorManagerDown
Resource	HealthManager
SubResource	CollectorManagerHealth
Message	Collector manager <name> UUID {1} is down for {2} days {3} hrs {4} min

G.4.3 Collector Manager Started

Table G-22 *Event Source Management (General) - Collector Manager Started*

Tag	Value
Severity	1
Event Name	CollectorManagerStarted
Resource	CollectorManager
SubResource	Internal
Message	Started Collector Manager...

G.4.4 Collector Manager Stopped

Table G-23 *Event Source Management (General) - Collector Manager Stopped*

Tag	Value
Severity	1
Event Name	CollectorManagerStopped
Resource	CollectorManager
SubResource	Internal
Message	Stopped Collector Manager...

G.4.5 Collector Service Callback

Table G-24 *Event Source Management (General) - Collector Service Callback*

Tag	Value
Severity	1
Event Name	restart
Resource	
SubResource	CollectorServiceCallback
Message	Restart Collector with Id: <ID>

G.4.6 Event Source Manager Callback

Table G-25 Event Source Management (General) - Event Source Manager Callback

Tag	Value
Severity	1
Event Name	restart
Resource	
SubResource	EventSourceManagerCallback
Message	Restart node with Id: <ID>

G.4.7 Initializing Collector Manager

Table G-26 Event Source Management (General) - Initializing Collector Manager

Tag	Value
Severity	1
Event Name	CollectorManagerInitializing
Resource	CollectorManager
SubResource	Internal
Message	Initializing Collector Manager...

G.4.8 Update Collector Manager

Table G-27 Event Source Management (General) - Update Collector Manager

Tag	Value
Severity	1
Event Name	UpdateCollectorManagerConfiguration
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Updating Collector Manager <name> configuration with <id>. <updates>

G.4.9 Lost Contact With Collector Manager

Table G-28 Event Source Management (General) - Lost Contact With Collector Manager

Tag	Value
Severity	
Event Name	LostContactWithCollectorManager
Resource	HealthManager
SubResource	CollectorManagerHealth
Message	Lost contact with collector manager <name> UUID {1}--down for {2} days {3} hrs {4} min

G.4.10 No Data Alert

Table G-29 Event Source Management (General) - No Data Alert

Tag	Value
Severity	1
Event Name	NoDataAlert
Resource	CollectorManager
SubResource	objectName
Message	No data received for {7} {0} (ID {1}) for last {2} days {3} hrs {4} min {5} sec (threshold {6} ms)

G.4.11 Persistent Process Died

Collector Engine sends this event when the persistent process Connector detects that its controlled process has died.

Table G-30 Event Source Management (General) - Persistent Process Died

Tag	Value
Severity	5
Event Name	PersistentProcessDied
Resource	AgentManager
SubResource	AgentManager
Message	Persistent Process on port <port ID> has died.

G.4.12 Persistent Process Restarted

Collector Engine sends this event when the persistent process Connector is able to restart the controlled process that had died.

Table G-31 *Event Source Management (General) - Persistent Process Restarted*

Tag	Value
Severity	1
Event Name	PersistentProcessRestarted
Resource	AgentManager
SubResource	AgentManager
Message	Persistent Process on port <port ID> has restarted.

G.4.13 Port Start

Collector Manager sends this event when a port is started.

Table G-32 *Event Source Management (General) - Port Start*

Tag	Value
Severity	1
Event Name	PortStart
Resource	AgentManager
SubResource	AgentManager
Message	Processing started for port_<port ID>

G.4.14 Port Stop

Collector Manager sends this event when a port is stopped.

Table G-33 *Event Source Management (General) - Port Stop*

Tag	Value
Severity	1
Event Name	PortStop
Resource	AgentManager
SubResource	AgentManager
Message	Processing stopped for port_<port ID>

G.4.15 Reestablished Contact With Collector Manager

Table G-34 Event Source Management (General) - Reestablished Contact With Collector Manager

Tag	Value
Severity	
Event Name	ReestablishedContactWithCollectorManager
Resource	HealthManager
SubResource	CollectorManagerHealth
Message	Reestablished contact with collector manager {0} UUID {1} after {2} days {3} hrs {4} min

G.4.16 Restart Plugin Deployments

Table G-35 Event Source Management (General) - Restart Plugin Deployments

Tag	Value
Severity	
Event Name	restartPluginDeployments
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Restart deployments of plugin: {0}

G.4.17 Restarting Collector Manager (Cold Restart)

Table G-36 Event Source Management (General) - Restarting Collector Manager (Cold Restart)

Tag	Value
Severity	1
Event Name	CollectorManagerRestart
Resource	CollectorManager
SubResource	Internal
Message	Restarting Collector Manager (Cold restart)

G.4.18 Restarting Collector Manager (Warm Restart)

Table G-37 Event Source Management (General) - Restarting Collector Manager (Warm Restart)

Tag	Value
Severity	1
Event Name	CollectorManagerRestart
Resource	CollectorManager
SubResource	Internal
Message	Restarting Collector Manager (Warm restart)

G.4.19 Start Event Source Group

Table G-38 Event Source Management (General) - Start Event Source Group

Tag	Value
Severity	1
Event Name	startEventSourceGroup
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Start Connector: {0}

G.4.20 Start Event Source Manager

Table G-39 Event Source Management (General) - Start Event Source Manager

Tag	Value
Severity	1
Event Name	startEventSourceManager
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Start Collector Manager: <eventSourceManagerID>

G.4.21 Starting Collector Manager

Table G-40 Event Source Management (General) - Starting Collector Manager

Tag	Value
Severity	1
Event Name	CollectorManagerStarting
Resource	CollectorManager
SubResource	Internal
Message	Starting Collector Manager

G.4.22 Stop Event Source Group

Table G-41 Event Source Management (General) - Stop Event Source Group

Tag	Value
Severity	1
Event Name	stopEventSourceGroup
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Stop Connector: {0}

G.4.23 Stop Event Source Manager

Table G-42 Event Source Management (General) - Stop Event Source Manager

Tag	Value
Severity	1
Event Name	StopEventSourceManager
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Stop Collector Manager: <eventSourceManagerID>

G.4.24 Stopping Collector Manager

Table G-43 Event Source Management (General) - Stopping Collector Manager

Tag	Value
Severity	1
Event Name	CollectorManagerStopping
Resource	CollectorManager
SubResource	Internal
Message	Stopping Collector Manager...

G.5 Event Source Management - Event Sources

- ◆ [Section G.5.1, “Start Event Source,” on page 227](#)
- ◆ [Section G.5.2, “Stop Event Source,” on page 227](#)
- ◆ [Section G.5.3, “Start Event Sources,” on page 228](#)
- ◆ [Section G.5.4, “Stop Event Sources,” on page 228](#)
- ◆ [Section G.5.5, “Update Event Source Configuration,” on page 228](#)

G.5.1 Start Event Source

Table G-44 Event Source Management (Event Sources) - Start Event Source

Tag	Value
Severity	
Event Name	startEventSource
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Start EventSource: {0}

G.5.2 Stop Event Source

Table G-45 Event Source Management (Event Sources) - Stop Event Source

Tag	Value
Severity	
Event Name	stopEventSource
Resource	EventSourceManagement

Tag	Value
SubResource	EventSourceManagerService
Message	Stop EventSource: {0}

G.5.3 Start Event Sources

This event is generated when multiple event sources are started at once.

Table G-46 Event Source Management (Event Sources) - Start Event Source

Tag	Value
Severity	1
Event Name	startEventSource
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Starting event sources <names of event sources> with ids < corresponding ids of event sources>

G.5.4 Stop Event Sources

This event is generated when multiple event sources are stopped at once.

Table G-47 Event Source Management (Event Sources) - Stop Event Source

Tag	Value
Severity	1
Event Name	stopEventSource
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Stopping event sources <names of event sources> with ids < corresponding ids of event sources>

G.5.5 Update Event Source Configuration

Table G-48 Event Source Management (Event Sources) - Update Event Source Configuration

Tag	Value
Severity	1
Event Name	UpdateEventSourceConfiguration
Resource	EventSourceManagement

Tag	Value
SubResource	EventSourceManagerService
Message	Updating event source <name> with id <id>.<updates>

G.6 Event Source Management - Collectors

- ♦ [Section G.6.1, “Start Collector,” on page 229](#)
- ♦ [Section G.6.2, “Stop Collector,” on page 229](#)
- ♦ [Section G.6.3, “Update Collector Configuration,” on page 229](#)

G.6.1 Start Collector

Table G-49 Event Source Management (Collectors) - Start Collector

Tag	Value
Severity	1
Event Name	startCollector
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Start Collector: {0}

G.6.2 Stop Collector

Table G-50 Event Source Management (Collectors)- Stop Collector

Tag	Value
Severity	1
Event Name	stopCollector
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Stop Collector: {0}

G.6.3 Update Collector Configuration

Table G-51 Event Source Management (Collectors)- Update Collector Configuration

Tag	Value
Severity	1

Tag	Value
Event Name	UpdateCollectorConfiguration
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Updating collector <name> with id <id>. <updates>

G.7 Event Source Management - Event Source Servers

- ♦ [Section G.7.1, “Start Event Source Server,” on page 230](#)
- ♦ [Section G.7.2, “Stop Event Source Server,” on page 230](#)
- ♦ [Section G.7.3, “Update Event Source Server Configuration,” on page 231](#)

G.7.1 Start Event Source Server

Table G-52 Event Source Management (Event Source Servers)- Start Event Source Server

Tag	Value
Severity	1
Event Name	startEventSource Server
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Start EventSource Server: <event Source Server ID>

G.7.2 Stop Event Source Server

Table G-53 Event Source Management (Event Source Servers)- Stop Event Source Server

Tag	Value
Severity	1
Event Name	stopEventSourceServer
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Stop EventSourceServer: <eventSourceServerID>

G.7.3 Update Event Source Server Configuration

Table G-54 Event Source Management (Event Source Servers)- Update Event Source Server Configuration

Tag	Value
Severity	1
Event Name	UpdateEventSourceServerConfiguration
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Updating event source server <name> with <id>. <updates>

G.8 Event Source Management - Connectors

- ◆ [Section G.8.1, “Start Connector,” on page 231](#)
- ◆ [Section G.8.2, “Stop Connector,” on page 232](#)
- ◆ [Section G.8.3, “Update Connector Configuration,” on page 232](#)
- ◆ [Section G.8.4, “Data Received After Timeout,” on page 232](#)
- ◆ [Section G.8.5, “Data Timeout,” on page 233](#)
- ◆ [Section G.8.6, “File Rotation,” on page 233](#)
- ◆ [Section G.8.7, “Process Auto Restart Error,” on page 233](#)
- ◆ [Section G.8.8, “Process Start Error,” on page 234](#)
- ◆ [Section G.8.9, “Process Stop,” on page 234](#)
- ◆ [Section G.8.10, “WMI Connector Status Message,” on page 234](#)

G.8.1 Start Connector

Table G-55 Event Source Management (Connectors) - Start Connector

Tag	Value
Severity	1
Event Name	startConnector
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Starting Connector <name> with ID <ID>

G.8.2 Stop Connector

Table G-56 Event Source Management (Connectors) - Stop Connector

Tag	Value
Severity	1
Event Name	stopConnector
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Stopping Connector <name> with ID <ID>.

G.8.3 Update Connector Configuration

Table G-57 Event Source Management (Connectors) - Update Connector Configuration

Tag	Value
Severity	1
Event Name	updateConnectorConfiguration
Resource	EventSourceManagement
SubResource	EventSourceManagerService
Message	Updating connector <name> with <id>. <updates>

G.8.4 Data Received After Timeout

When the File Connector is configured with a DataTimeout greater than 0 in the package.xml file and the DataTimeout period without reading any data and then new data is read from the file, the following internal event is generated.

Table G-58 Event Source Management (Connectors)- Data Received After Timeout

Tag	Value
Severity	4
Event Name	FileUpdatedAfterTimeout
Resource	FileConnector
SubResource	FileConnector
Message	After Event source<File Event Source ID> reached time out of<Timeout Period>, file<File Location> received new data.

G.8.5 Data Timeout

When the File Connector is configured with a `DataTimeout` greater than 0 in the `package.xml` file and no data is read from the file in the `DataTimeout` period, the following internal event is generated.

Table G-59 *Event Source Management (Connectors)- Data Timeout*

Tag	Value
Severity	4
Event Name	FileTimeout
Resource	FileConnector
SubResource	FileConnector
Message	Event source <File Event Source ID> reached time out of <Timeout Period> when processing file <File Location>.

G.8.6 File Rotation

When the File Connector is configured to use file rotation and the Connector changes from one file to the next, the following internal event is generated.

Table G-60 *Event Source Management (Connectors)- File Rotation*

Tag	Value
Severity	4
Event Name	RotatingFile
Resource	FileConnector
SubResource	FileConnector
Message	File rotated for event source <File Event Source ID>. Rotating file from <Previous File Location> to <New File Location>.

G.8.7 Process Auto Restart Error

Table G-61 *Event Source Management (Connectors)- Process Auto Restart Error*

Tag	Value
Severity	4
Event Name	ProcessAutoRestartError
Resource	ProcessConnector
SubResource	ProcessConnector

Tag	Value
Message	Process <{0}> [command: {1}] was automatically restarted more than the allowed {2} automatic restart(s) in {3} min. The process will no longer be automatically restarted. Please check process configuration.

G.8.8 Process Start Error

Table G-62 Event Source Management (Connectors)- Process Start Error

Tag	Value
Severity	1
Event Name	ProcessStartError
Resource	ProcessConnector
SubResource	ProcessConnector
Message	Error starting command: {0}

G.8.9 Process Stop

Table G-63 Event Source Management (Connectors) - Process Stop

Tag	Value
Severity	1
Event Name	ProcessStop
Resource	ProcessConnector
SubResource	ProcessConnector
Message	Process <{0}> exited [command: {1}]

G.8.10 WMI Connector Status Message

Table G-64 Event Source Management (Connectors) - WMI Connector Status Message

Tag	Value
Severity	4
Event Name	WMIConnectorStatusMessage
Resource	WMIConnector
SubResource	WMIConnector
Message	<Exception>

G.9 Data Objects

- ♦ [Section G.9.1, “Configuration,” on page 235](#)

G.9.1 Configuration

Table G-65 Data Objects - Configuration

Tag	Value
Severity	
Event Name	New/Update/Remove
Resource	Core
SubResource	FilterConfig,GlobalFilterConfig,SEARCH_HISTORY
Message	Updating Config Object: <name> by User: _SYSTEM

G.10 Search

- ♦ [Section G.10.1, “Event Search,” on page 235](#)

G.10.1 Event Search

Table G-66 Search - Event Search

Tag	Value
Severity	1
Event Name	EventSearch
Resource	Indexed Search
SubResource	Events
Message	Search Started <search parameters>

G.11 Data Retention Policy

- ♦ [Section G.11.1, “Create Data Retention Policy,” on page 236](#)
- ♦ [Section G.11.2, “Update Data Retention Policy,” on page 236](#)
- ♦ [Section G.11.3, “Delete Data Retention Policy,” on page 236](#)

G.11.1 Create Data Retention Policy

Table G-67 Data Retention Policy - Create Data Retention Policy

Tag	Value
Severity	1
Event Name	CreateRetentionPolicy
Resource	IndexedLog
SubResource	IndexedLogRetentionPolicy
Message	Creating Data Retention Policy: <name>

G.11.2 Update Data Retention Policy

Table G-68 Data Retention Policy - Update Data Retention Policy

Tag	Value
Severity	1
Event Name	UpdateRetentionPolicy
Resource	IndexedLog
SubResource	IndexedLogRetentionPolicy
Message	Update Data Retention Policy: <name>

G.11.3 Delete Data Retention Policy

Table G-69 Data Retention Policy - Delete Data Retention Policy

Tag	Value
Severity	1
Event Name	DeleteRetentionPolicy
Resource	IndexedLog
SubResource	IndexedLogRetentionPolicy
Message	Delete Data Retention Policy: <name>

G.12 Disk Usage Configuration

- ♦ [Section G.12.1, “Change Disk Usage Config,” on page 237](#)

G.12.1 Change Disk Usage Config

Table G-70 Disk Usage Configuration - Change Disk Usage Config

Tag	Value
Severity	1
Event Name	ChangeDiskUsageConfig
Resource	Core
SubResource	DiskMonitorService
Message	Changing disk usage configuration, local storage: high water mark: <high water mark in percentage>, low water mark: <low water mark in percentage> network storage: usage limit <usage limit in percentage>

G.13 Report Definitions and Report Results

- ♦ [Section G.13.1, “Remove Report Definition,” on page 237](#)
- ♦ [Section G.13.2, “Remove Report Definitions,” on page 238](#)
- ♦ [Section G.13.3, “Remove Report Result,” on page 238](#)
- ♦ [Section G.13.4, “Remove Report Results,” on page 238](#)

G.13.1 Remove Report Definition

Table G-71 Report Definitions and Report Results - Remove Report Definition

Tag	Value
Severity	1
Event Name	RemoveReportDefinition
Resource	Reporting
SubResource	ReportingService
Message	Removing report definition: <name>

G.13.2 Remove Report Definitions

Table G-72 Report Definitions and Report Results - Remove Report Definitions

Tag	Value
Severity	1
Event Name	RemoveReportDefinition
Resource	Reporting
SubResource	ReportingService
Message	Removing report definitions: <names of deleted report definitions>

G.13.3 Remove Report Result

Table G-73 Report Definitions and Report Results - Remove Report Result

Tag	Value
Severity	1
Event Name	RemoveReportResult
Resource	Reporting
SubResource	ReportingService
Message	Removing report result: <name>

G.13.4 Remove Report Results

Table G-74 Report Definitions and Report Results - Remove Report Results

Tag	Value
Severity	1
Event Name	RemoveReportResults
Resource	Reporting
SubResource	ReportingService
Message	Removing report results: <names of deleted report results>

G.14 General

- ♦ [Section G.14.1, "Configuration Service,"](#) on page 239
- ♦ [Section G.14.2, "Controlled Process is started,"](#) on page 239
- ♦ [Section G.14.3, "Controlled Process is stopped,"](#) on page 240

- ◆ Section G.14.4, “Importing Auxiliary,” on page 240
- ◆ Section G.14.5, “Importing Plugin,” on page 240
- ◆ Section G.14.6, “Load Esec Taxonomy To XML,” on page 241
- ◆ Section G.14.7, “Process Auto Restart Error,” on page 241
- ◆ Section G.14.8, “Process Restarts,” on page 241
- ◆ Section G.14.9, “Proxy Client Registration Service (medium),” on page 242
- ◆ Section G.14.10, “Restarting Process,” on page 242
- ◆ Section G.14.11, “Restarting Processes,” on page 242
- ◆ Section G.14.12, “Starting Process,” on page 243
- ◆ Section G.14.13, “Starting Processes,” on page 243
- ◆ Section G.14.14, “Stopping Process,” on page 243
- ◆ Section G.14.15, “Stopping Processes,” on page 244
- ◆ Section G.14.16, “Store Esec Taxonomy From XML,” on page 244
- ◆ Section G.14.17, “Watchdog Process is started,” on page 244
- ◆ Section G.14.18, “Watchdog Process is stopped,” on page 244

G.14.1 Configuration Service

Table G-75 General - Configuration Service

Tag	Value
Severity	
Event Name	saveConfig
Resource	
SubResource	ConfigService
Message	Saving configuration, unit {0} app {1} userId {2}

G.14.2 Controlled Process is started

Watchdog is run as a service. Its main purpose is to keep Sentinel Log Manager processes running. If a process dies, Watchdog automatically restarts that process. This event is sent out when a process is started.

Table G-76 General - Controlled Process is started

Tag	Value
Severity	1
Event Name	ProcessStart
Resource	Sentinel
SubResource	Process

Tag	Value
Message	Process <ProgramName> spawned (command <pID>)

G.14.3 Controlled Process is stopped

This event is sent out when a process is stopped. The severity is set to 5 if the process was set to respawn (that is, it is not expected to die). The severity is set to 1 if the process was set to run once.

Table G-77 General - Controlled Process is stopped

Tag	Value
Severity	1/5
Event Name	ProcessStop
Resource	Sentinel
SubResource	Process
Message	Process <ProgramName> exited (command <exit_code>)

G.14.4 Importing Auxiliary

Table G-78 General - Importing Auxiliary

Tag	Value
Severity	
Event Name	importAuxiliary
Resource	
SubResource	PluginRepositoryService (Medium)
Message	Import auxiliary file <auxiliaryJarName> into plugin <pluginID>.

G.14.5 Importing Plugin

Table G-79 General - Importing Plugin

Tag	Value
Severity	1
Event Name	importPlugin
Resource	PluginRepository
SubResource	PluginRepositoryService
Message	Import plugin <name> (ID <ID>) of type <type>.

G.14.6 Load Esec Taxonomy To XML

Table G-80 General - Load Esec Taxonomy To XML

Tag	Value
Severity	
Event Name	loadEsecTaxonomyToXML
Resource	
SubResource	EsecTaxonomyNodeService
Message	Loading Esecurity taxonomy Info to an xml format:

G.14.7 Process Auto Restart Error

This event is sent out when a process is stopped. The severity is set to 5 if the process was set to respawn (that is, it is not expected to die). The severity is set to 1 if the process was set to run once.

Table G-81 General - Process Auto Restart Error

Tag	Value
Severity	1/5
Event Name	ProcessAutoRestartError
Resource	Sentinel
SubResource	Process
Message	Process <{0}> [command: {1}] was automatically restarted more than the allowed {2} automatic restart(s) in {3} min. The process will no longer be automatically restarted. Please check process configuration.

G.14.8 Process Restarts

Table G-82 General - Process Restarts

Tag	Value
Severity	1
Event Name	ProcessRestart
Resource	Sentinel
SubResource	Process
Message	Process <ProgramName> spawned (command <pID>)

G.14.9 Proxy Client Registration Service (medium)

Table G-83 General - Proxy Client Registration Service (medium)

Tag	Value
Severity	
Event Name	registerClient
Resource	
SubResource	ProxyClientRegistrationService (medium)
Message	Registering new client

G.14.10 Restarting Process

Table G-84 General - Restarting Process

Tag	Value
Severity	1
Event Name	restartProcess
Resource	SentinelHealth
SubResource	SentinelHealthService
Message	Restarting process <name> on Sentinel server <name> UUID {2}

G.14.11 Restarting Processes

Table G-85 General - Restarting Processes

Tag	Value
Severity	1
Event Name	restartProcesses
Resource	SentinelHealth
SubResource	SentinelHealthService
Message	Restarting <number> processes: <number> name <name> server <name> server ID <ID>;

G.14.12 Starting Process

Table G-86 General - Starting Process

Tag	Value
Severity	1
Event Name	startProcess
Resource	SentinelHealth
SubResource	SentinelHealthService
Message	Starting process <name> on Sentinel server <name> UUID {2}

G.14.13 Starting Processes

Table G-87 General - Starting Processes

Tag	Value
Severity	1
Event Name	startProcesses
Resource	SentinelHealth
SubResource	SentinelHealthService
Message	Starting <number> processes: <number> name <name> server <name> server ID <ID>;

G.14.14 Stopping Process

Table G-88 General - Stopping Process

Tag	Value
Severity	1
Event Name	stopProcess
Resource	SentinelHealth
SubResource	SentinelHealthService
Message	Stopping process <name> on Sentinel server <name> UUID {2}

G.14.15 Stopping Processes

Table G-89 General - Stopping Processes

Tag	Value
Severity	1
Event Name	stopProcesses
Resource	SentinelHealth
SubResource	SentinelHealthService
Message	Stopping <number> processes: <number> name <name> server <name> server ID <ID>;

G.14.16 Store Esec Taxonomy From XML

Table G-90 General - Store Esec Taxonomy From XML

Tag	Value
Severity	
Event Name	storeEsecTaxonomyFromXML
Resource	
SubResource	EsecTaxonomyNodeService
Message	Storing Esecurity taxonomy Info:

G.14.17 Watchdog Process is started

As the Watchdog process starts, the following internal event is generated.

Table G-91 General - Watchdog Process is started

Tag	Value
Severity	1
Event Name	ProcessStart
Resource	WatchDog
SubResource	WatchDog
Message	WatchDog Service Starting

G.14.18 Watchdog Process is stopped

When the Watchdog service is stopped, the following internal event is generated.

Table G-92 *General - Watchdog Process is stopped*

Tag	Value
Severity	5
Event Name	ProcessStop
Resource	WatchDog
SubResource	WatchDog
Message	WatchDog Service Ended

