AUTHORIZED DOCUMENTATION

Administration Guide

Novell® Sentinel™ Log Manager 1.0.0.4

1.0.0.4

February 08, 2010

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide assumes that you have already installed Novell® 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.

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) 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). 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).

For more information about installation and system requirements, see *Sentinel Log Manager 1.0.0.4 Installation Guide*.

Documentation Conventions

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

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

Overview

1

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, regional data aggregation, and simple searching and reporting functionality for a broad range of applications and devices.

1.1 Novell Sentinel Log Manager Features

For more information about Sentinel Log Manager features, see "Novell Sentinel Log Manager Features" in the *Sentinel Log Manager 1.0.0.4 Installation Guide*.

1.2 Novell Sentinel Log Manager Interface

For more information about Sentinel Log Manager Web interface, see "Novell Sentinel Log Manager Interface" in the *Sentinel Log Manager 1.0.0.4 Installation Guide*.

1.3 Architecture

For more information about Sentinel Log Manager architecture, see "Architecture" in the *Sentinel Log Manager 1.0.0.4 Installation Guide*.

1.4 Terminologies

This section describes the terminologies used in this document.

Collectors: Collectors parse the data and deliver a richer event stream by injecting taxonomy, exploit detection, and business relevance into the data stream before events are correlated, analyzed, and sent to the database.

Connectors: The Connectors use industry standard methods to connect to the data source to get raw data.

Data Retention: The data retention policy defines the duration for which the events remain and deleted from the Sentinel Log Manager server.

Event Source Management: The Event Source Management (ESM) interface allows you to manage and monitor connections between Sentinel™ and its event sources by using Sentinel Connectors and Sentinel Collectors.

Events Per Second: Events per second (EPS) is a value to measure how fast a network generates data from its security devices and applications. It is also a rate on which Sentinel Log Manager can collect and store data from the security devices.

Integrator: Integrators are plug-ins that allow Sentinel systems to connect to other external systems. JavaScript actions can use Integrators to interact with other systems.

Raw Data: Raw data varies from Connector to Connector because of the format of the data stored on the device. The system processes a record or data at a time. The raw data contains the information about the raw data message, raw data (record) ID, time the raw data was received (as stamped by the Collector Manager), IDs of the event source, Connector, Collector, and Collector Manager node IDs and a SHA-256 hash of the raw data.

Security Considerations for Sentinel Log Manager

2

This section provides specific instructions on how to securely install, configure, and maintain Novell® Sentinel™ Log Manager.

2.1 Securing Communication Across the Network

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.

2.1.1 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 `<Install_Directory>/config/configuration.xml`:

```
 <jms brokerURL="ssl://
localhost:61616?wireFormat.maxInactivityDuration=0&amp;jms.copyMessageOnSend=
false" interceptors="compression" keystore="../config/
.activemqclientkeystore.jks" keystorePassword="password"
password="1fef3bcdd3fbcbc5cd795346a9f04ddc" 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
`ssl://`	Indicates that SSL is used for secure connection. You should not modify this value.
`localhost`	The hostname or IP address where the Java* message service (JMS) server is running.
`61616`	The port that the JMS server is listening on.
`?wireFormat.maxInactivityDuration=0&jms.copyMessageOnSend=false`	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.
`interceptors="compression"`	Enables compression over the connection. You should not modify this value.
`keystore="../config/.activemqclientkeystore.jks"`	The path to the Java keystore, which is used to check if the server is trusted.
`keystorePassword="password"`	The password to the Java keystore file.
`password="1fef3bcdd3fbcbc5cd795346a9f04ddc"`	The password to present to ActiveMQ for authenticating the connection. This corresponds to a password in the *`Install_Directory`*`/config/activemqusers.properties` file.
`username="system"`	The username to present to ActiveMQ for authenticating the connection. This corresponds to a username in the *`Install_Directory`*`/config/activemqusers.properties file`.

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

2.1.2 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 1.0.0.4 Installation Guide*.

ESM knows to use SSL by reading the following information in *Install_Directory*/config/configuration.xml:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory">
      <transport type="ssl">
        <ssl host="164.99.18.132" port="10013" keystore="./novell/sentinel/
.proxyClientKeystore" />
      </transport>
    </strategy>
```

2.1.3 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). To configure the encryption, refer to PostgreSQL Encryption Options (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.

2.1.4 Communication between the 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 with 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, refer to the Connector and Event source vendor documentation.

2.1.5 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).

2.1.6 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.

To allow pgAdmin to connect from any client machine, add the following line in the *Install_Dirirectory*/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.

2.1.7 Communication between Sentinel Log Manager and NFS/CIFS Archive Servers

Sentinel Log Manager can be configured to archive event and raw data to a remote CIFS or NFS* server. These protocols do not offer data encryption, so consider security implications before deciding the type of archive location to use. An alternative is to use direct attached storage (local or SAN), which does not suffer from the same security vulnerabilities. If you choose to use CIFS or NFS, it is important to configure the CIFS or NFS server properly to maximize the security of your data.

For more information about configuring the archive server settings, see "Configuring Archive Server Settings" in the *Sentinel Log Manager 1.0.0.4 Installation Guide*.

2.2 Securing Users and Passwords

2.2.1 Operating System Users

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

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 during uninstallation or reinstallation of a 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.

2.2.2 Sentinel Application and Database Users

All Sentinel Log Manager application users are native database users and their passwords are protected by the native database platform. These users have only read access to certain tables in the database so that they can execute queries against 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:

dbuser: 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 at installation, which is stored encrypted in the *`Install_Directory`*`/server.xml` file. To change the password for the `appuser`, use the *`Install_Directory`*`/bin/dbconfig` utility.

For more information, see "Command Line Utilities" on page 141.

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.

2.3 Securing Sentinel Data

IMPORTANT: Because of the highly sensitive nature of the data on the 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 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, when the password is stored, it is first encrypted to avoid unauthorized access to the clear-text password.

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

Database credentials are stored in the <Installation_Directory>/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 configuration.xml file:

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.Ac
tiveMQStrategyFactory" name="ActiveMQ">
      <jms brokerURL="ssl://
localhost:61616?wireFormat.maxInactivityDuration=0&amp;jms.copyMessageOnSend=
false" interceptors="compression" keystore="../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	The database tables and file system at *Install_Directory*/config. This configuration information includes the encrypted database, event source, integrators, and passwords.	The database (EVENTS, CORRELATED_EVENTS, and the EVT_SMRY_* and AUDIT_RECORD tables), and the file system at *Install_Directory*/data/events. **NOTE:** Event data can be archived to the file system as part of the partition management job.
Collector Manager	The file system at *Install_Directory*/data/eventdata and *Install_Directory*/data/rawdata. The most sensitive configuration information is the client key pair used to connect to the message bus.	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 *Install_Directory*/data/collector_mgr.cache directory.

2.4 Securing the Operating System

- Sentinel Log Manager is supported on SUSE® Linux Enterprise Server (SLES) 11. For more information on securing a SLES machine, see the SUSE Linux Enterprise Server 11 documentation (http://www.novell.com/documentation/sles11/book_sle_security/?page=/documentation/sles11/book_sle_security/data/book_sle_security.html).
- If the Sentinel Log Manager is accessible from outside the corporate network, a firewall should be employed to prevent direct access to the Sentinel Log Manager server.

  Enable the following ports in the firewall:

Table 2-3 *List of Components and their Ports*

Component	Port
ActiveMQ	61616 and 61617
PostgreSQL	5432
Tomcat	8443
Proxied trusted client	10014
internal_gateway_server and internal_gateway Used between the engine and the manager	5556
Event Source Management user interface SSL Proxy	10013
Audit Connector	1289

Component	Port
Syslog Connector TCP	1468
Syslog Connector SSL	1443
Syslog Connector UDP	1514 (and 514, which can be forwarded to 1514)

Sentinel Log Manager also listens for connections from the localhost on other randomly assigned TCP port numbers. For the system to function properly, connections from localhost to any port should be allowed.

For more information on enabling a firewall on SLES 11, see Configuring the Firewall with YaST (http://www.novell.com/documentation/sles11/book_sle_security/?page=/documentation/sles11/book_sle_security/data/book_sle_security.html) in the *SLES 11 Security Guide*.

Only localhost access is required for the 5432 and 5556 ports.

2.5 Auditing Sentinel

Sentinel generates events for many of its internal actions. These events can be accessed through a search or analyzed by a report.

To include only audit and internal events in your search results, select the *include system events* check box and include the `st:"I" OR st:"A" OR st:"P"` criteria in your search query.

2.6 Generating an SSL Certificate for the Server

You can replace the self-signed certificate with a certificate signed by a major Certificate Authority (CA), such as VeriSign*, Thawte*, or Entrust*. You can also replace the self-signed certificate with a certificate signed by a less common CA, such as a CA within your company or organization.

Configuring Data Storage

3

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

3.1 Data Storage Overview

Sentinel Log Manager receives two separate, but similar data streams from the collector managers: the event data and the raw data. Both types of data on Sentinel Log Manager are moved from the online, compressed, file-based storage to a user-configured, compressed archive storage location on a regular basis.

Data files are deleted from the local and archive 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 these policies are configured by the Sentinel Log Manager administrator.

3.1.1 Raw Data

Raw data are the unprocessed events that are received by the connector and sent directly to the Sentinel Log Manager message bus, and then written to the Sentinel Log Manager server. The original event is not altered, but the following additional information are also sent to the message bus with each event:

- SHA-256 hash of the event
- Chaining indicator (which is reset to 0 whenever the Sentinel Log Manager event source is restarted)

All raw data are sent to the Sentinel Log Manager; there is no filtering on raw data.

The time-based raw data files are closed (changed to read-only) after a duration and no more events are written to them. After these files are closed, they are compressed and archived to the configured location.

- "Raw Data Storage" on page 22
- "Raw Data Representation" on page 23

Raw Data Storage

In Sentinel Log Manager, raw data is always stored. 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 the closed files. Files in the open state have a `.open` extension. When they are closed, they will be renamed to have a `.log` extension. Sometime after they are closed, they will be compressed and will then have a `.zip` extension. After being compressed, they are moved to archive storage and are no longer present in the local storage.

The following table describes the directory structure of the online raw data under the installation directory:

Table 3-1 *Raw Data Directory Structure*

Directory structure	Description
`/data`	The primary directory for all data storage.
`/data/rawdata`	The sub directory where all raw data is stored.
`/data/rawdata/online`	The directory where all the online raw data is stored.
`/data/rawdata/EventSource UUID`	The sub directory 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 `online` subdirectory. That subdirectory contains all raw data received from that event source.
`/data/rawdata/EventSource UUID/Month`	The subdirectory name is in the yyyy-mm format (for example: 2009-05 is May of 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	Each file in the Month directory contains data received during a specific one-hour period. Most data in the file have a time stamp that are within the one-hour period. The name of the file indicates the day of the month and the one-hour period that is represented. The filename format is dd-hhmm.extension. Where: *dd* is the day of the month. *hh* is the hour of the day. *mm* is the minute of the hour. extension is either open or log or zip (compressed). For example: A name with the extension 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. A name with the extension 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., and the file is closed, but not yet compressed. A name with the extension 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.

The following examples show filenames as they might appear relative to the installation directory:

- data/rawdata/online/E20D0840-1E0A-102C-9F30-000C2949BA91/2009-05/08-0000.zip: Compressed raw data received on May 8, 2009 between 12:00 a.m. and 01:00 a.m.
- data/rawdata/online/E20D0840-1E0A-102C-9F30-000C2949BA91/2009-05/08-0100.open: Uncompressed raw data received on May 8, 2009 in every hour.

Raw Data Representation

Each raw data event is represented as a single line in a raw data file. Each line is a JSON object that has the following fields:

Table 3-2 *Raw Data Representation*

Field Name	Description
EventDate	This is the date and time when the Sentinel Log Manager received this event and not the date and time when the event has occurred. Example: “05/07/2009 05:23.790”

Field Name	Description
EventRecordID	The record ID of the corresponding event record in the event store. **NOTE:** If no event record was ever created (because of filtering) this record ID might not point to anything. Example: "595829C0-1C8F-102C-A922-000C2949BA91"
RawData	The original raw data received by the event source.
RawDataHash	The SHA256 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. To detect tampering, each raw data event is stored with a SHA256 hash value. Example: cc661009e2f3dc565c0c7fe25b705219004dcd8132c0b0a7e987bfdcb55e49cf
EventSourceID	The UUID of the event source the raw data came from. Example: A2A0C600-1C6C-102C-A781-000C2949BA91
EventSourceGroupID	The UUID of the event source group (Connector) to which the event source was connected when the raw data was received. Example: A2A0C600-1C6C-102C-A77A-000C2949BA91 **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 other.
CollectorID	The UUID of the Collector that the Connector and event source were connected to when the raw data was received. **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. Example: A2A0C600-1C6C-102C-A779-000C2949BA91
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 chain ID number is generated. To detect tampering, each raw data event is stored with a Chain ID and a Chain Sequence number. Example: 1241630654754

Field Name	Description
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 would record only from the next arrival of raw data. Nonetheless, the raw data chain sequence should continue uninterrupted across 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).

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 47. Event data are subject to filtering rules set up on the event source, connector, and collector, so event data may be dropped, if required.

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 archived.

Online partitions are stored in the *install_directory*`/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
`/data`	The primary directory for all data storage.
`/data/eventdata`	The sub directory where all event data is stored.

Directory structure	Description
/data/eventdata/YYYYMMDD_<classid>	A partition consists of the events for a single day (midnight-midnight UTC) within a given data retention class and is held within a sub-directory named YYYYMMDD_<class-id>. Where, **YYYYMMDD:** is the UTC date stamp. **<class_id>:** is a UUID identifier associated with the data retention class.
/data/eventdata/YYYYMMDD_<class_id>/events.evt	The events.evt directory 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.

3.1.3 Archiving

Archiving is the process of copying closed data files from the local storage location to the archive 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.

Archiving processes are applied to both the raw data and event data.

- “Raw Data Archiving” on page 26
- “Event Data Archiving” on page 26

Raw Data Archiving

A raw data file is in one of the following three states at the online location:

xx.open: A file to which data is currently being written.

xx.log: A file to which data is no longer being written. This type of file has not been compressed yet.

xx.zip: A file that is already been compressed. The compression process runs every 10 minutes, by default. These files appear in both the online and archive locations if archiving is configured and enabled.

If data archiving is configured and enabled, compressed raw data files are copied in every 15 minutes to the configured archive location.

For more information about raw data storage, see “Raw Data Storage” on page 22.

Event Data Archiving

The event data stored on the Sentinel Log Manager server are archived if data archiving is enabled and configured.

If archiving is enabled, the closed files are archived whenever the server starts. They are also archived at midnight UTC every night. These files are already compressed in the local storage location, but the indexes for these files are compressed before being moved to the archive. If the archive location is not configured or if there is any problem while archiving, attempts are made every 60 seconds until archiving succeeds.

3.1.4 Data Retention

The data retention policies control when data is deleted from the system. There is one policy for the raw data; there may be multiple policies that apply to the event data.

3.2 Configuring Data Archiving

You can enable data archiving on Sentinel Log Manager for both the raw data and event data. You can configure following three types of archive locations:

- User-configured SAN mount location or a local directory on the Sentinel Log Manager server. (This is the recommended configuration.)
- Remotely configured CIFS share.
- Remotely configured NFS share.

For more information about the archive server configuration settings, see "Configuring Archive Server Settings" in the *Sentinel Log Manager 1.0.0.4 Installation Guide*.

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

3.2.1 Configuring Archive Locations

NOTE: The NFS, CIFS, and SAN must be configured in such a way that Sentinel Log Manager has read and write permissions for it.

Configuring SAN/Local Directory as an Archive Location

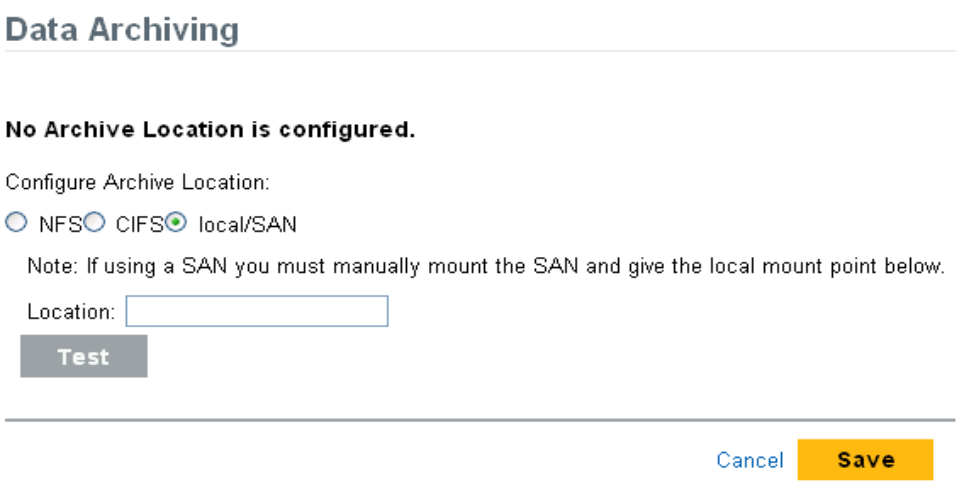
This is the preferable configuration for the best performance, security, and reliability.

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

The *Storage* tab is displayed on the right pane of the page.

3 Click the *Configuration* tab.

4 In the Data Archiving section, select the *local/SAN* option.



5 In the *Location* field, specify the local directory path or the location on which the SAN is mounted.

If you are using a storage area network (SAN), you must manually mount the SAN, and specify the mount location.

6 Click the *Test* button to check the write permissions for the specified location.

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

If the location is not configured, the test fails, and a message is displayed stating the reason for the failure.

7 Click *Save* to configure the specified archive location.

Configuring a CIFS Server as an Archive Location

For more information about configuring the CIFS server, see "CIFS Configuration" in the *Sentinel Log Manager 1.0.0.4 Installation Guide*.

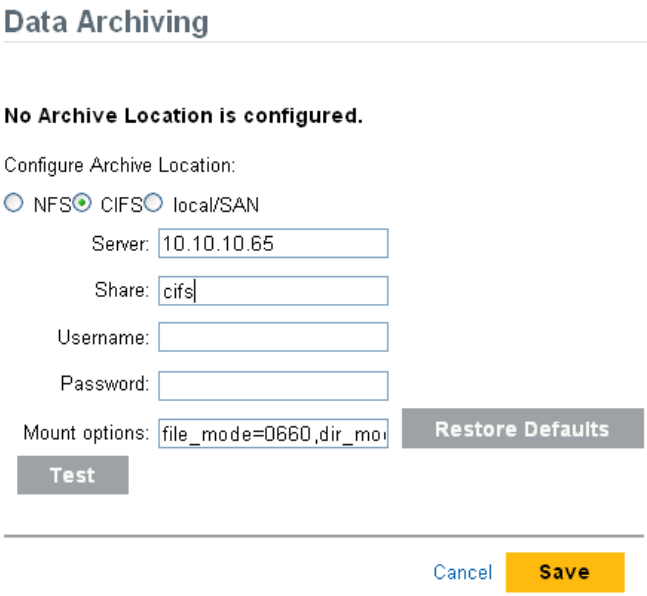
1 Log in to the Sentinel Log Manager as an administrator.

2 Click the *storage* link in the upper left corner of the page.

The *Storage* tab is displayed on the right pane of the page.

3 Click the *Configuration* tab.

4 In the Data Archiving section, select the *CIFS* option.



5 In the *Server* field, specify the IP address or host name of the machine where the CIFS server is configured.

6 In the *Share* field, specify the share name of the 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.

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

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

9 The *Mount options* field specifies the options that are used while mounting the archived location of the CIFS server.

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

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

10 Click the *Restore Defaults* button to restore the default mount options.

11 The *Mount options* field specifies the options of the CIFS server.

You can also specify a new mount location.

12 Click the *Restore Defaults* button to change to the default mount location.

13 Click the *Test* button to mount the 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 a message is displayed the reason for failure.

14 Click *Save* to configure the specified archive location.

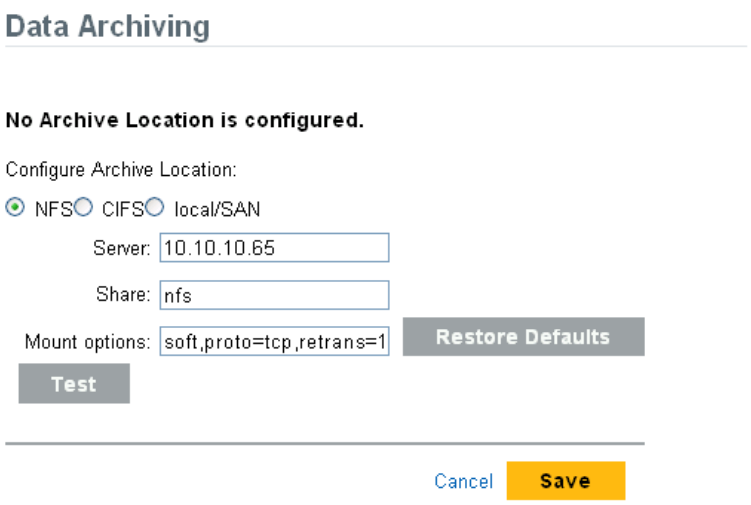
Configuring an NFS Server as an Archive Location

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.

For more information about configuring the NFS server, see "NFS Configuration" in the *Sentinel Log Manager 1.0.0.4 Installation Guide*.

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

   The *Storage* tab is displayed on the right pane of the page.
3. Click the *Configuration* tab.
4. In the Data Archiving section, select the *NFS* option.



5. In the *Server* field, specify the IP address or host name of the machine where the NFS server is configured.
6. In the *Share* field, 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.
7. The *Mount options* field specifies the options that are used while mounting the archived 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).

   The default mount options are `soft,proto=tcp,retrans=1,timeo=60`.
8. Click the *Restore Defaults* button to restore the default mount options.
9. Click the *Test* button 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.

NOTE: This procedures tests a subset of all of the settings that are necessary for the NFS server and client.

10 Click *Save* to configure the specified archive location.

3.2.2 Enabling or Disabling Data Archiving

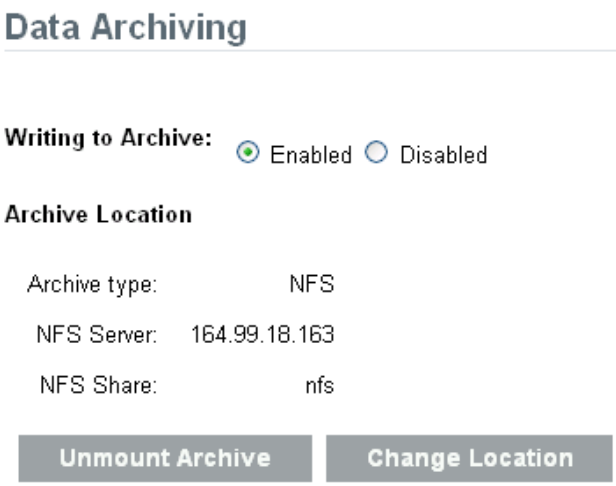
The enabling and disabling data archiving options appear only when the archive location is configured. However, event search and reporting work even when the data archiving is disabled.

1 Log in to the Sentinel Log Manager as an administrator.

2 Click the *storage* link in the upper left corner of the page.

The *Storage* tab is displayed on the right pane of the page.

3 Click the *Configuration* tab.



4 To enable writing to archive select *Enabled*.

You can write both the raw data and event data at the configured archive location. To configure data archive locations, refer to "Configuring Archive Locations" on page 27.

5 To disable writing to archive the raw data select *Disabled*.

This selection disables the writing of raw data and event data archiving.

NOTE: You cannot write to the archive location, but you can still read the archived data. Search shows the events that are archived, and you can also download the archived raw data.

6 Click *Save*.

3.2.3 Unmounting Archive Location

Unmount Archive option appears only if the archive location is configured. If the archive is unmounted, data archiving is disabled. Searches and reports would include only the online data.

1 Log in to the Sentinel Log Manager as an administrator.

2 Click the *storage* link in the upper left corner of the page.

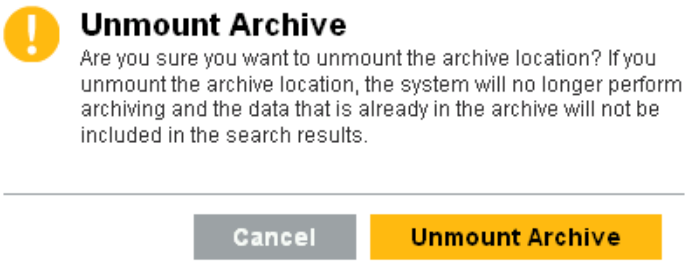
The *Storage* tab is displayed on the right pane of the page.

3 Click the *Configuration* tab.

4 To unmount the data archiving, select *Unmount Archive*.

When you unmount the archive location, Sentinel Log Manager can no longer access the archive data. If the archive location is configured to a remote location (NFS or CIFS), the archive location is unmounted.

A confirmation message is displayed, asking if you really want to unmount the archive location.



5 Click *Unmount Archive*.

3.2.4 Changing the Archive Location

The *Change Location* option is displayed only if the archive location is configured.

1 Log in to the Sentinel Log Manager as an administrator.

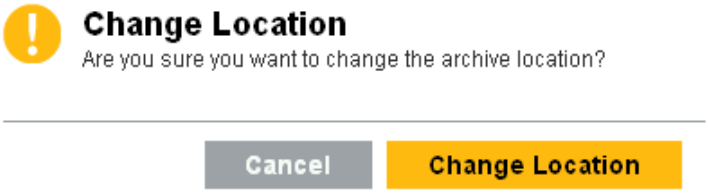
2 Click the *storage* link in the upper left corner of the page.

3 The *Storage* tab appears on the right pane of the page.

4 Click the *Configuration* tab.

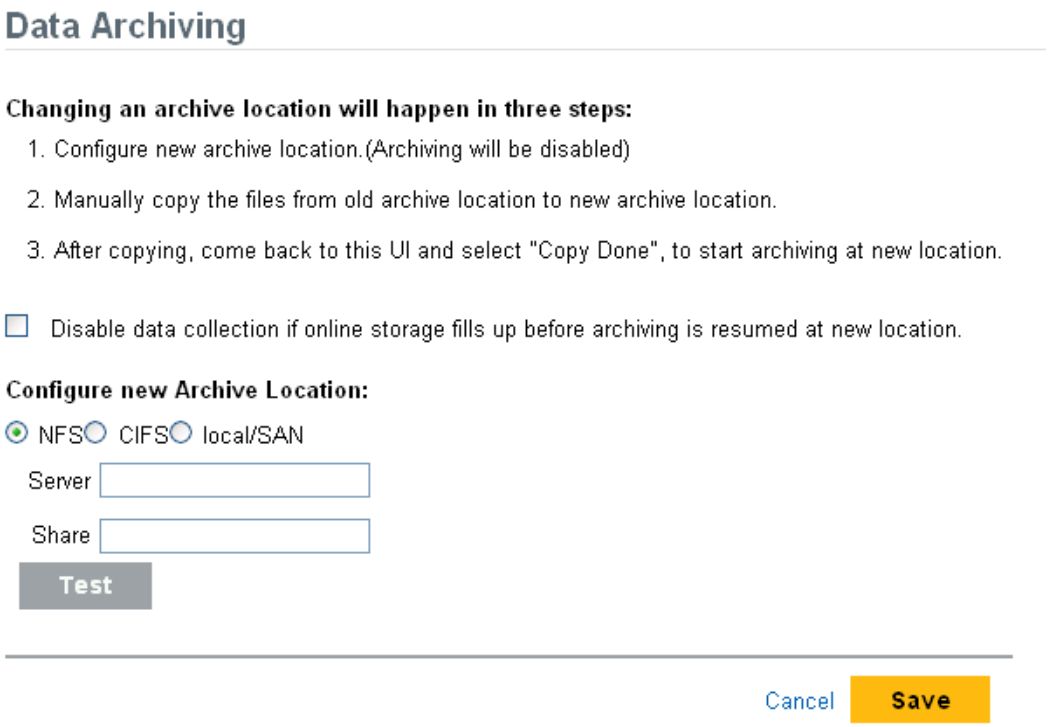
5 In the Data Archiving section, select *Change Location*.

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



6 Click *Change Location*.

The following page allows you to configure a new archive location.

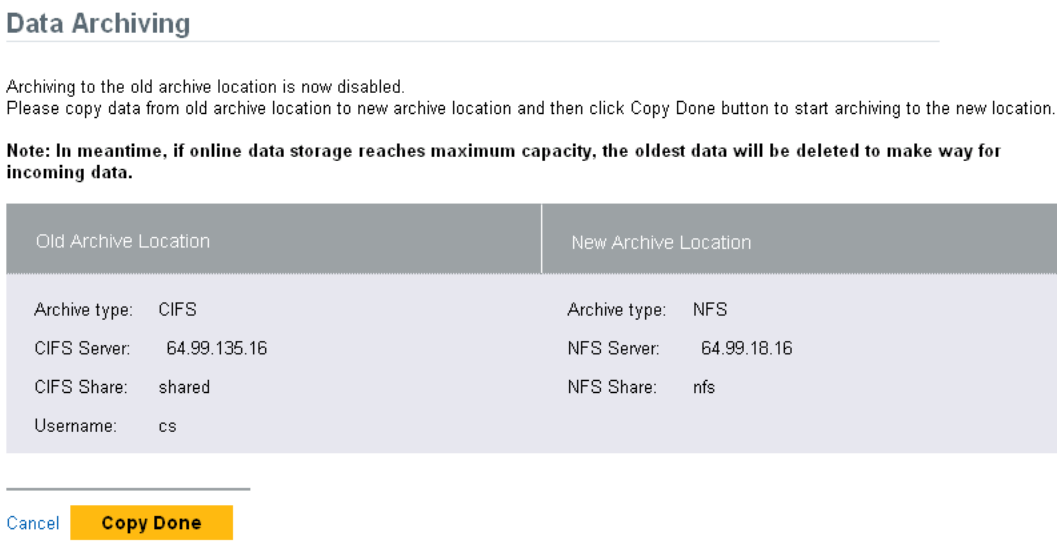


7 Select the check box to disable data collection if local storage fills up before archiving is resumed at new location. Otherwise, the oldest data is deleted to make space for the incoming data.

8 Configure the new archive location.

For more information about configuring the NIFS or CIFS or local/SAN archive locations, see "Configuring Archive Locations" on page 27.

9 Click *Save* to save the changes and configure the new archive location.



10 Manually copy the files from the old archive location to the new archive location.

11 After copying the files, select the *Copy Done* option to start data archiving to the new location.

12 Click *Cancel* to return to the previous archive configuration.

3.3 Configuring Data Retention Policies

You can configure one or more data retention policies to control the duration for which specific types of events are retained in the Sentinel Log Manager. 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. 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, data retention policy is refreshed every 30 seconds to reflect the changes made by multiple users. For every 30 seconds, the refresh operation synchronizes the policy table and reflects the changes made to the retention policies by multiple administrators.

- Section 3.3.1, “Raw Data Retention Policy,” on page 34
- Section 3.3.2, “Event Data Retention Policies,” on page 34
- Section 3.3.3, “Rules for Applying Appropriate Retention Policy,” on page 37

3.3.1 Raw Data Retention Policy

The raw data retention policy controls how long the raw data is kept in the system before being deleted. The data retention policy table contains a raw data retention policy. Like the default data retention policies for events, the Raw Data Retention policy cannot be deleted or disabled. However, you can change the *Keep at most* (number of days after which the raw data file is deleted) and *Keep at Least* (minimum number of days the raw data file is kept) values.

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

3.3.2 Event Data Retention Policies

The event data retention policies control how long different types of event data are kept in the system before being deleted.

- “Adding a Data Retention Policy” on page 34
- “Activating or Deactivating a Data Retention Policy” on page 36
- “Editing a Data Retention Policy” on page 36
- “Deleting a Data Retention Policy” on page 36

Adding a Data Retention Policy

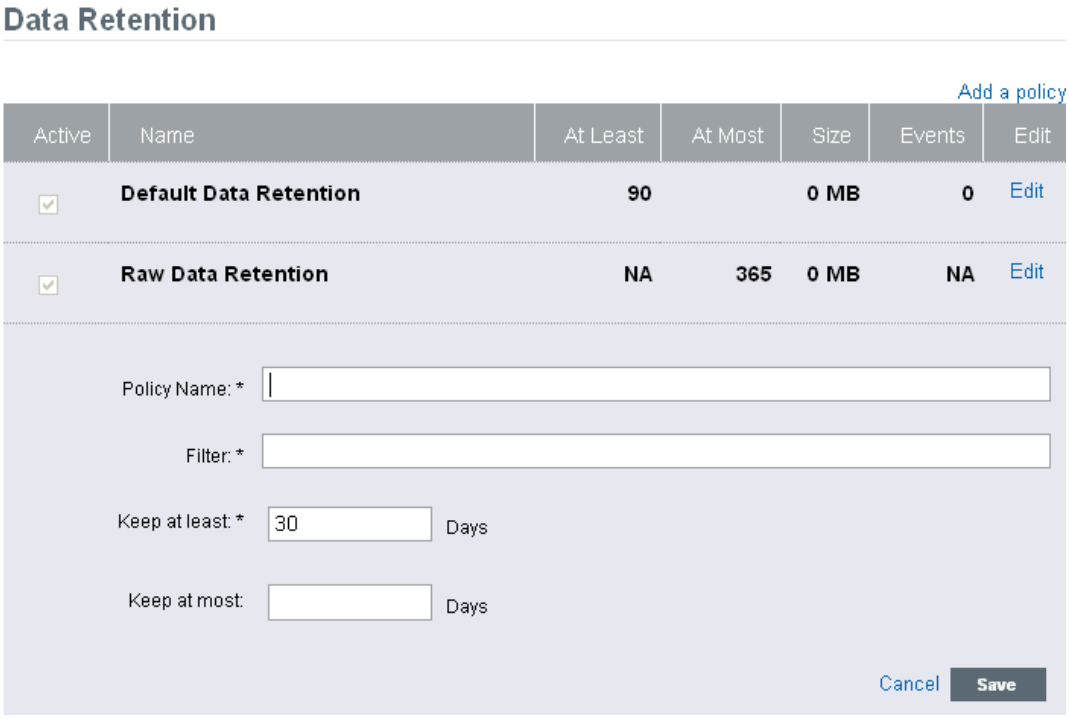
1 Log in to the Sentinel Log Manager as an administrator.

2 Click the *storage* link in the upper left corner of the page.

The *Storage* tab appears on the right pane 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.



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, 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 77.

7 Click the *show tips* link to view the tag names that can be used for defining 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 Specify the minimum number of days to retain the events in the system in the *Keep at least* field. 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 count 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 on top of the policy table.

For more information, see "Data Expiration Policy" on page 145.

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.

   The *Storage* tab is displayed on the right pane 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 next to the policy, in the column headed *Active*.
5. To deactivate the retention policy, clear the check box next to the policy.

   You cannot disable the default data retention policy.

Editing a Data Retention Policy

NOTE: You cannot edit the name of the default data retention policy. You can only change the *Keep at Least* and *Keep at Most* values.

---

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

   The *Storage* tab is displayed on the right pane 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.

You can edit only one policy at a time. If a policy is currently being edited and you edit another policy, the previously opened editor is closed and changes are not saved.

Deleting a Data Retention Policy

You cannot delete the Default Data Retention and Raw Data Retention policies.

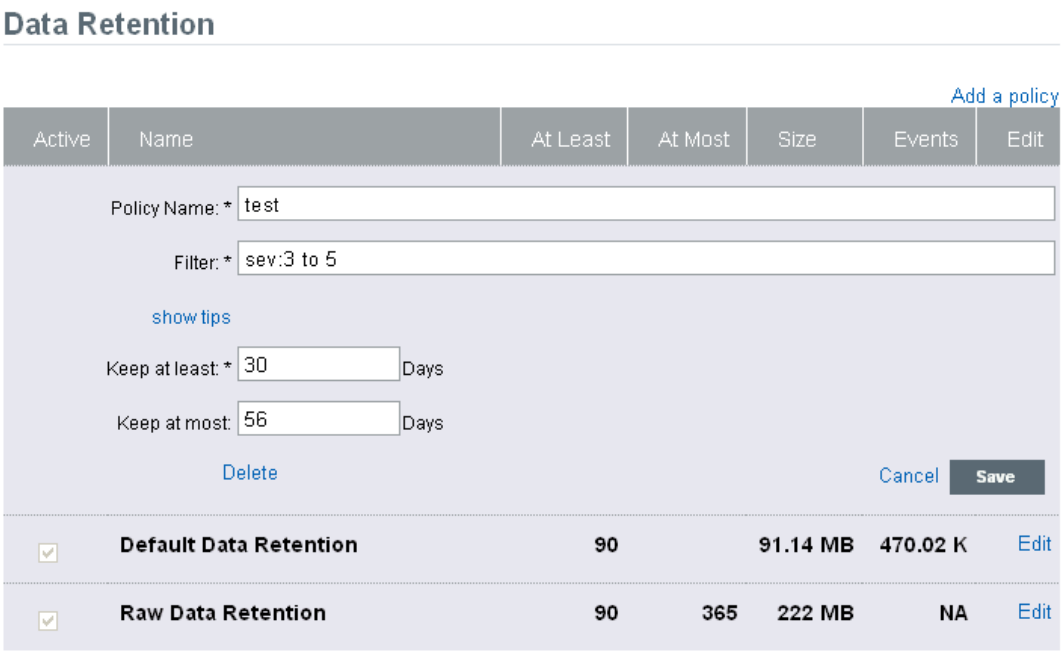
1. Log in to the Sentinel Log Manager as an administrator.
2. Click the *storage* link in the upper left corner of the page.

   The *Storage* tab is displayed on the right pane of the page.
3. Click the *Configuration* tab.

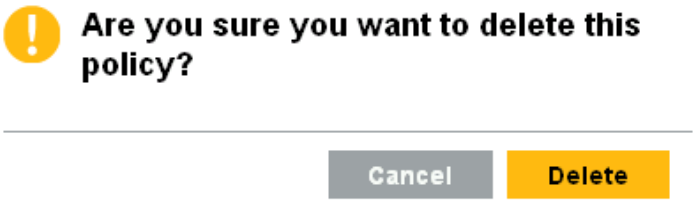
The data retention policy table is displayed in the *Data Retention* section.

4 To delete the retention policy, click the *Edit* link next to the configured policy.

The policy editor opens within the policy table.



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 Appropriate Retention Policy

You can apply multiple data retention policies that apply to the event data, including the Default Data Retention policy. To determine how long an event is retained before being deleted from the local and archive data stores 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.

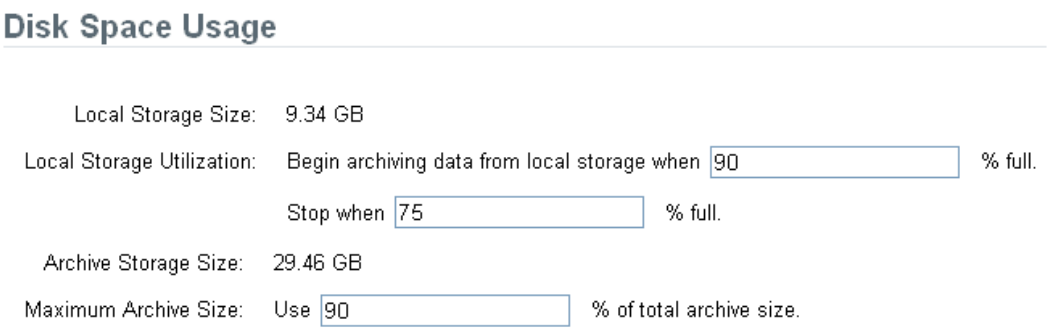
3.4 Configuring Disk Space Usage

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

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

   The *Storage* tab is displayed on the right pane 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 the Sentinel Log Manager.



4. Specify the local storage utilization value:
   - Specify a value to start the data archiving from local storage when the specified percentage of value is full.
   - Specify a value to stop the data archiving from local storage when the specified percentage of value is full.

   Archive storage size specifies the value of the archive 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 archived every one hour and the file hash is computed for archived files. The file hash is used to check the integrity of the archived files.

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

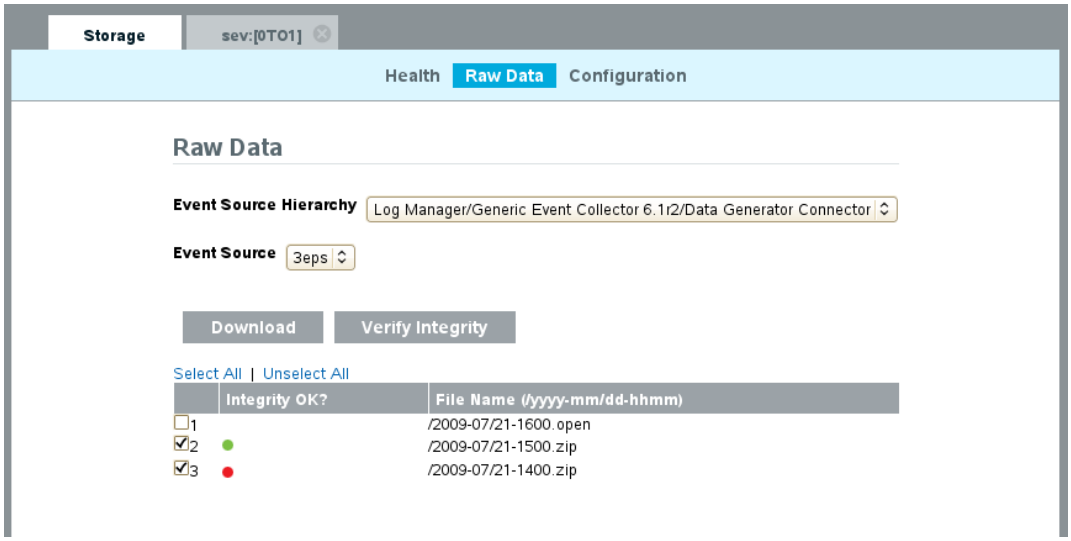
   The *Storage* tab is displayed on the right pane of the page.
3. Click the *Raw Data* tab.
4. In the *Raw Data* section, select the desired collector and connector combination from the Event Source hierarchy drop-down list.
5. The *Event Source* field displays the list of associated event sources (hostnames or IP addresses). Select the event source from the drop-down list.

   The table displays the list of local and archived 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, click the check box on the left side of the raw data file.

   The *Verify Integrity* and *Download* options are only enabled when you select a file from the table.
8. Click *Verify Integrity* to verify the integrity of the selected archived files by comparing the hash values for the selected archived files.

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

   The hash is computed and updated in database only for archived files, but not for the local raw data files. As the raw data files are updated until they are archived, the hash value cannot be computed or updated for these files. So it is not possible to check the integrity of the local raw data files.



9. Select the raw data file, then click *Download* to download the selected archived and/or 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 archived files are selected, the zip file would also contains a hash file corresponding to each of the archive files downloaded.

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

10 Click *Close*.

3.6 Viewing Online and Archive Data Capacity

The Data Storage Health page, available only to administrators, shows online and archive data capacity (if configured).

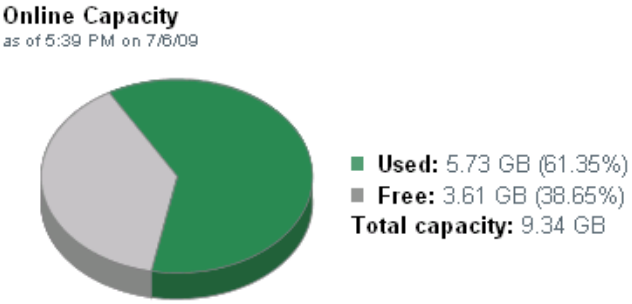
To view the online and archive data capacity:

1 Log in to the Sentinel Log Manager as an administrator.

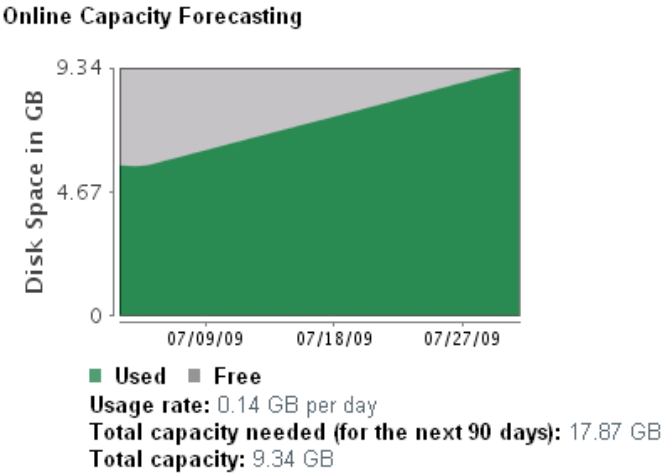
2 Click the *storage* link in the upper left corner of the page.

This page shows the free data space as gray and the used data archiving space as green.

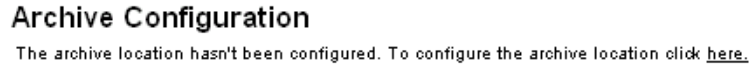
The health page displays the online capacity.



The health page of Sentinel Log Manager also displays forecasts about the online data capacity.

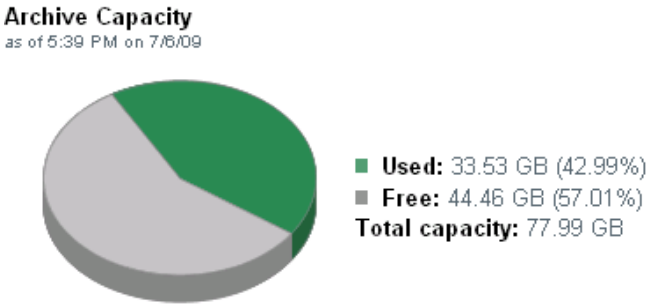


If the archive location is not configured, the following message is displayed on the Health page.

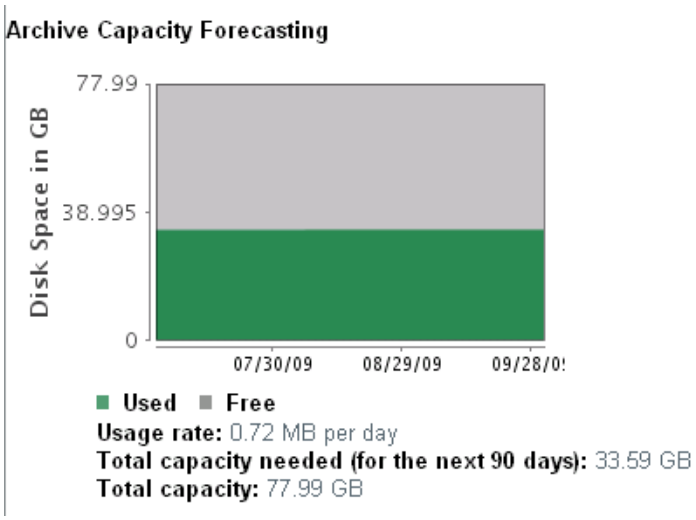


The Click here link displays the Data Archive page to configure the archive location. For more information refer to “Configuring Data Archiving” on page 27.

If Sentinel Log Manager is configured to archive data, the health page displays the archive capacity:



The health page of Sentinel Log Manager also forecasts the archive data capacity.



3.7 Using Sequential-Access Storage for Long Term Data Storage

Sequential-access storage (such as tape) is a cost effective storage mechanism to store large amount of data. Sentinel Log Manager does not support interfacing with the data stored on tape directly, as it requires the data to be on a storage system that supports random access, such as data on your typical hard drive.

The high level approach is to configure Sentinel Log Manager to retain data for longer duration to perform searches and run report on the data you regularly need to access and to copy data to tape before Sentinel Log Manager deletes it. To search or run report on data that was copied to tape, but deleted from Sentinel Log Manager, copy the data from tape back into Sentinel Log Manager to include the newly recovered data in its search results.

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

3.7.1 Determining What Data You Need to Copy to Tape

There are two types of data in Sentinel Log Manager:

- Raw data are the unprocessed events that are received by the connector and sent directly to the Sentinel Log Manager message bus and then written to the disk on the Sentinel Log Manager server. Raw data retention comes under legal requirements. Raw data cannot be searched or reported on, because it is not processed or indexed.
- Event data is generated by a collector after processing the raw data. Event data is indexed for searching and can be searched and reported on. Although this data is not usually included in the legal requirements, it is often important to retain, because it makes the data search easier.

If you want to store raw data to comply with legal requirements and are not concerned to search or run report on that data at a later time, you can just copy the raw data to tape. However, if you want to perform search or report on the data, you should copy both the raw data and the event data to tape so that you can later recopy both sets of data back into Sentinel Log Manager.

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.

3.7.2 Backing Up Data

Sentinel Log Manager provides following backup options:

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

Data: This option takes longer because it involves backing up all the data in the data and archive directories.

NOTE: Archive directories can be located on a remote machine.

Events should be archived regularly.

- You should periodically export all the ESM configurations and save them. When the environment is relatively stable, you can generate a full ESM export including the entire tree of the ESM components. This action captures the plug-ins as well as the configuration of each node. The resulting `.zip` file should be backed up and archived as a normal file.

  If changes such as updating plug-ins or adding nodes are made to ESM 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.

3.7.3 Configuring Sentinel Log Manager Storage Utilization

Sentinel Log Manager allows you to configure local and archive storage space size to store data, before it deletes the data from the Sentinel Log Manager server. Use these size limits to ensure that your storage system is not 100% utilized, which might result in undesirable behaviors such as data corruption. Additionally, you should also leave extra space in your archive storage so that at a later time you can copy data from tape back into Sentinel Log Manager. By decreasing the archive utilization setting, Sentinel Log Manager creates space to copy data back from tape.

3.7.4 Sentinel Log Manager Data Retention

Sentinel Log Manager allows you to configure the duration to keep the data on disk before it deletes the data. If your hard drive storage space is not sufficient to store data long enough to meet your legal requirements, you can use tape storage mechanism to store the data beyond the specified data retention duration. Therefore, retention policies should be configured long enough to make sure the data you want to regularly search and to report on is retained within Sentinel Log Manger, for example the most recent 90 days worth of data. Additionally, retention policy should ensure that Sentinel Log Manager is not prematurely deleting the data due to storage utilization limits. If the storage utilization limit exceeds and data is prematurely being deleted, you should change the policy to expand the data storage space.

3.7.5 Copying Data to Tape

Depending on what data you need to retain for long term, you need to setup a process to copy raw and/or event data to tape.

The following section discusses how each type of data is stored in Sentinel Log Manager so that you can setup copy operations to copy the data out of Sentinel Log Manager onto tape.

- “Copying Raw Data to Tape” on page 43
- “Copying Event Data to Tape” on page 44

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 as the closed file. Files in the open state have a `.open` extension. When they are closed, they will be renamed to

have a `.log` extension. Sometime after they are closed, they will be compressed and will then have a `.zip` extension. After being compressed, they are moved to archive storage and are no longer present in 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 22.

You should wait until raw data files have been compressed and moved to archive storage before copying them to tape. Make sure that they are not in the process of being compressed or copied when you copy them to tape (if there is still a `.log` file of the same name, it is likely that the `.zip` file is still being created). At the same time, the raw data files must be copied before the Sentinel Log Manager Raw Data Retention Policy expires so that you avoid losing the data.

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 partitions, 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 and subdirectories whose date is at least 48 hours old should be in the closed state.

For more information on event data directory hierarchy, see Table 3-3, "Event Data Directory Structure," on page 25.

You should wait until event data partitions have been copied to archive 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 archive 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 archive 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 Copying Data from Tape Back Into Sentinel Log Manager

This section discusses how to restore data that was deleted from Sentinel Log Manager due to the data retention time elapsed, but backed up to tape.

NOTE: Current version of Sentinel Log Manager does not fully support restoring deleted data partitions. As a result, you will find that after restoring the partition and updating the database to reactivate the partition, Sentinel Log Manager will reapply the retention policy to it the next time it runs the policy check tasks. The policy check tasks are executed on the following intervals:

- **For Raw Data:** Every 1 hour policy check starts when the Sentinel Log Manager starts. This is configurable by setting the `RawDataConsumer.fileSpanMinutes` property in the `config/server.xml` file. However, the same property is used to determine the time range of the raw data files, so increasing this value will also increase the size of the raw data file. Due to the presence of two different time range, raw data files in your system may cause confusing behavior.

- **For Event Data:** Once a day, at midnight UTC (GMT)

- "Restoring Raw Data from Tape" on page 45
- "Restoring Event Data from Tape" on page 45

Restoring Raw Data from Tape

To restore raw data, copy the data from tape back into its original location (maintaining the original directory hierarchy). The Sentinel Log Manager database keeps track of what files were deleted, so you will need to update the entry in the database to inform it that this raw data file is no longer deleted. To do so, execute an `UPDATE SQL` command similar to the following for each raw data file you have restored:

```
UPDATE raw_data_files SET state = 'ARCHIVED' WHERE file_name = '/6D029DD0-
7F53-102C-B23E-000C294414C6/2009-01/10-0100.zip'
```

Updating the database will allow you to view the raw data file in the list of raw data files under the *Storage* > *Raw Data* tab of the Sentinel Log Manager user interface.

Alternatively, as the raw data is a text file, you can extract and then read the extracted raw data by using a text file reader.

Restoring Event Data from Tape

To restore event data, copy the data from tape back into its original location (maintaining the original directory hierarchy). The Sentinel Log Manager database keeps track of what event partitions were deleted, so you will need to update the entry in the database to inform it that this partition is no longer deleted. To do so, execute an `UPDATE SQL` command similar to the following for each event partition you've restored:

```
UPDATE ixlog_part SET state = 60 WHERE name = '20090811_408E7E50-C02E-4325-
B7C5-2B9FE4853476'
```

Where, the value for `name` is the directory name for the partition.

NOTE: Updating the database will allow you to perform searches and run reports on the data in this event partition by using the Sentinel Log Manager user interface.

As stated earlier in the NOTE above, Sentinel Log Manager will again begin to manage the life cycle of that partition and will eventually delete it again based on the same criteria that it deleted it in the first place. You can get around this by creating an additional retention policy with a very long minimum retention period and then reassigning the partition to use the new retention policy, as follows:

```
UPDATE ixlog_part SET ret_pol_id = '6faa7ec0-7f73-102c-bd20-001676e4a757'
WHERE name = '20090811_408E7E50-C02E-4325-B7C5-2B9FE4853476'
```

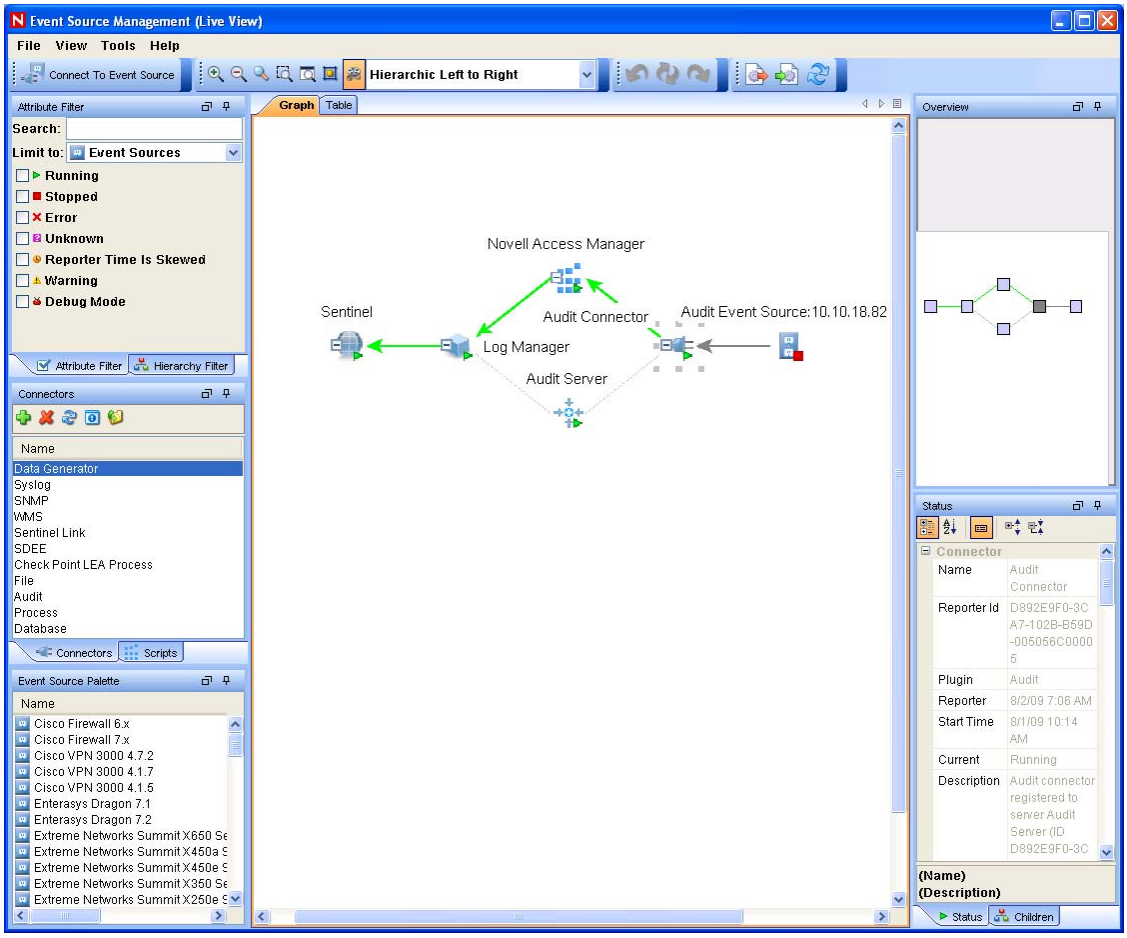
Where, the value for `name` is the directory name for the partition and the value for `ret_pol_id` is the id of the retention policy as listed in the md_config table.

Configuring Data Collection

4

Novell® 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.

Figure 4-1 *Hierarchy of Plug-ins In the Event Source Management (Live View)*



Novell Sentinel Log Manager supports a wide variety of Connectors and also includes a variety of Collectors with parsing logic for specific event sources.

For a list of supported connectors and event sources packaged with this release, see "System Requirements" in the *Sentinel Log Manager 1.0.0.4 Installation Guide*.

To download the new, additional and updated Collector and Connector plug-ins, see the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/sentinel61.html).

The configuration required to integrate a new event source with Novell Sentinel Log Manager varies depending on the type of event source and the communication method selected.

For more information about editing Collectors that are already included in the 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) and Collector documentation at the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/sentinel61.html) respectively.

The detailed documentation for Connectors and Collectors can be accessed by clicking on the *PDF* icon next to the Collector on the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/sentinel61.html).

Novell recommends that you review the full documentation for any new event source integration to ensure that all available features are enabled.

NOTE: Every Collector has its own associated Collector packs. The new Collector packs include reports that can be uploaded and used in the Sentinel Log Manager interface. For more information about extracting the reports, see Section 6.5, “Extracting the Reports from the Collector Packs,” on page 97.

4.1 Configuring Syslog Data Collection

The Sentinel Log Manager is preconfigured to accept syslog data from syslog event sources that are sending data over TCP (port 1468), UDP (port 1514), or SSL (port 1443). Additionally, if your firewall is enabled and supports iptables, Sentinel Log Manager automatically forwards events to UDP port 514 to port 1514.

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 your event sources, it automatically chooses the best Collector to parse the data, parses the data into events, and stores the event and raw data in the configured archived location. You can also configure Sentinel Log Manager to listen on additional ports.

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:

4.1.1 Configuring Syslog Servers

When you point your syslog event sources to Sentinel Log Manager, it automatically creates an event source entry to track data that is being received from the event source and to allow 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 that are generating the syslog messages, regardless of whether they are being aggregated by a syslog relay or not.

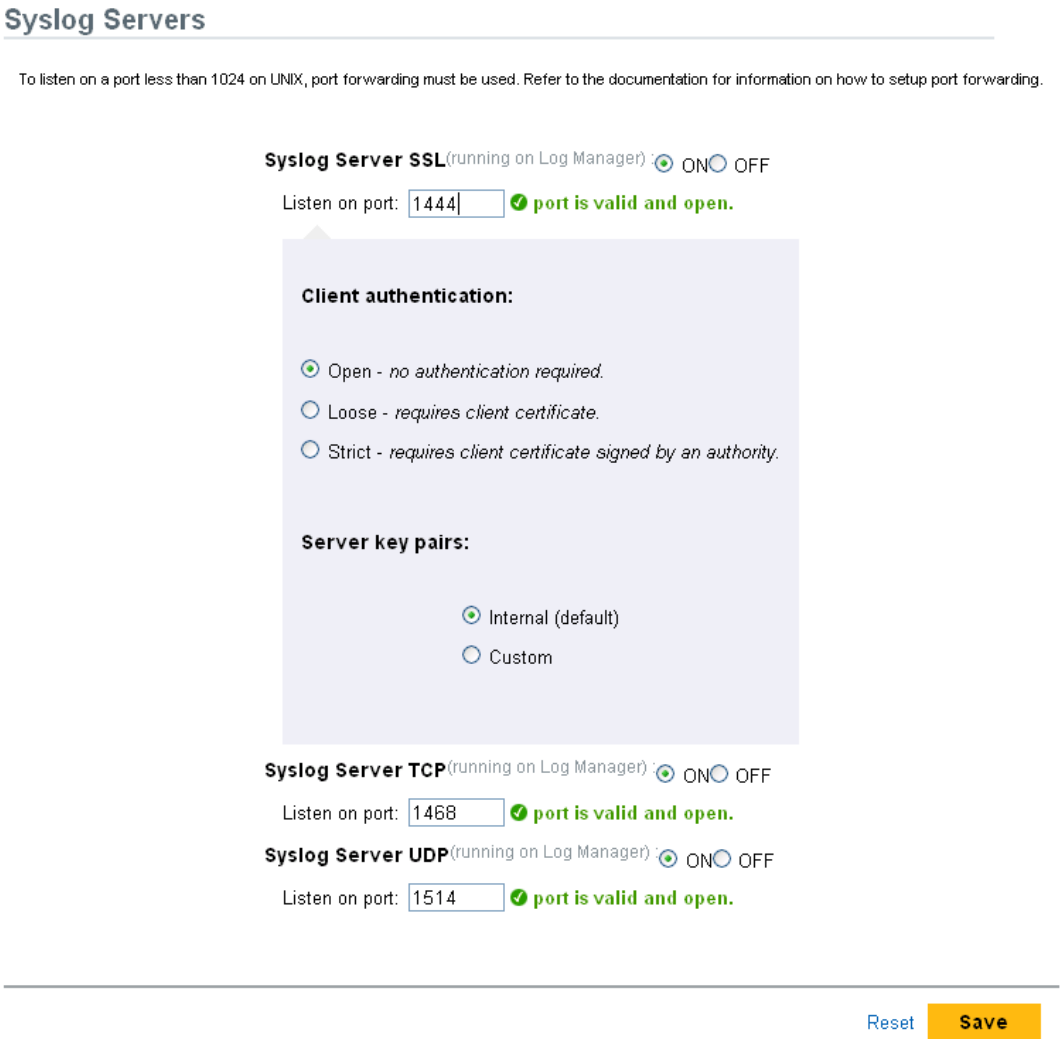
The Sentinel Log Manager web interface allows you to configure ports to listen on to receive syslog data.

To add or remove syslog servers, use the Event Source Management interface. For more information, see "Launching Event Source Management" on page 57.

In the *Syslog Server* section, you can start or stop data collection for each of the syslog server ports by using the on or off options next to them.

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

   The *Collection* tab is displayed on the right pane of the page.
3. Select the *Event Source Server*s 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 respectively.

5 To start or stop the data collection for each of the syslog server, 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 description of the status messages you get 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 `port is valid and open` message is displayed.
Red Cross Icon	If the specified port is not valid (non-numeric or not between 1 to 65535), a `port is not valid` 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 `port is valid but not open` 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 50.

8 Click *Reset* to change the specified settings to previous settings before saving it

9 Click *Save* to save the new settings.

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

4.1.2 Setting the Syslog Server Options

This section describes how to configure the type of client and sever authentication for syslog servers that uses SSL.

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 attempting to send their data. Use a strict client authentication policy that is applicable in your environment to prevent rogue syslog event sources from sending undesired data into the 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.

- “Importing a Truststore” on page 51
- “Server Key Pair” on page 52

Creating a Truststore

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

1. Log in to the Sentinel Log Manager server as novell.
2. Go to `/opt/novell/sentinel_log_mgr_1.0_x86/data/updates/done`.
3. To extract the `syslog_connector.zip` file.

   ```
   unzip syslog_connector.zip
   ```

4. Either copy the `TruststoreCreator.sh` or `TruststoreCreator.bat` file 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*. The keystore file must be imported into the truststore.

Importing a Truststore

For strict authentication, the administrator can import a truststore by using the *Import* button. This helps ensure that only authorized event sources are sending data to Log Manager. The truststore must include either the event source certificate or the certificate of the certificate authority that signed it.

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

To import a truststore:

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

   The *Collection* tab is displayed on the right pane 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 truststore file (for example, `my.keystore`)
6. Specify the password for the truststore file.
7. Click *Import*.
8. If desired, click *Details* to see more information about the truststore.
9. Click *Reset* to change the specified settings to previous setting before saving it
10. Click *Save*.

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

Server Key Pair

The Sentinel Log Manager is installed with a built-in certificate, 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 the Sentinel Log Manager as an administrator.
2. Click the *collection* link at the upper left corner of the page.

   The *Collection* tab is displayed on the right pane 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 truststore file.
6. Specify the password for the truststore file.
7. Click *Import*.

   If there is more than one public-private key pair associated with the file, select the desired key pair, and click *OK*.
8. Click *Details* to see more information about the server key pair.
9. Click *Reset* to change the specified settings to previous setting before saving it
10. 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 likely options in your firewall configuration interface to allow you to configure the same port forwarding as described here.

As Sentinel Log Manager runs as the novell user, it cannot directly listen on ports that are less than 1024. To listen on a port that is less than 1024, use port forwarding to forward data to a port that Sentinel Log Manager can directly listen on. Sentinel Log Manager comes with the *Install_Directory*`/bin/config_firewall.sh` script to assist you in getting port forwarding setup. This script contains an example command of forwarding UDP port 514 to port 1514. This script is automatically run every time Sentinel Log Manager service startup `/etc/init.d/sentinel_log_mgr` script is executed with the start option by the `root` user.

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
```

4.2 Configuring Data Collection for Novell Audit Server

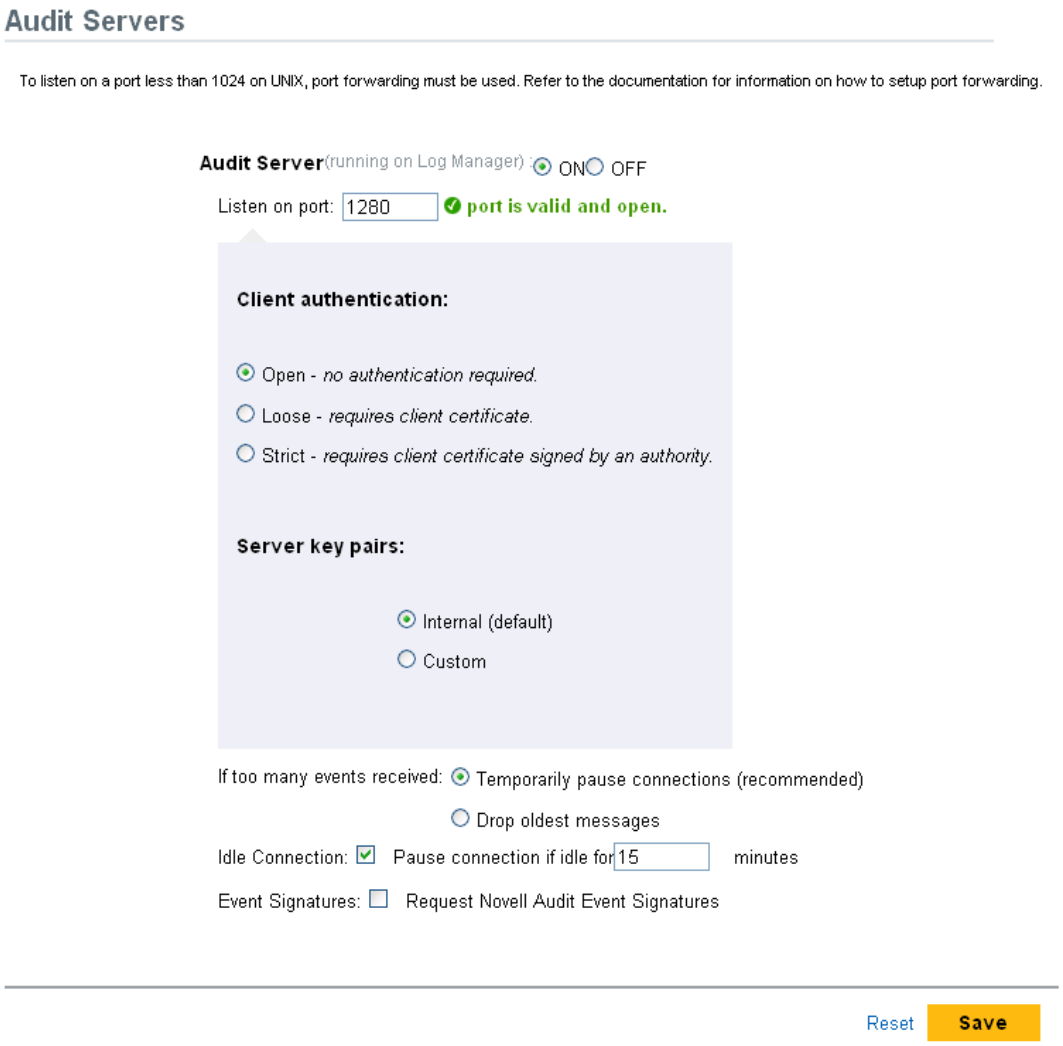
The following sections describe how you can configure audit server port to receive data and how you can set the audit server options:

4.2.1 Specifying the Audit Server Settings

To specify the data collection settings for the audit server:

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

   The *Collection* tab is displayed on the right pane of the page.
3. Select the *Event Source Servers* tab.



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

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 55.

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 55.

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

Temporarily pause connections: Drops the existing connections and stops accepting new connections until the buffer has space for the new messages. In the meantime, messages are cached by the event sources.

Drop oldest messages: Drops the oldest messages to accept new messages.

WARNING: There is no supported method for recovering dropped messages, if you select *Drop oldest 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 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 Click *Reset* to change the specified settings to previous settings before saving it

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 audit server and its event sources, see Section 4.4, "Managing Event Sources," on page 60.

4.2.2 Setting the Audit Server Options

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

- "Port Configuration and Port Forwarding for the Audit Server" on page 55
- "Client Authentication for the Audit Server" on page 55

Port Configuration and Port Forwarding for the Audit Server

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

Binding to ports less than 1024 requires root privileges. So use a port greater 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 event source 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) 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`*

   where *protocol* is tcp or udp, *incoming port* is the port on which the messages are arriving, and *IP:rerouted port* is 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 Truststore" on page 56
- "Importing a Truststore" on page 56
- "Server Key Pair" on page 57

Creating a Truststore

For strict authentication, you must have a truststore that contains either the event source's certificate or the certificate for the certificate authority (CA) that signed the event source's certificate. After you have a DER or PEM certificate, you can create the truststore by using the CreateTruststore utility that comes with Log Manager.

1. Log in to the Sentinel Log Manager server as novell.
2. Go to `/opt/novell/sentinel_log_mgr_1.0_x86/data/updates/done`.
3. Unzip the `audit_connector.zip` file.

   ```
   unzip audit_connector.zip
   ```
4. Either 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`) in it. It is protected by the password *password1*.

Importing a Truststore

For strict authentication, the administrator can import a truststore by using the *Import* button. This helps ensure that only authorized event sources are sending data to Log Manager. The truststore must include either the certificate of the event source or the certificate of the certificate authority that signed it.

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

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

   The *Collection* tab is displayed on the right pane 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 truststore file (for example, `my.keystore`)
6. Specify the password for the truststore file.
7. Click *Import*.

8 If desired, click *Details* to see more information about the truststore.

9 Click *Reset* to change the specified settings to previous setting before saving it

10 Click *Save*.

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

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 the Sentinel Log Manager as an administrator.

2 Click the *collection* link in the upper left corner of the page.

The *Collection* tab is displayed on the right pane 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 truststore file.

6 Specify the password for the truststore file.

7 Click *Import*.

If there is more than one public-private key pair in the file, select the desired key pair and click *OK*.

8 Click *Details* to see more information about the server key pair.

9 Click *Reset* to change the specified settings to previous setting before saving it

10 Click *Save*.

4.3 Configuring Data Collection for Other Event Sources

The *Advanced* tab is used to monitor and configure advanced data collection capabilities beyond the settings currently available in the web interface.

4.3.1 Launching Event Source Management

You can add Collectors, Connectors, and event sources in the Event Source Management (Live View) window and point to log manager for the data collection.

Java 1.6 Web Start is required to launch the Event Source Management Web application. If Java is not installed on your system, click *Download Java* link. The Java Download page appears in a new tab. Click the *Free Java Download* button to download the Java from Sun Microsystems Web site.

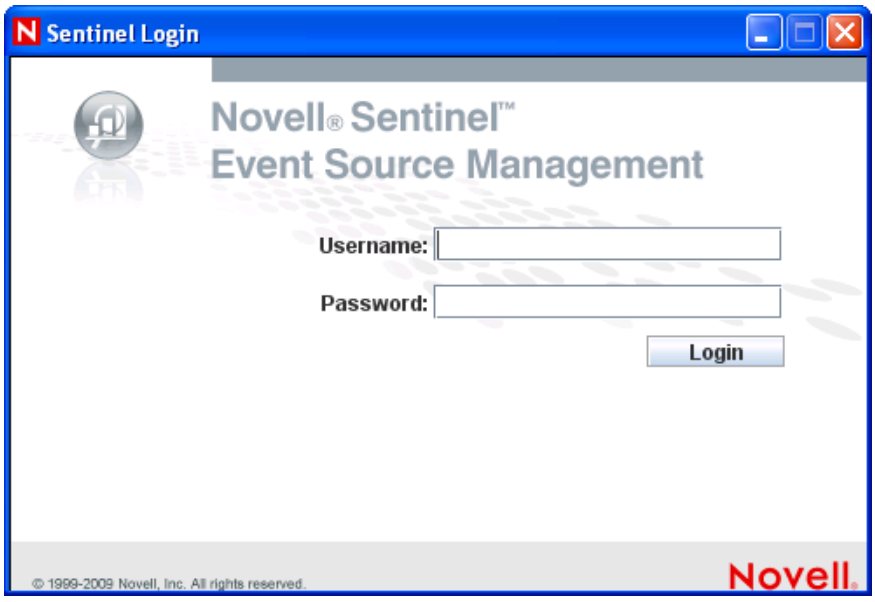
NOTE: Update the JRE to the JRE 1.6 Update 13 (both 32 and 64 bit versions), if you are using the openSUSE 11.1. Then use the java web start (javaws) launcher command to launch the ESM.

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

- Add or edit 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 Live View.
- View and configure Connectors and Collectors that are installed with Sentinel.
- 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 using these components.

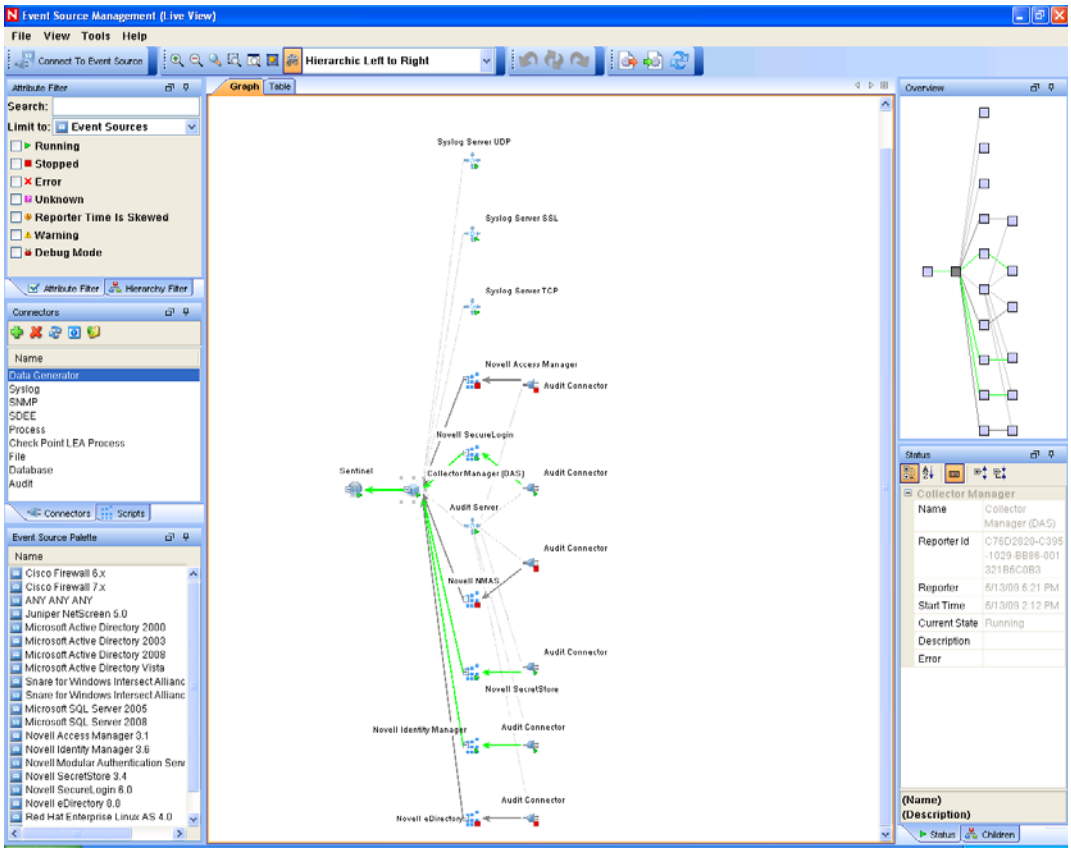
Use the following procedure to launch the Event Source Management (Live View) window:

1. Log in to the 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 *Launch* button to launch the Event Source Management (ESM) interface.
5. The Novell® Sentinel™ Event Source Management Login window is displayed.



6. Specify the administrators username and password, to login to Novell Sentinel Log Manager, then click *Login*.

   The report administrator user's and auditor user's cannot login to Novell Sentinel Event Source Management interface.
7. 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 and the event sources that are providing data to Sentinel. 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 then can be monitored in real time within the ESM interface.

8 The following table describes about 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.
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 ESM.

Component	Description
Collector	Collectors instantiate the parsing logic for data from a particular event source. Each Collector icon in ESM 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 6.1Content 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 ESM represents the Connector code as well as the runtime configuration of that code. You can download the Connectors from the Sentinel 6.1 Content 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	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 Server	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 done 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/#admin).

4.4 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.

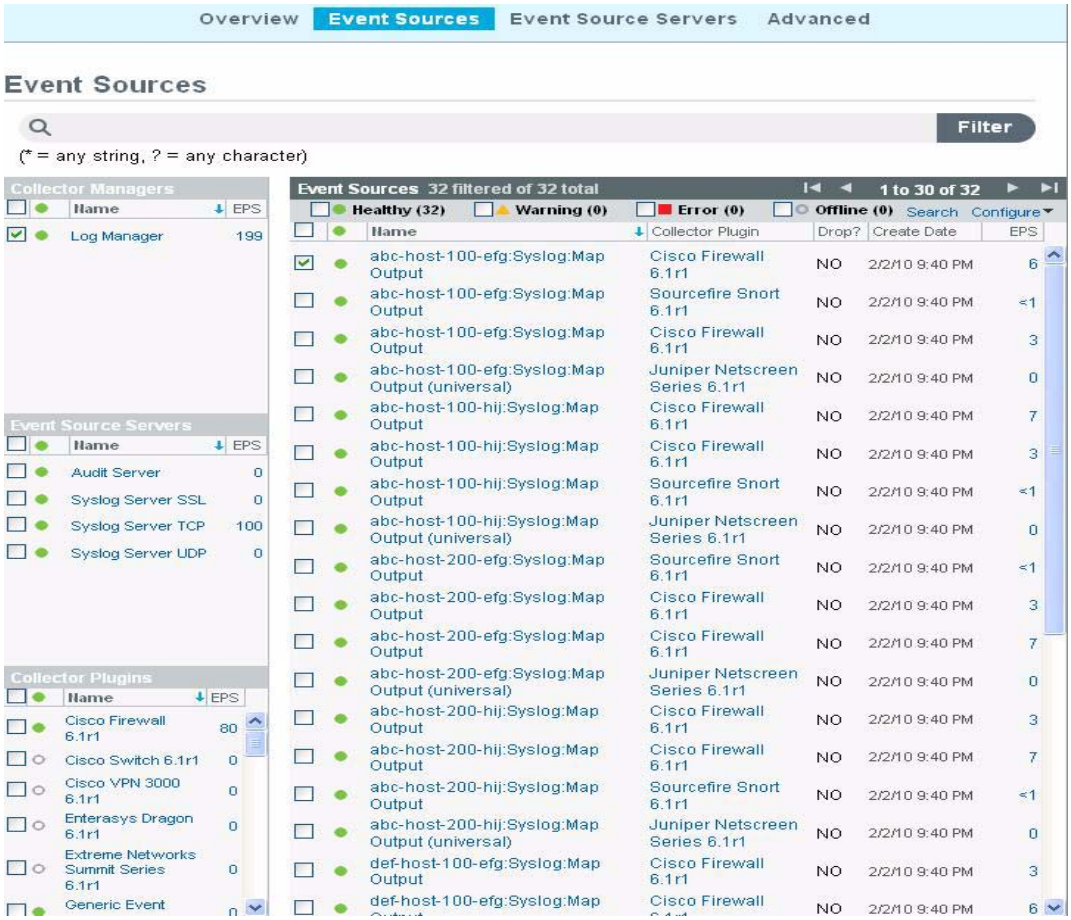
You can refine the displayed event sources by selecting Collector Managers, Event Source Servers, and Collector Plugins. You can also specify a filter on the event source name and select particular event source health states you want to view. All of these refinement selections and filters are stored 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 refinement selections.

To view the event sources:

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

   The *Collection* tab is displayed on the right pane of the page.
3. Click the *Event Sources* tab.

   The Event Sources page is displayed.



The left pane of the Event Sources page has following three sections:

Collector Managers: Lists all of the Collector Managers associated with the Sentinel system.

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

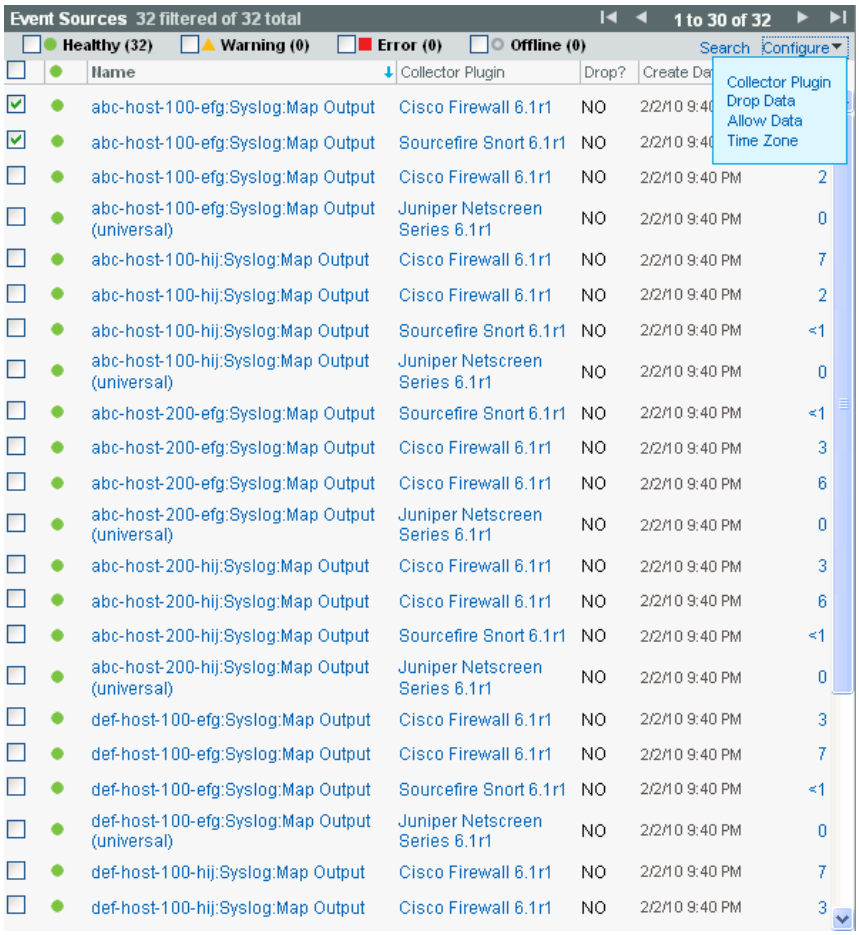
Collector Plugins: Lists all of the Collector plug-ins associated with the Sentinel system.

The *Event Sources* section at 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 "Launching Event Source Management" on page 57.

---

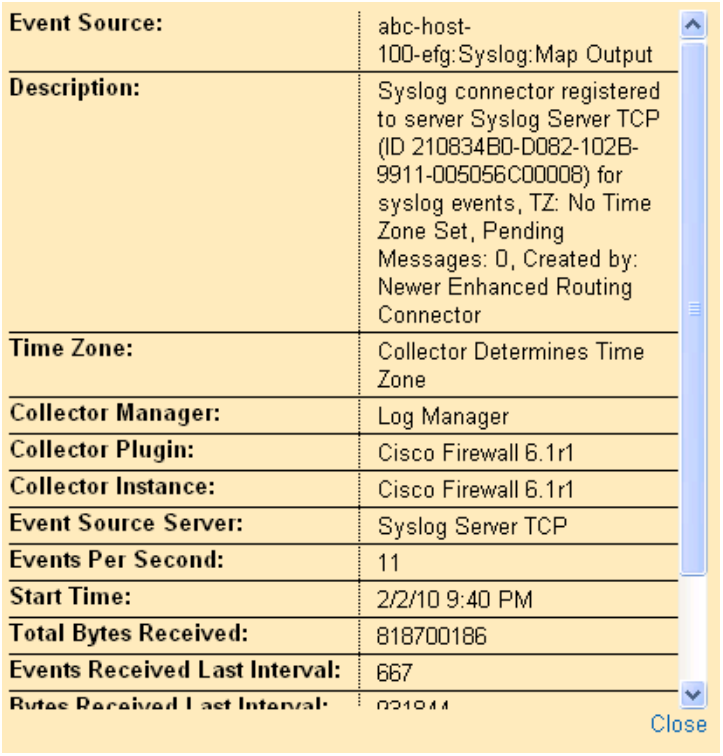
4 In the *Event Sources* section, to select or deselect the event sources, click the check boxes next to the respective event source.



To select all the available event sources, click 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. When you click the column header the respective column header displays in bold text. When a column header is first clicked, the sort order will be ascending. A blue down arrow will be displayed to indicate that the sort order is ascending. If the column header is clicked a second time, the sort order will be changed to descending, and a blue up arrow will be displayed to indicate that the sort order is descending.

When you click the event source's *Name* or *EPS* value, a pop-up is displayed with additional information about the event source. The pop-up displays the *Event Source*, *Description*, *Time Zone*, *Collector Manager*, *Collector Plugin*, *Collector Instance*, *Event Source Server*, *Events Per Second*, *Start Time*, *Total Bytes Received*, *Events Received Last Interval*, *Bytes Received Last Interval*, *Interval*, *Last Time Bytes Received*, *Health*, and *Error* fields with their values. When you click the *Collector Plugin* column, a pop-up is displayed with additional information about the collector plug-in.



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

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

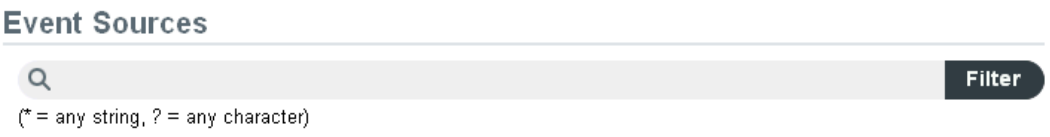
Columns	Description
Collector Plugin	Specifies the collector plug-in name the event source is connected to. **NOTE:** This is the name of the collector plug-in, not the name of the collector instance. You can sort the event sources based on collector plug-in name.
Drop	Specifies whether data from the associated event source should be dropped or not. **YES:** If *Drop Data* is set to YES, all data received from the event source is dropped. This means that the raw data will not be saved and events will not be generated. **NO:** If *Drop Data* is set to NO, all raw data from the event source is saved and events are generated. When 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 may not get generated if the filter causes the data to be ignored. You can sort the event sources based on the drop data status.
Create Date	Specifies the date and time when the event source was created. You can sort the event sources based on when they were created.
EPS	Specifies the events per second value received from the event source. You can sort the event sources based on their events per second value. **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.

5 To filter the event sources by name, type a name value in the filter text box, then click *Filter*.

Matching value is case insensitive. The name value may 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*`. Below are some common filter type examples:

- 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 the `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.

6 To view the event sources based on the health status, select the *Healthy*, *Warning*, *Error*, and *Offline* check boxes.

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

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

---

7 To display only event sources that are connected to particular Collector Managers, select one or more Collector Managers from the *Collector Managers* section.

NOTE: If none of the Collector Managers are selected, event sources refinement is not performed based on the Collector Managers. It is essentially equivalent to selecting all Collector Managers.

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

To select all the available Collector Managers, click 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.

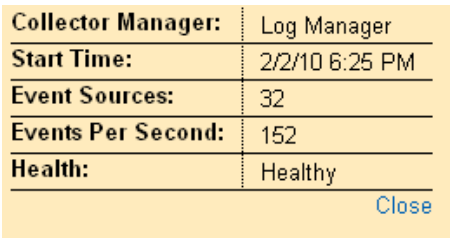
NOTE: If none of the Collector Managers are selected, the event sources table displays all the configured event sources.

The following fields are available in the *Collector Managers* section:

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.

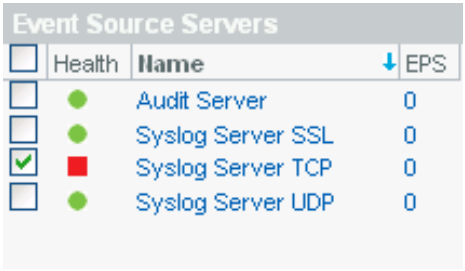
- **Health:** Indicates the health of the Collector Managers. You can sort the Collector Managers based on their health status.
- **Name:** Displays the name of the Collector Managers. You can sort the Collector Managers in alphabetical order based on their names.
- **EPS:** Displays the events per second value received from the event sources. You can sort the Collector Manager based on the events per second value.

When you click the *Name* or *EPS* value column, a pop-up is displayed with additional information about the Collector Manager. The pop-up displays the *Collector Manager*, *Start Time, Event Sources*, *Events Per Second*, and *Health* fields with their values.



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

NOTE: 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 will also include event sources that are not connected to any event source server.



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

To select all the available event source servers, click the check box at the top of the column.

The right pane displays the list of event sources connected to the selected event source servers.

NOTE: If none of the event source servers are selected, the event sources table displays all of the configured event sources, including event sources which are not connected to any event source server.

To sort the event source servers 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.

- **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.

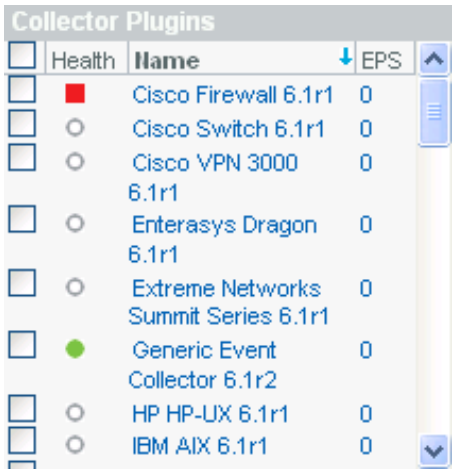
When you click the *Name* or *EPS* value column, a common pop-up is displayed with additional information about the event source server. The pop-up displays the *Event Source Server*, *Description*, *Collector Manager*, *Event Sources*, *Port*, *Events Per Second*, *Start Time*, *Total Bytes Received*, *Bytes Received Last Interval*, *Interval*, *Last Time Bytes Received*, *and Health* fields with their values.

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

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

NOTE: 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.



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

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

The right pane displays the list of event sources connected to all the Collector instances of the selected Collector plug-ins.

NOTE: If none of the collector plug-ins are selected, the event sources table displays all the configured event sources.

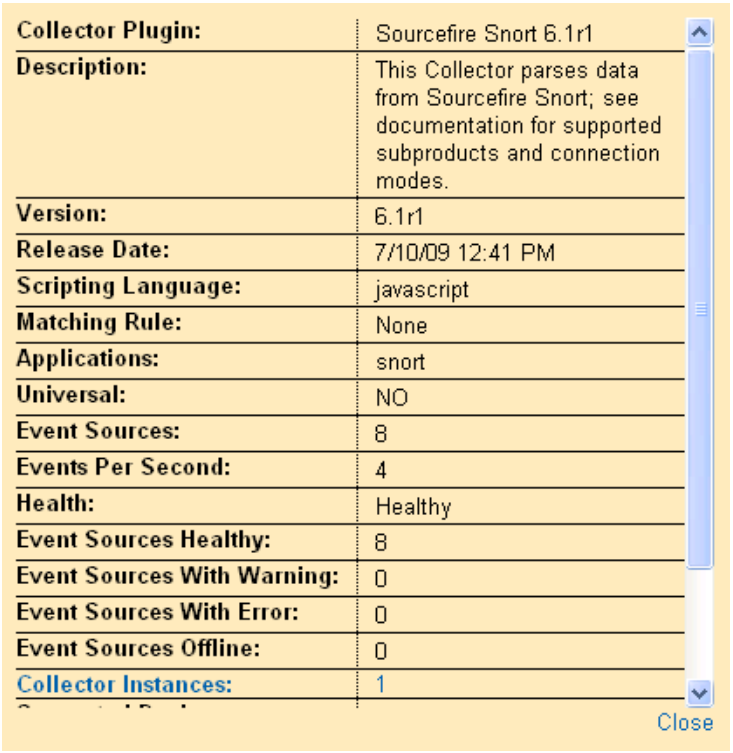
To sort the collector plug-ins by *Name* or *EPS* values, click the appropriate column header. When you click the column header the respective column header displays in bold text.

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

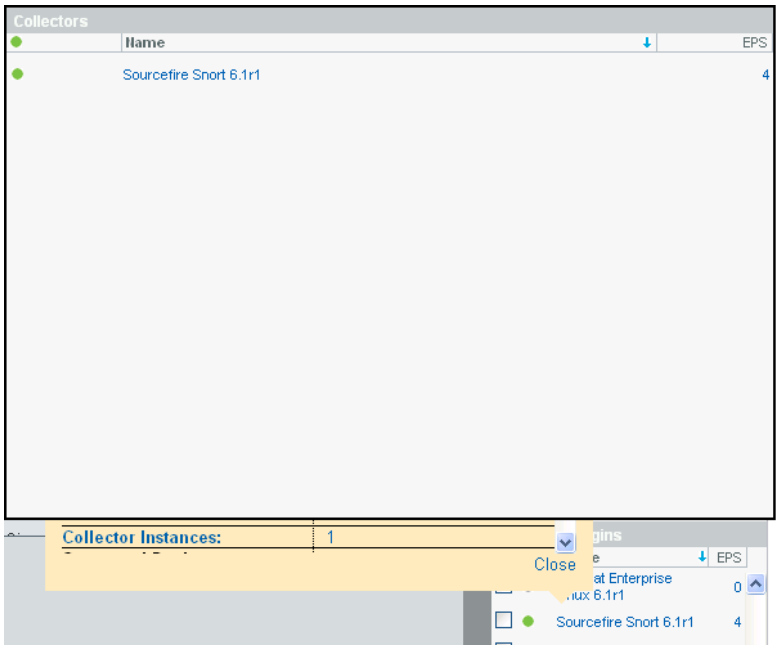
  With the exception of the green icon (healthy state), the icon does not necessarily mean that all event sources connected to the collector plug-in are in state indicated by the icon.

  The red icon (error state) indicates that one or more event sources connected to the collector plug-in are in an error state, not necessarily all of them. To get more detailed information, click on the *Name* or *EPS* column value to see a help pop-up. The help pop-up will show additional information about the collector plug-in health state.
- **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.

When you click the *Name* or *EPS* value column, a pop-up is displayed with additional information about the event source server. The pop-up displays the *Collector Plugi*n, *Description*, *Release Date*, *Scripting Language*, *Matching Rule*, *Applications*, *Universal*, *Event Sources*, *Events Per Second*, *Health*, *Event Sources Healthy*, *Event Sources With Warning*, *Event Sources With Error*, *Event Sources Offline*, *Collector Instances* and *Supported Devices* fields with their values.



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



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

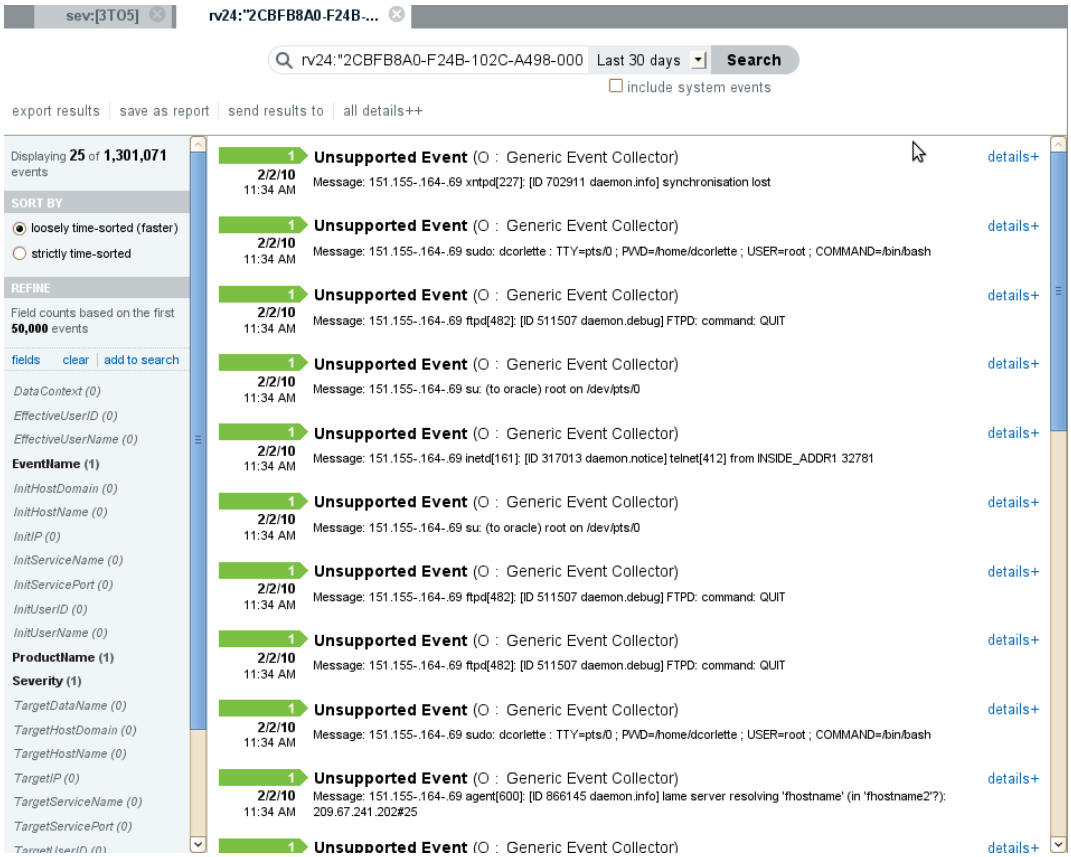
The Event source section displays 30 event sources per page.

11 To view the event search result for an event source, select the event source from the list and click the *Search* link.

A new search results tab is displayed with the search results 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.

Results for all selected event sources will be returned as shown in the following image:



12 To change the data logging status for one or more event sources, select the event sources from the list, click the *Configure* link, and select either *Drop Data* or *Allow Data* option,

Drop Data: If *Drop Data* is selected, the selected event source(s) will drop all the events received. Messages will not be sent to the collector(s) the selected event sources are connected to.

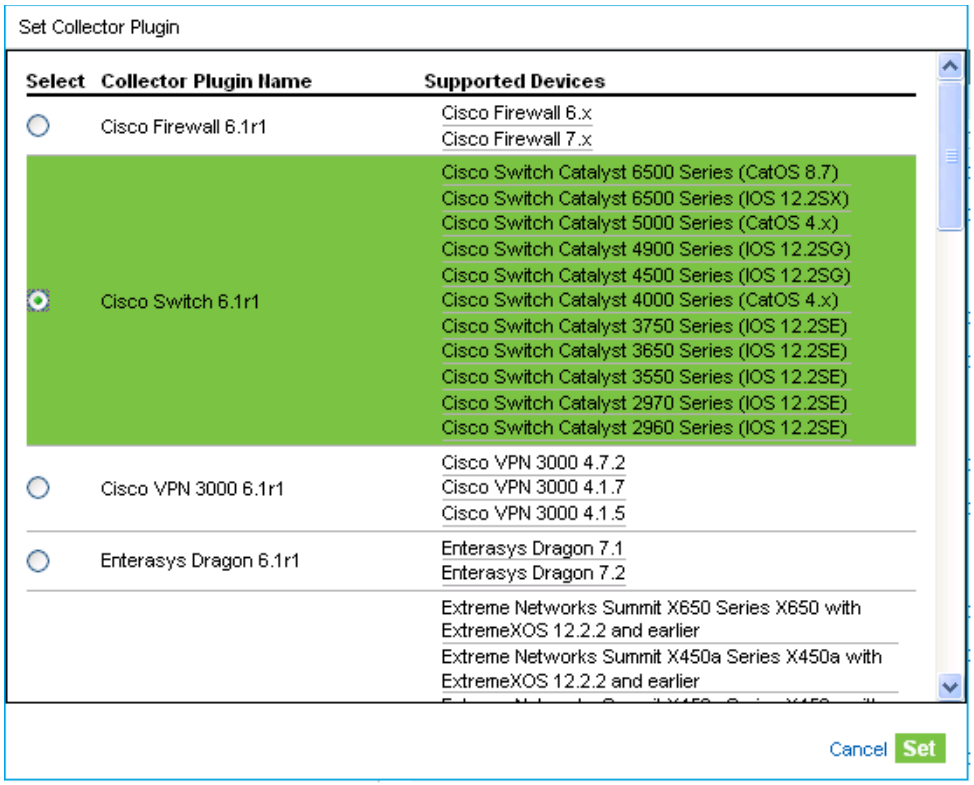
Allow Data: If *Allow Data* is selected, the selected event sources will forward events received to the Collector(s) they are connected to.

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

---

13 To change the associated collector plug-in for one or more event sources, select the event source(s) from the list, click the *Configure* link, and select the *Collector Plugin* option.

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



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

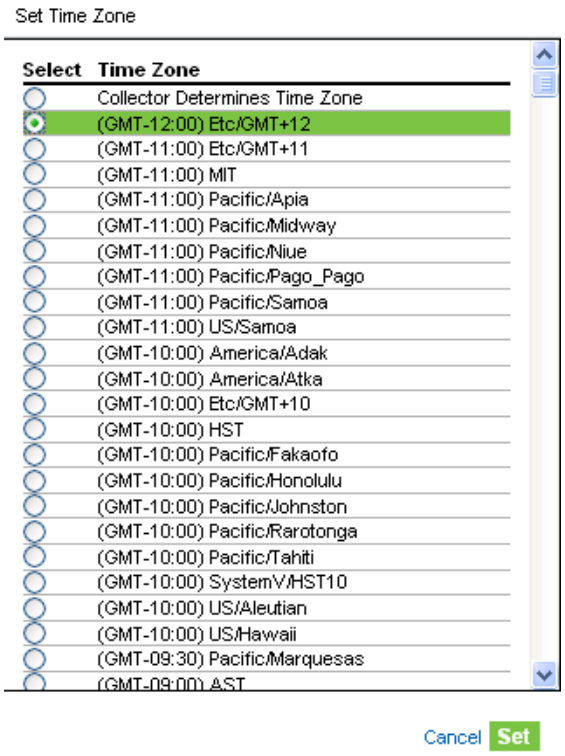
The selected event sources are connected to the selected Collector plug-in.

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

---

15 To change the time zone setting for one or more event sources, select the event source(s) from the list, click the *Configure* link, and select the *Time Zone* option.

The *Set Time Zone* window is displayed.



16 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 will not show the new time zone until after the changes are complete, and the display is refreshed from the database.

Changes on this page might take some time to display completely.

4.5 Viewing Events Per Second Statistics

- Section 4.5.1, “Viewing Graphical Representation of Events Per Second Value,” on page 72
- Section 4.5.2, “Viewing Events Per Second Value of Event Source Servers,” on page 73

4.5.1 Viewing Graphical Representation of Events Per Second Value

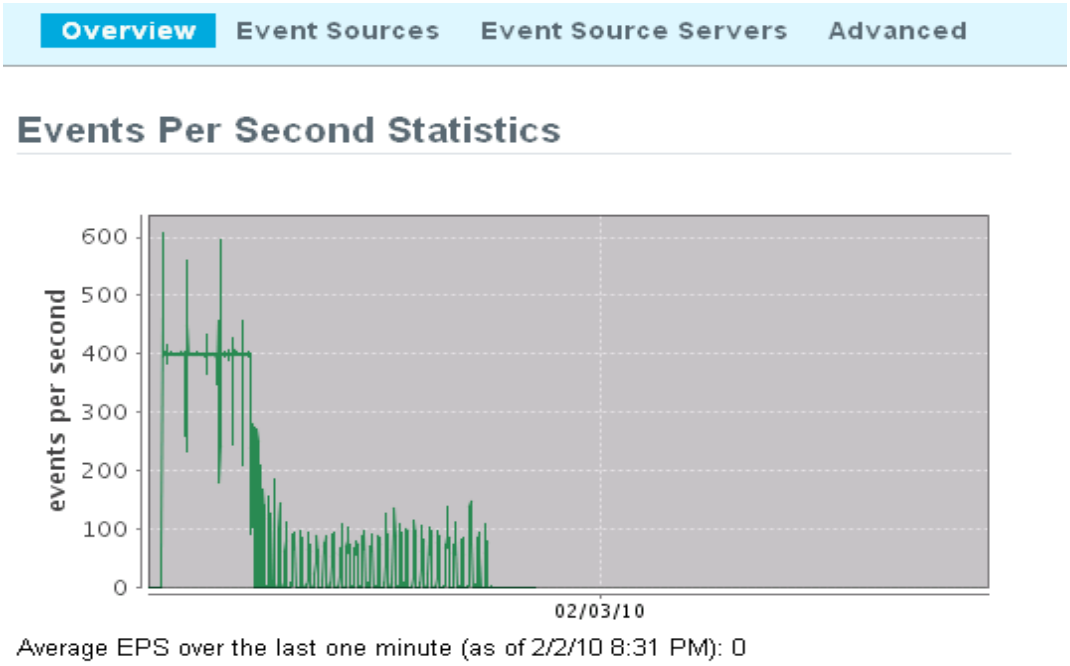
1 Log in to the Sentinel Log Manager as an administrator.

2 Click the *collection* link in the upper left corner of the page.

The *Collection* tab is displayed on the right pane of the page.

3 In the *Overview* section, you can view events per second 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.



4.5.2 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.

   The *Collection* tab is displayed on the right pane 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.

Searching

5

Novell® Sentinel™ Log Manager can perform a search on events. Each time you perform a search for an event, a tab opens with the search results. In each tab you can again refine your search.

The search includes all the online data currently in the flat files at the `data` directory and the archived data in zip format at the configured location; and can also include searching of internal events of Sentinel Log Manager if you select *Include System Events*. By default, events are returned in a loosely time sorted order in reverse chronological order. This sort order relates to how the events are stored in the file system partitions.

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).

This section gives you an understanding of searching for an event, refining search results, viewing search results, exporting the search results, saving a search query as report template, and sending the search results to an action instance.

5.1 Running an Event Search

Users can run simple or advanced searches.

5.1.1 Running a Basic Search

A basic search runs against all of the event fields listed in Table C-1 on page 149. Few basic searches include the following event values:

- `root`
- `127.0.0.1`
- `Lock*`
- `driverset0`

NOTE: If time is not synchronized across your server, client, and event sources, you might get unexpected results from your search. Searches for the time durations such as Custom, *Last 1 hour*, and *Last 24 hours* display results based on the timezone of the machine on which the search is performed.

To run a basic search:

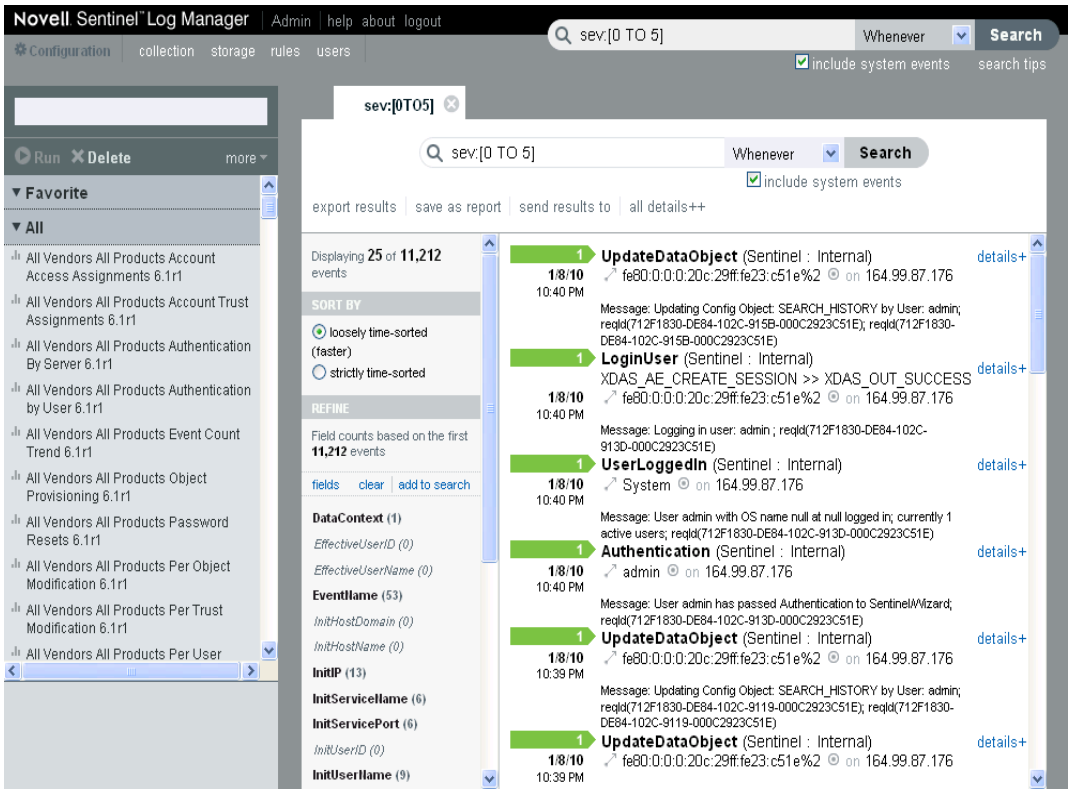
1. Type the Search criteria in the *Search* field and click the *Search* button on the upper right corner of the page.

   Sentinel Log Manager is configured to run a default search for non-system events with severity 3 to 5 when a user clicks the *Search* button for the first time. Otherwise, it reuses the last search term the user entered.

   To know more about the case-sensitive fields and tokenized (not case-sensitive) fields, see Appendix C, "Event Fields," on page 149.

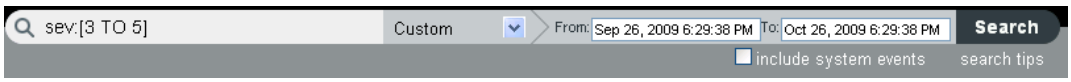
2. For using a different search criteria, type the search term in the *Search* field (for example, `admin`).

   To retrieve all the log events from all the sources, select *Include System Events* to include events that are generated by Sentinel Log Manager system operations, and run the search for the `sev:[0 TO 5]` as shown in the following image:



3 Select a time period for the search. Most of the time settings are self-explanatory, and the default is *Last 30 Days*.

- *Custom* allows you to select a start date and time and an end date and time for the query. The start date should be lower than the end date, and the time is based on the machine's local time.
- *Whenever* searches both online and archive data in the data directory.



4 Click *Search*.

All fields in the index are searched for the specified text. A spinning icon indicates that the search is taking place.

The event summary displays the search results on the search dashboard pane.

5.1.2 Running an Advanced Search

An advanced search can search for a value in a specific event field or fields. The advanced search criteria are based on the short names for each event field and the search logic for the index. To know about the field names, their descriptions, the short names that are used in advanced searches, and to know whether the fields are visible in the basic and detailed event views, see Table C-1, "Event Fields," on page 149.

NOTE: To perform a search, click the *search tips* link to use the tag names defined in the table.

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:authentication 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 source IP of 123.45.67.89 and an event of 'Set Password'.)

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

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

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

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

The advanced search criteria are modeled on the search criteria for the Apache* Lucene* open source package. More details about the search criteria is available at Lucene Query Parser Syntax (http://lucene.apache.org/java/2_3_2/queryparsersyntax.html).

5.1.3 Search Expression History

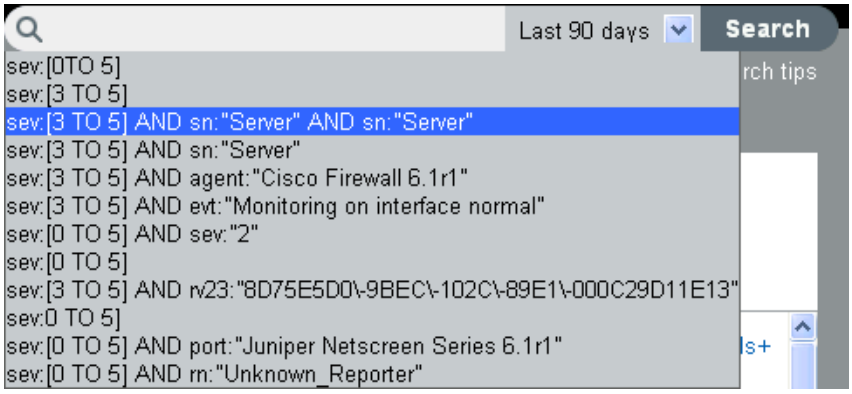
Sentinel Log Manager allows you to select a search expression value from the recently used search expressions list, while performing a search. When you click or enter a value in the *Search* text box, recently used search expressions values appear. You can select one of the search expression values to re-execute the same search.

- When you enter a text value in the *Search* text box, the closely matched search expressions values appear in the recently used search expression list.

  The search expression history list displays a maximum of 15 expressions values.
- When the text is not entered in the *Search* text box, the search expression list displays the recently used search expressions. The most recent search expression value appears at the top of the list.
- For each user, a maximum of 250 search expressions values are stored. Once the number of search expressions exceeds the 250 value, the oldest ones are deleted from the list.

The following image displays the recently used search expressions list:

Figure 5-1 *Displays the Search Expression History list*



5.2 Refining Search Results

You can refine the search results based on a specific event field. You can use the search refinement pane in the Sentinel Log Manager User Interface to refine search results.

The refinement event fields listed in the Sentinel Log Manager User Interface are on a per-user basis and the settings are restored across sessions and at additional searches.

If you have multiple search tabs, you can select different event fields for each of these tabs. If you save these event field selections, then the subsequent searches display the event fields saved in the previous setting.

For more information on each of these event fields, see Appendix C, “Event Fields,” on page 149.

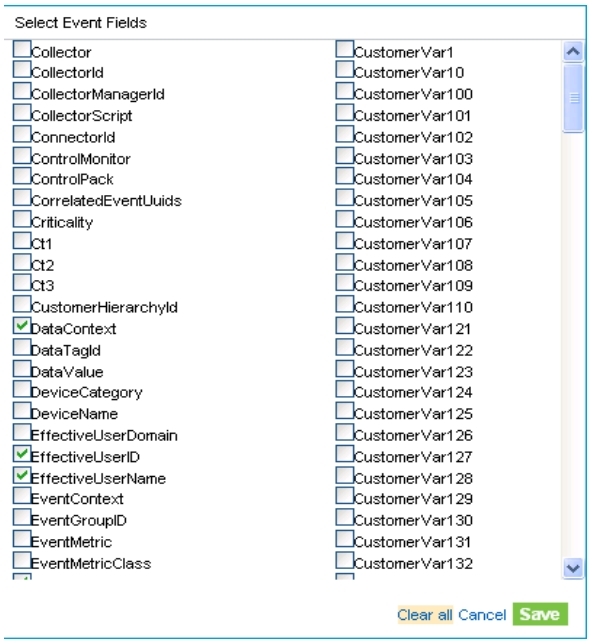
For performance considerations, the number of events sampled to calculate the event field value statistics are limited. If the search result set contains less than 50,000 events, the refinement field will be based on the entire result set. However, if the result set contains more than 50,000 events, only the first 50,000 will be sampled. The sampling size is displayed in the field count label as `Field counts based on the first <sample-size> events`, where `<sample-size>` will be 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 75.
3. Select an option from *SORT BY* to sort the search results.

   You can sort the search results based on the time when the event occurred and when the event was stored.
4. Click *fields* in the *REFINE* section.The *Select Event Fields* window is displayed.



NOTE: The events selection is on a per-user basis. Each user can have a different set of selected events.

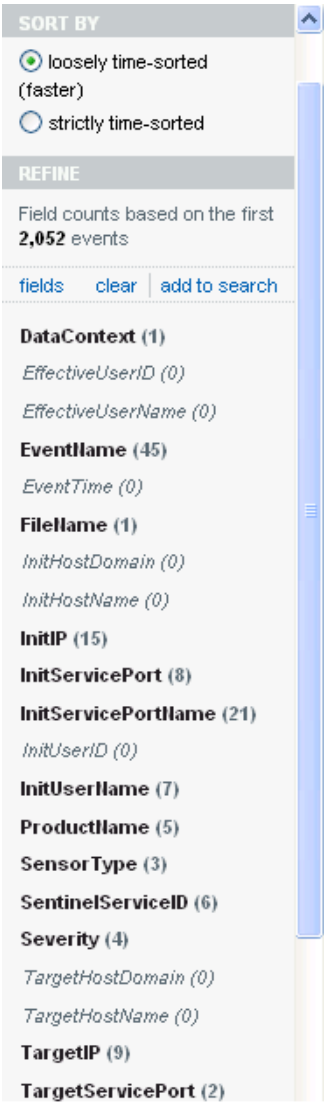
4a To refine the search, select the event fields from the available fields, and click *Save*.

4b To deselect all the selected event fields, click the *Clear all* link.

4c To undo any changes, and click *Cancel*.

5 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.



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

1. The refinement performs a new search with the additional terms intersected with the initial search string (using an AND operator). The new search will be run against all the events in the system, including the result set from the initial search. If new events came into the system that matches the refined search, they will be shown in the resultant set and the event count would be greater than the field value count.

2. If there are more than 50,000 events, the event field statistics will be 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. So, in the above scenario the displayed value count would be 50, but when the search is refined with this value it would return 1,000 events.

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

For example, if the search results contained events that had severities 1, 2, 5, and 4, then the event field will be 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 side represents the number of times the value appears in the search result.

If there are multiple unique values occurring at the same number of times in a search, then 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, of which an event of severity 4 was logged most recently, then the unique value 4 would appear at the top of the list.

7 To save the selected unique values in the search refinement term popup, click *OK*.

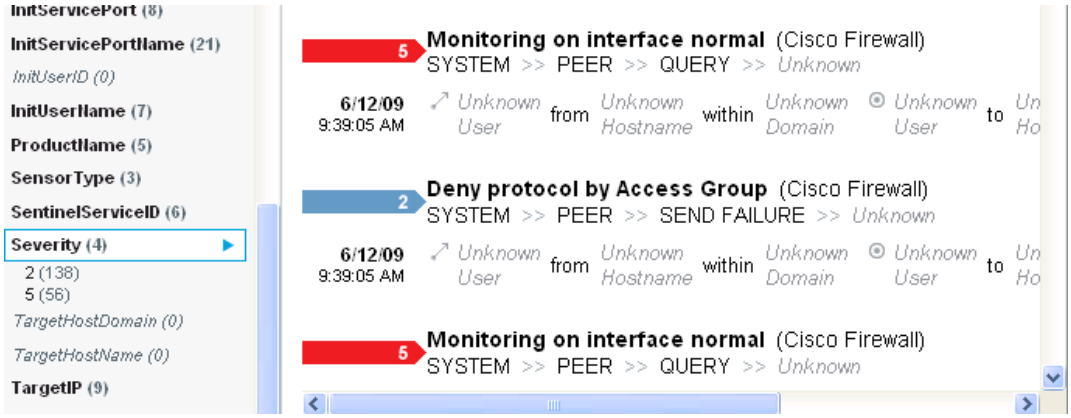
8 To display the unique values in the order of least frequent to most frequent, click *reverse*.

NOTE: 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.

---

9 Select one or more of the unique value check boxes to refine the search results for the particular event field, and then click *Save*. Selected event field values are listed under the event field in the *REFINE* pane.

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



10 Repeat Step 4-Step 9 to further refine the search.

11 Click *clear* to clear the selected unique event field values from the *REFINE* pane and to return to the previous search results.

12 Click *add to search* to add the refined search values to the current search tab and to perform a new search after recalculating the unique event field values and counts.

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

5.3 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 5.3.1, “Basic Event View,” on page 82
- Section 5.3.2, “Event View with Details,” on page 83

5.3.1 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. If the Collector that processed the raw data could not find the information for a particular event field, information for that field is not displayed or is labeled as *Unknown*.

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. If you do not see the information, check to see if you need to reconfigure the system to send the syslog data to include the missing information

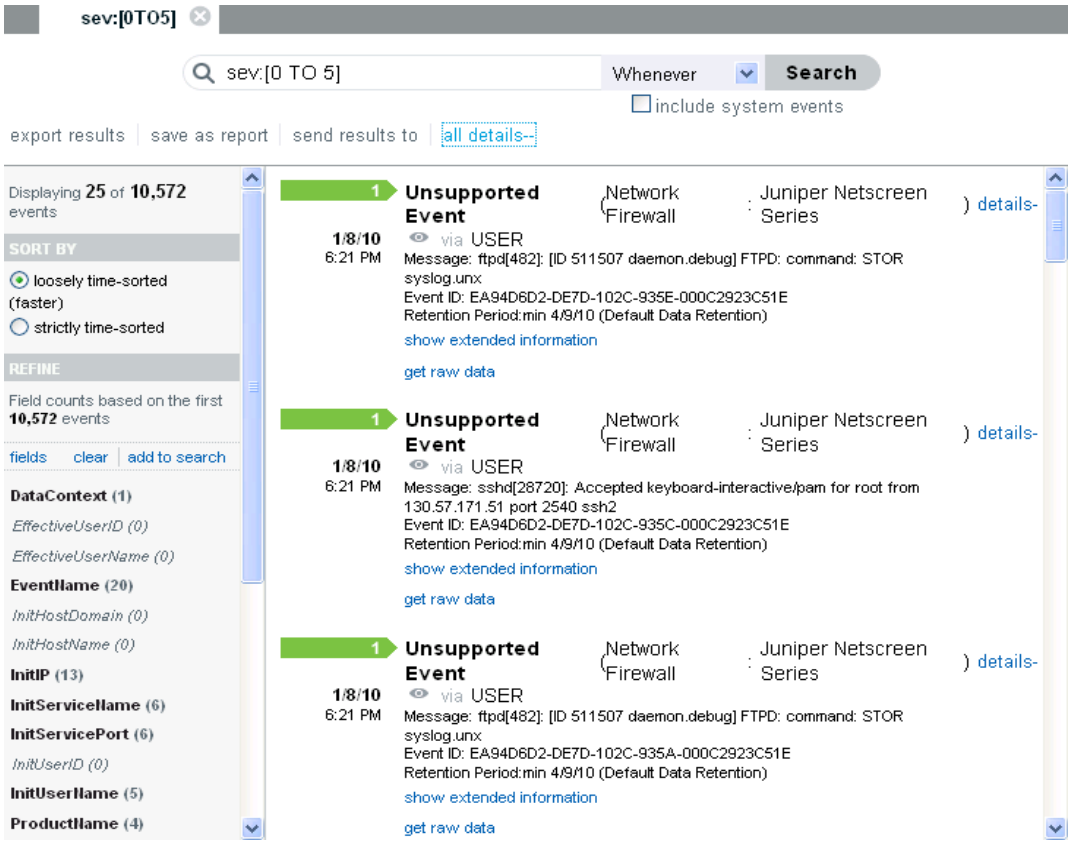
If the Collector parsing logic could not parse the existing raw data, the fields might not be displayed or might be labeled *Unknown*. To fix this, the Collector parsing logic needs to be enhanced.

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 inserted into 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 in the `data` directory and the search is shown as successful.

5.3.2 Event View with Details

1 To view the details about all the events, click the *all details* link at the top of the search results page.

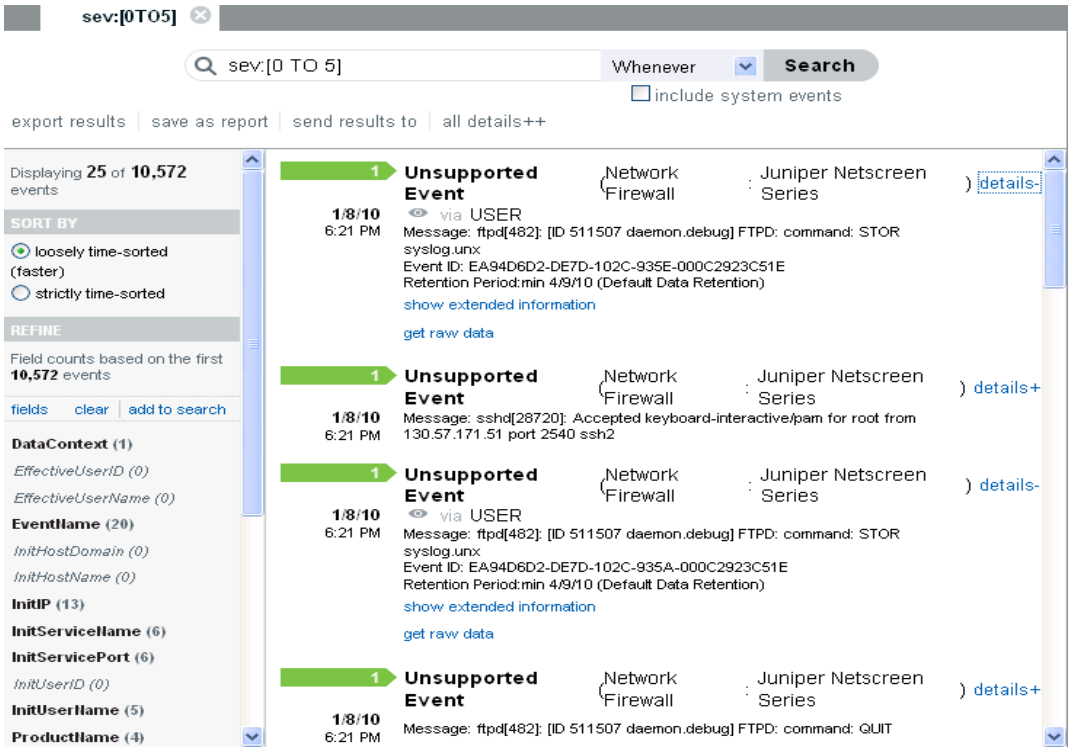
You can expand or collapse the details for all events on a page by using the *all details+* or *all details-* link.



2 To view details about any individual event, click the *details* link at the right side of the page.

You can expand or collapse the details for all events on a page by using the *details+* or *details-* link.

For example, you can display the Message, Event ID, and default data retention duration information for the events.



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

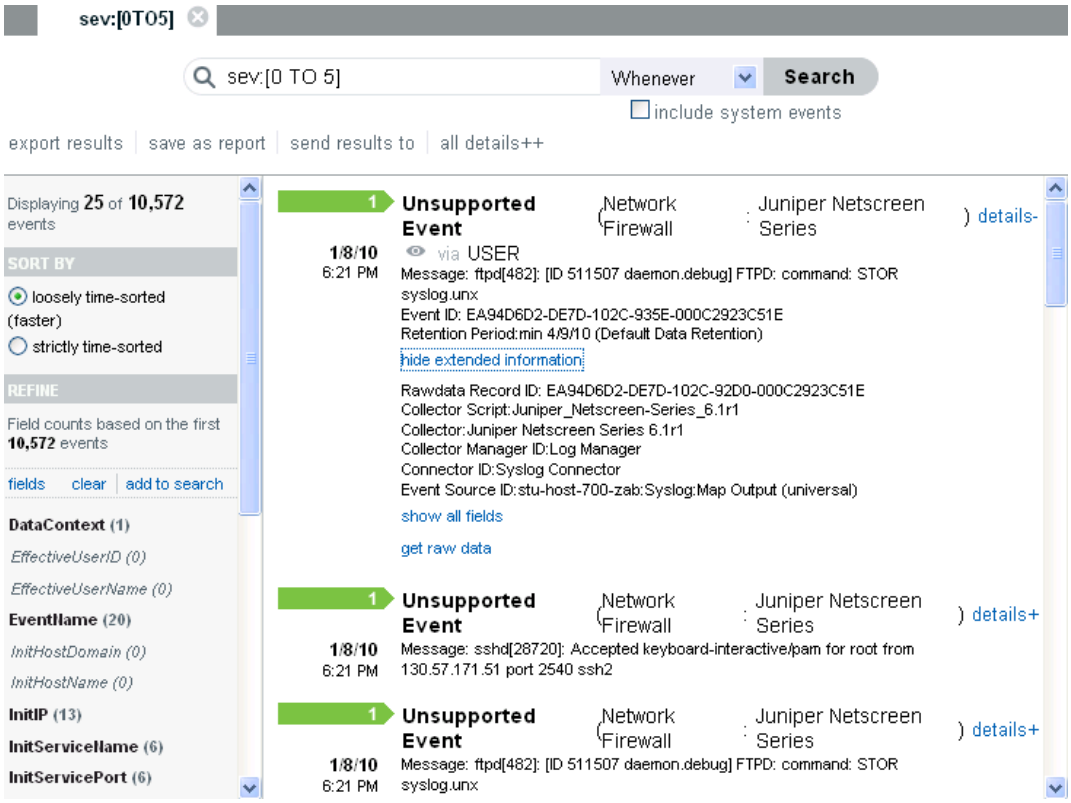
You can expand or collapse this information by using the *show extended information* or *hide extended information* links.

For example, it displays 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 Script:** Displays the name of the collector script. When you click the *Collector Script* field value, the value is added to the current search and provides information about other events parsed by the same collector script.
- **Collector name:** Displays the name of the collector. When you click the *Collector name* field value, the value is added to the current search and provides information about other events parsed by the same instance of the collector.
- **Collector Manager ID:** Displays the name of the Collector Manager. When you click the *Collector Manager ID* field value, the value is added to the current search and provides information about other events coming from the same Collector Manager.
- **Connector ID:** Displays the name of the connector. When you click the *Connector ID* field value, the value is added to the current search and provides information about other events coming from the same Connector node.

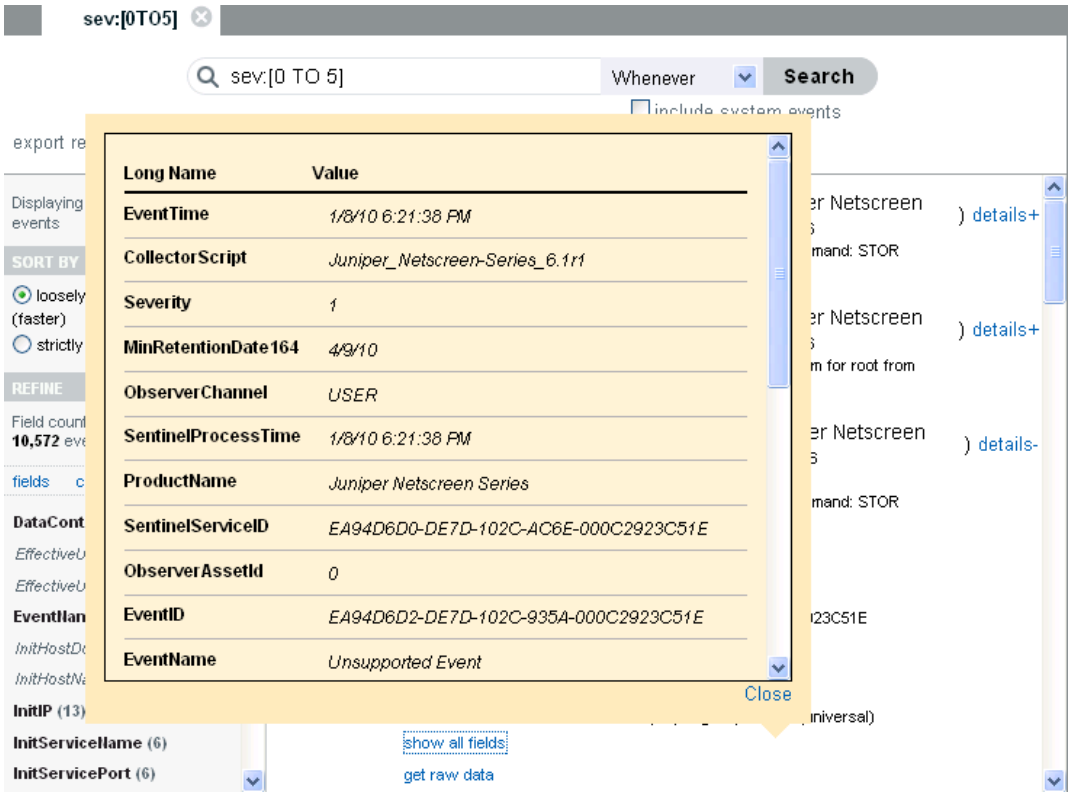
- **Event Source ID:** Displays the name of the Collector Manager. When you click the *Event Source ID* field value, the value is added to the current search and provides information about other events coming from the same Event Source.

If the Collector, Collector Manager, Connector, and EventSource plug-in instances are deleted, then 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.

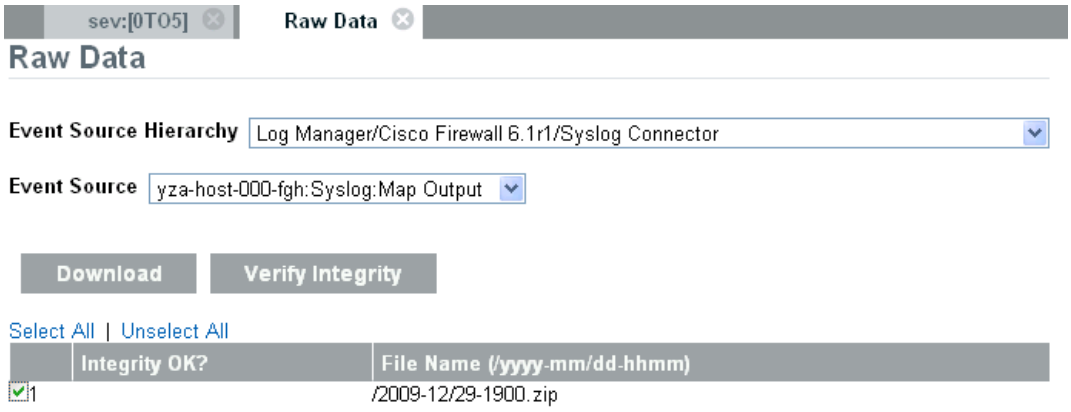
The list shows only the event fields that have values.



5 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.

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 39.



5.4 Exporting Search Results

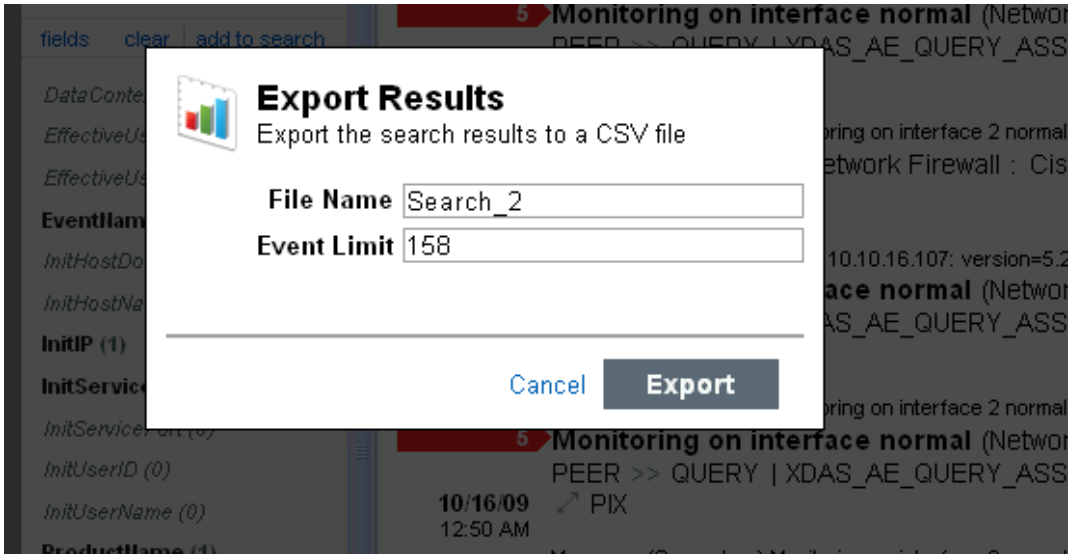
You can use the *Export Results* link to export your search results as a `.zip` file.

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

NOTE: If there are no results for the search, the *Export Results* link does not appear.

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

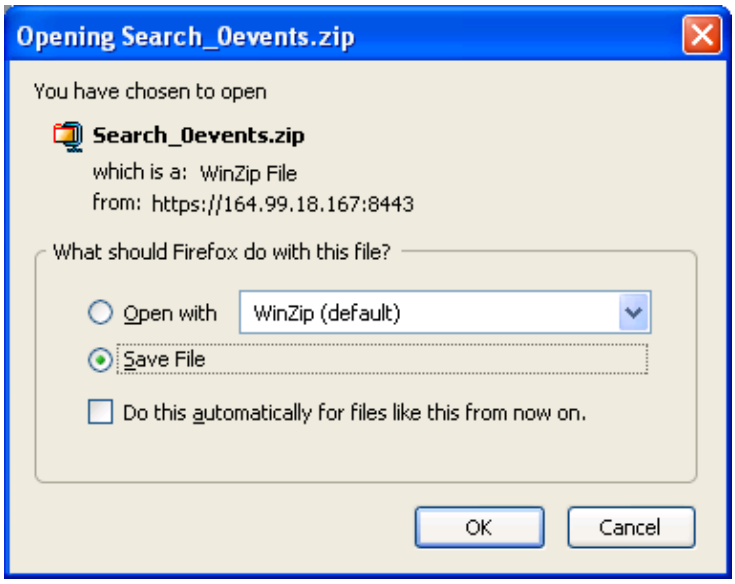
   An Export Results window is displayed.



4. In the *File Name* field, specify the filename to which you want to export the search results.
5. In the *Event Limit* field, specify the event limit 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, which is then zipped and provided for download.
6. Click the *Export* button to display an *Opening Search_xevents.zip* window with the option to save the `Search_xevents.zip` file on your local machine.



The *x* indicates the number of the tab search result.

For example; the first tab search result is named as *Search_0* and the second tab search result is named as *Search_1* and shown in the search result page.

NOTE: 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 events in the Sentinel Log Manager user interface and the exported events.

---

7 Click *OK* to save the `Search_xevents.zip` file.

This zip file contains information about the various fields of the event source.

5.5 Saving a Search Query as a Report Template

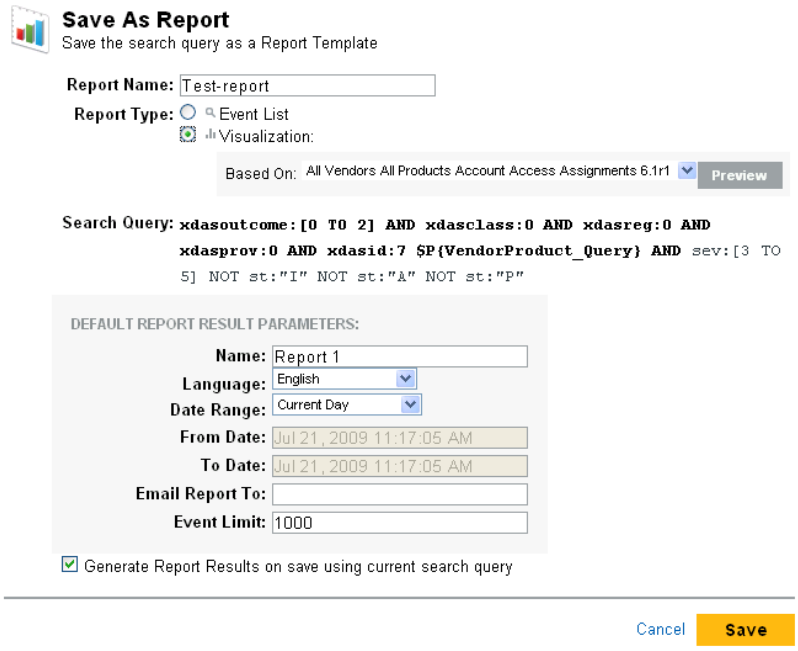
You can save a search result as a report template by using the *Save as Report* link at the top of the search results. You can use this report as a reference to create future reports.

1 Log in to Novell Sentinel Log Manager.

2 Perform a search.

3 To save the search query, click the *save as report* link.

A *Save as Report* dialog box is displayed.



4 Use the *Report Name* field to specify the report template name for the search.

5 Select one of the following report type formats:

- **Event List:** Select the *Event List* option to save the report in the search report format.
- **Visualization:** The *Based on* field lists the Jasper Reports saved in Sentinel Log Manager. Select a Jasper report from the *Based on* drop-down list to save the new report template in the Jasper report format.

6 Specify the data values you want for the report. To specify the Jasper report parameters, see Step 5 on page 93.

The *Search Query* field displays the text for the search.

7 In the *Name* field, specify the name of the report.

8 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.

9 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.

10 To generate report results when you click *Save*, select the *Generate report results on save using current search query* check box.

11 Click *Preview* to see a preview of the selected report.

12 Click *Save* to save the report definition.

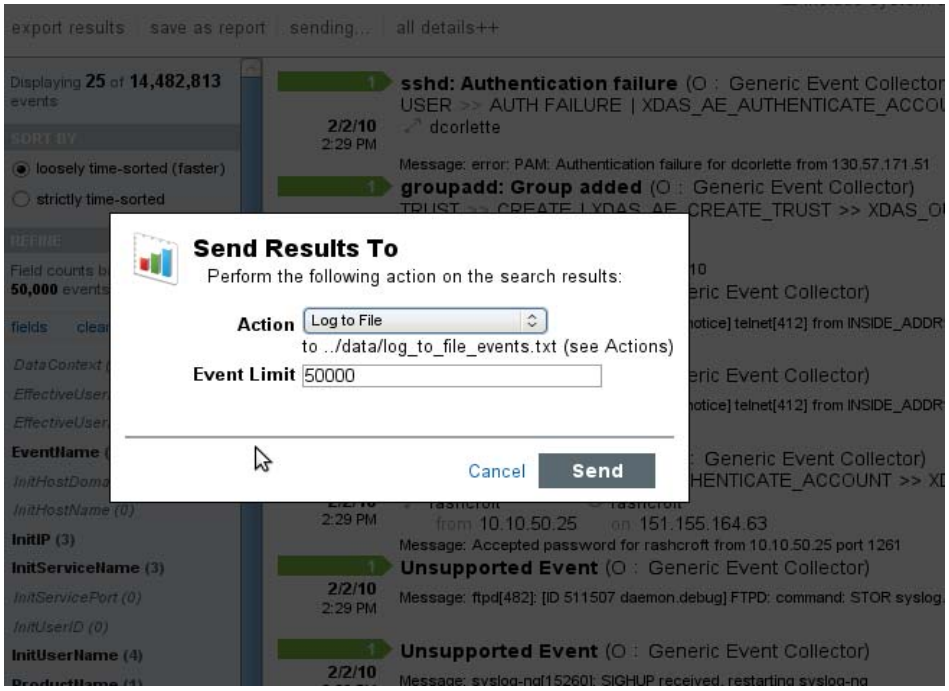
You can see the saved report definition in the Report Viewer pane in the Sentinel Log Manager interface. To view the reports, see "Viewing the Reports" on page 95.

5.6 Sending Search Results to an Action

You can send search results to a selected action in the 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.



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 7.2, “Configuring Actions,” on page 114.
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.

Reporting

6

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

Sentinel Log Manager supports two types of reports: JasperReports and Search reports. The JasperReports appear with a bar graph icon ( ), and Search reports appear with a magnifying glass icon ( ) next to the report definition. You can categorize the reports as All and Favorite reports.

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

6.1 Running Reports

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

The Report Viewer pane of Sentinel Log Manager page displays all the report definitions in the system. Reports run asynchronously, so users can continue to do other things in the application while the report is running.

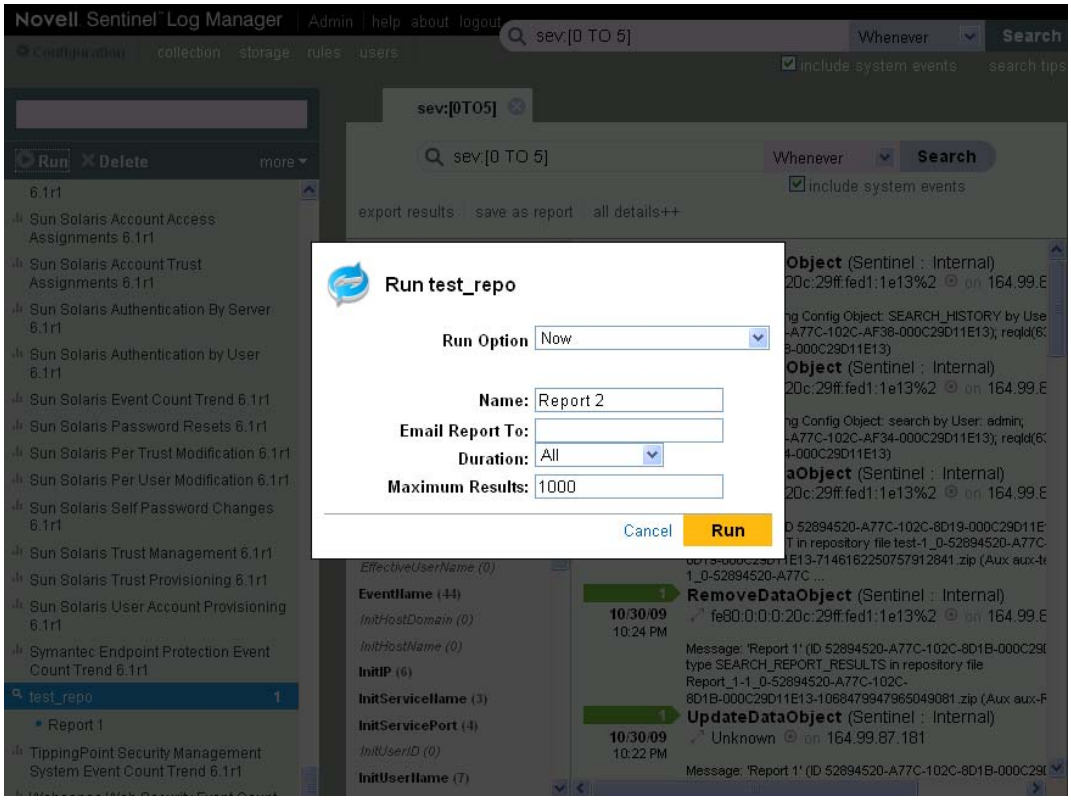
The user can run a report by using the desired parameters (such as a start and an end date), and can save the report results with a desired name. After the report runs, the results can be viewed by clicking on the *View* button located next to the relevant report result list. If the report format chosen is Jasper Report, then the results are displayed as a PDF. If the report format chosen is Search report, then the results are displayed at a new search results tab in the Search Dashboard on the right side of the Sentinel Log Manager user interface.

If the server was restarted while a report was processing, you see buttons to cancel or restart the report. If you restart the report, it uses the same parameters used at 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, not the date and time when the report was initially run.

Use the following procedure to run a report:

1 In the Report Viewer pane, select the report you want to run, and click the *Run* button located on top of the first Report Definition.

When the report definition runs, a Run *Report Name* screen is displayed that allows you to change the parameters to run a report (for example, report name, start date, and end date). The Sentinel Log Manager also allows you to schedule a report to run at regular intervals.



2 Set the run options for running the report.

3 Specify a name to identify the report results.

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

4 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.

Parameter	Description
Durations	If the report includes time period parameters, choose the date range. All time periods are based on the local time for the browser. ◆ **Last 1 hour:** Shows events of the last 1 hour. ◆ **Last 12 hours:** Shows events of the last 12 hours. ◆ **Last 24 hours:** Shows events of the last 24 hours. ◆ **Last 7 days:** Shows last seven days of events. ◆ **Last 30 days:** Shows events of 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 the last 90 days events. ◆ **Whenever:** Shows all events stored in the system. ◆ **Custom Date Range:** If you selected *Custom Date Range*, set the start date (From Date) and the end date (To Date) for the report. If any of the other settings is selected for the report type, these time settings are ignored.

5 To run a JasperReport, specify the following parameters:

Jasper Reports may also have number of additional parameters defined when creating the Jasper Report. To view the description for an additional parameter via a tooltip, hover the mouse over the parameter names on the Run Report form.

Parameter	Description
Help	Click *Help* to open the doc_plugin.pdf and to read the getting started notes for the selected JasperReport.
Maximum Results	Specify the maximum number of event search results to include in the report.
Language	Choose the language in which the report labels and descriptions should be displayed. The values are English, French, German, Italian, Japanese, Traditional Chinese, Simplified Chinese, Spanish, or Portuguese. The default value will be the language with which the current user logged in, provided that language is supported by the report. If the report does not support the language, then the report's default language (typically English) will be used. The data in the report is displayed in the language it was originally used by the event source.

Parameter	Description
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:** 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 last seven days of events. ◆ **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 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:** Shows events of a period whose start and end date are chosen. If any of the other settings is selected for the report type, these time settings are ignored.
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.

6 If the report needs to be mailed to more than one user, enter their e-mail addresses, separated by a comma, in the *Email Report to* field.

To enable mailing reports, configure the mail relay under *Rules* > *Configuration*.

7 Click *Run*.

A report results entry is created and mailed to the chosen recipients.

6.2 Scheduling a Report to Run Automatically

You can run the report immediately or schedule it to be run later, either once or on a recurring basis. For scheduled reports, choose a frequency and enter 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, 2009 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.

6.3 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 on the left pane of the page.

1. Click a report definition to view the report results in the Report Viewer pane.

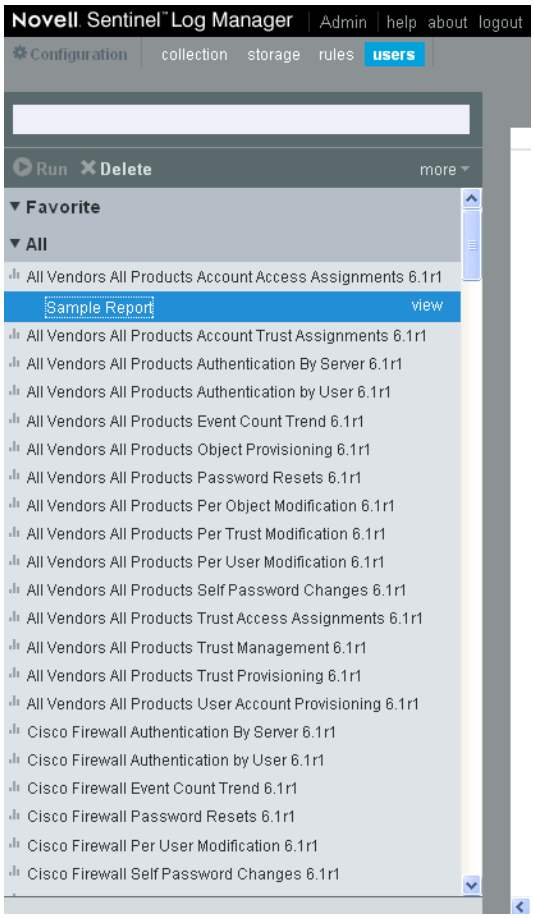
   All the report results are ordered by the creation time. If there are more than one report, the *show more* link displays the other report results.

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

   A report result without a blue dot next to it indicates that the report result has been read. 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 101.

2. Select a report result. The *View* button is displayed next to the report result.

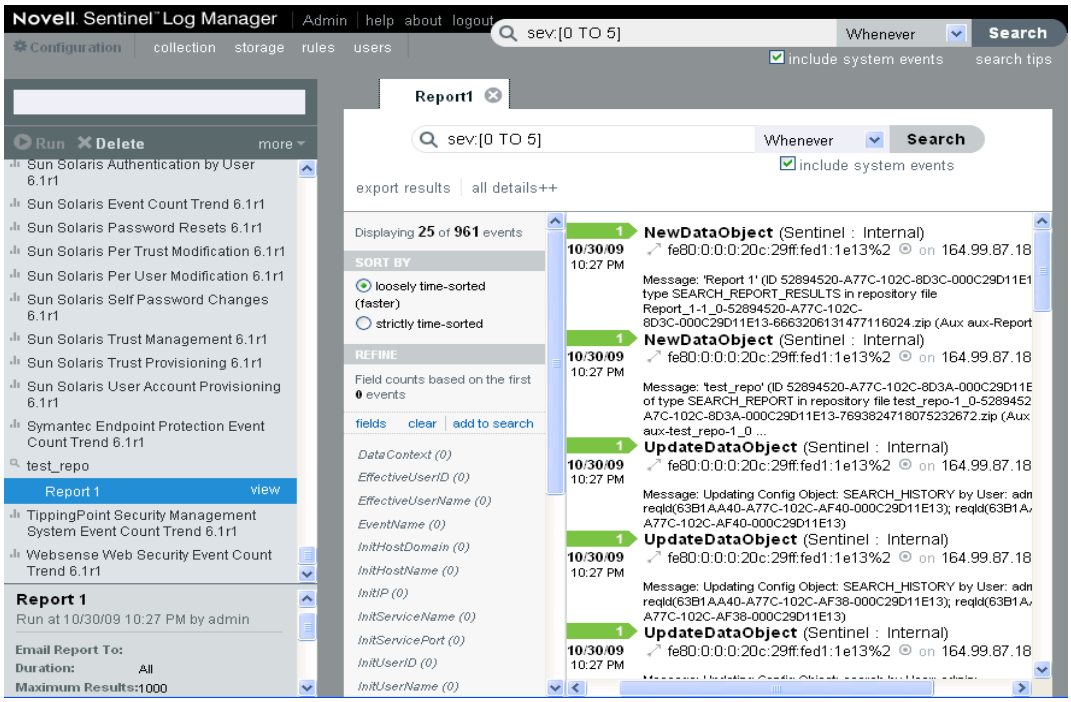


3 Click *View*.

- If the selected report is a Jasper report, clicking the *View* button displays the report in PDF format in a new window.
- If the selected report is a Search report, clicking the *View* button displays the report in the right pane of the Search Dashboard.

You can check 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.



4 Click the *Sample Report* to display a *View* link.

5 Click *View* to find out how the completed report looks with a set of sample data.

Report results are organized from newest to oldest.

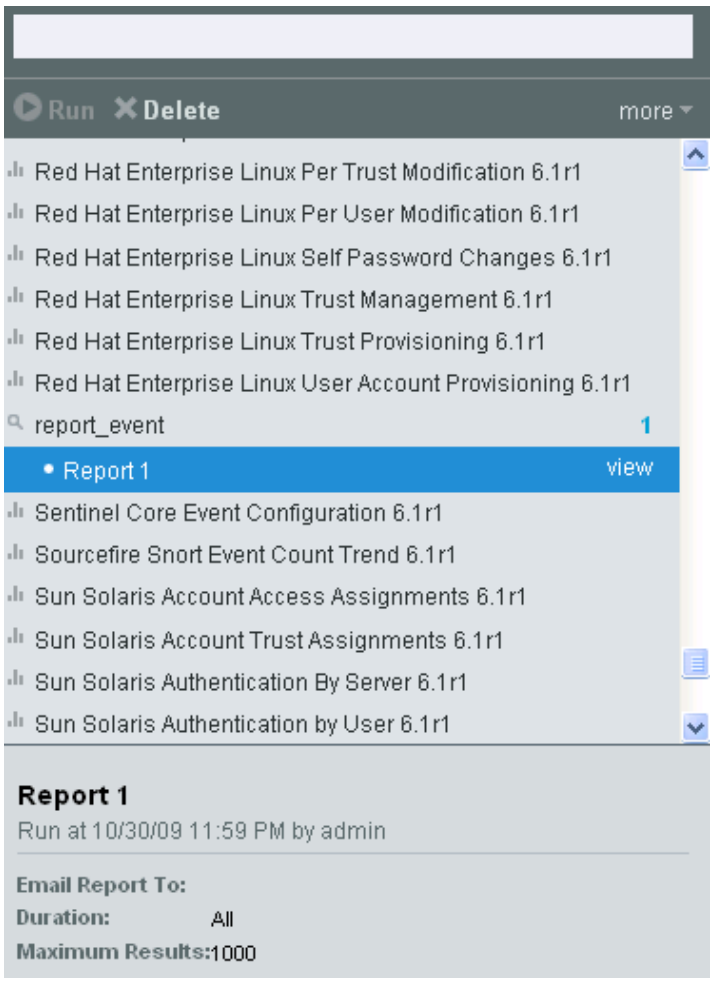
6.4 Viewing Report Parameters

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 Click a report definition to expand it.

2 Select the report to view the parameters associated with the selected report.

The report parameters are displayed in the status pane as shown in the following image.



6.5 Extracting the Reports from the Collector Packs

Collector Pack contains the event source setup instructions, associated scripts, utilities, and the Sentinel Log Manager reports specific to the data of the associated collector.

The Collector Pack Extractor utility allows you to extract the collector pack contents. You can use the instructions and scripts to configure the associated event sources. The reports that are extracted from the new collector can be uploaded to the Sentinel Log Manager.

These collector packs are available on the Sentinel Content Web site (http://support.novell.com/products/sentinel/sentinel61.html).

To extract the reports from the collector packs:

1. Copy all the Collector Packs from which you want to extract the Event Source Setup instructions, associated scripts and utilities, and Sentinel Log Manager reports to a temporary directory.

2 Download the Collector Pack Extractor from the Sentinel Content Web site (http://support.novell.com/products/sentinel/sentinel61.html) that is available under the *Utilities* tab.

3 Copy the `cpextractor.jar` file to the same directory.

4 Execute the jar by using either of the following steps:

- **On Windows:** Double click the jar (if the java environment is properly configured)
- **On Linux:** Run the command `java -jar cpextractor.jar`.

5 For each Collector Pack a new directory is created with the same base name of the collector. The newly created directory contains:

- **jasperreports:** This is a sub directory that contains all the extracted Sentinel Log Manager reports.
- **instructions.txt:** (Optional) This is a text file that contains the required instructions to configure event source.

This directory can also contain additional files that are required for event source configuration.

6 To proceed with event source configuration, follow the instructions provided in Section 4.3.1, "Launching Event Source Management," on page 57.

7 If any additional steps are needed for event source configuration, follow the steps given in the `instructions.txt` file. Otherwise, to add a report, see "Adding the Report Definitions" on page 98.

6.6 Adding the Report Definitions

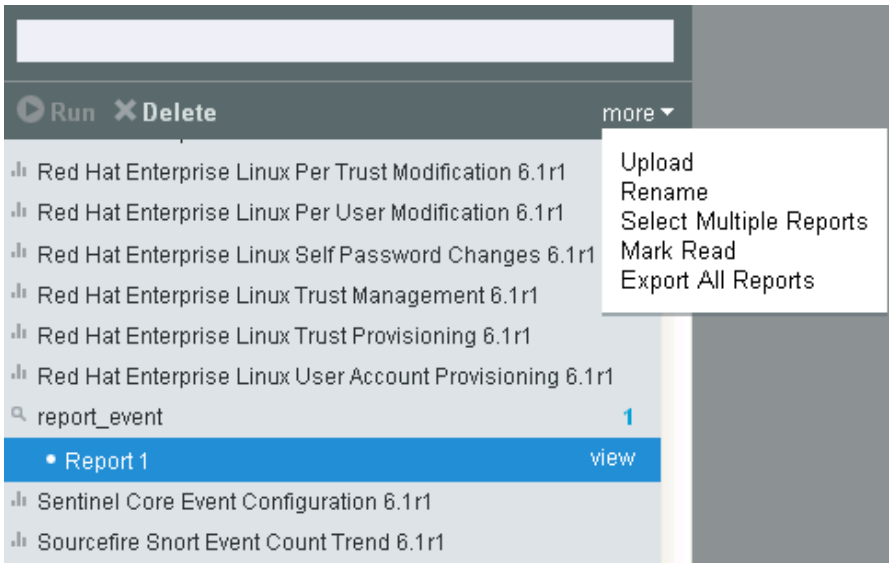
Additional report plug-ins (special `.zip` or `.rpz` files that include the report definition other than the metadata and resources used by the report) can be uploaded into the Sentinel Log Manager. Both JasperReport type plug-ins and Search type plug-ins can also be uploaded.

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/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).

Use the following procedure to add or upload a report:

1 Click the *more* drop-down list in the Report Viewer pane and select *Upload*.



2 Browse and select the report plug-in `.zip` file from your local machine.

3 Click *Open*.

4 Click *Upload*.

5 If the same report already exists in the report repository, decide based on the report's unique ID whether to replace the existing report or not.

   Sentinel Log Manager displays details of both the reports.

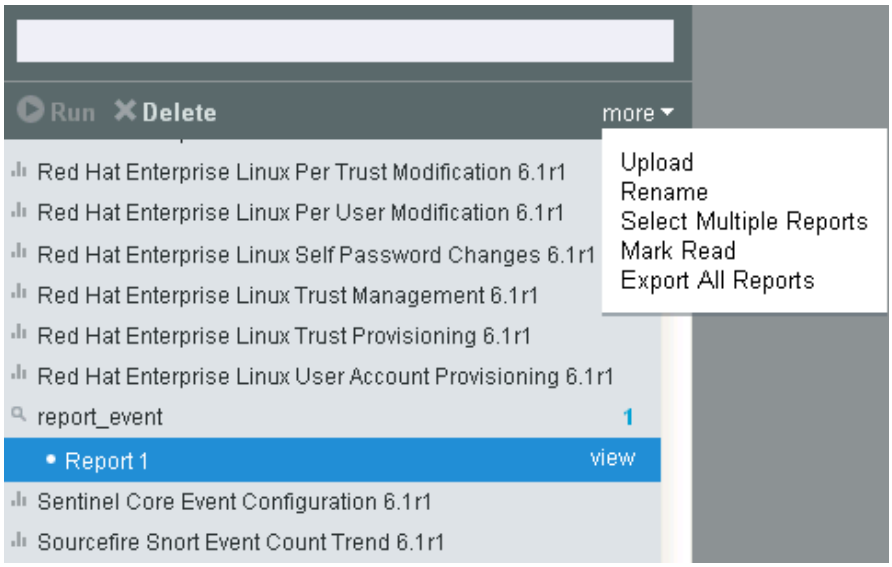
The new report definition is added to Report Template list in alphabetical order and can be run immediately, if required.

6.7 Renaming a Report Result

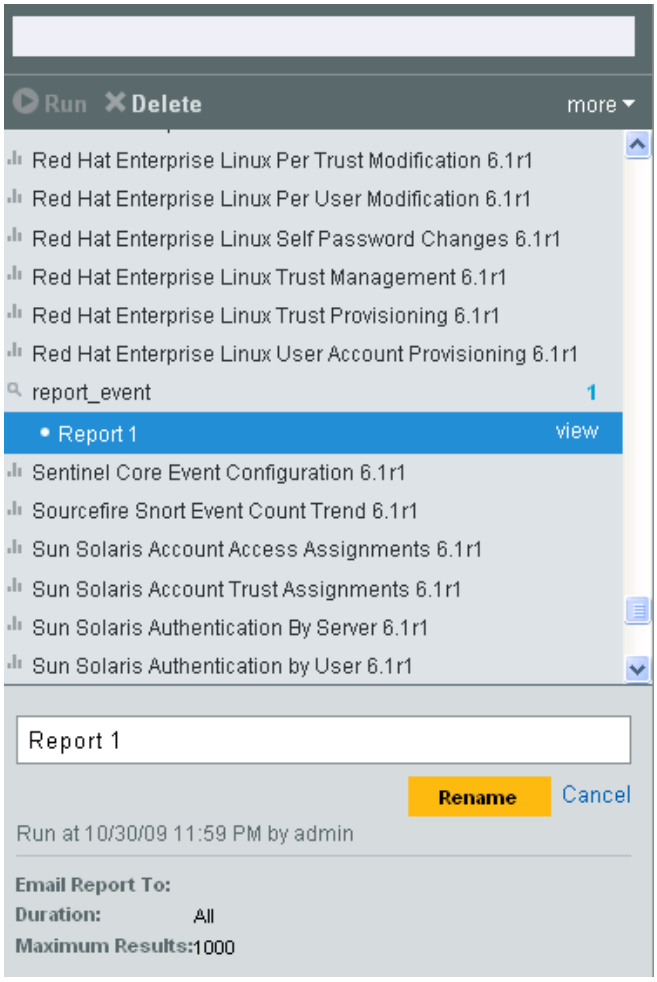
1 Click a report definition to view the report results in the Report Viewer pane.

2 Select a report result.

3 Click the *more* drop-down list in the Report Viewer pane and select *Rename*.



4 Specify a name in the bottom left status pane.



5 Click *Rename*.

The selected report result is renamed under the report definition.

6.8 Marking Report Results as Read or Unread

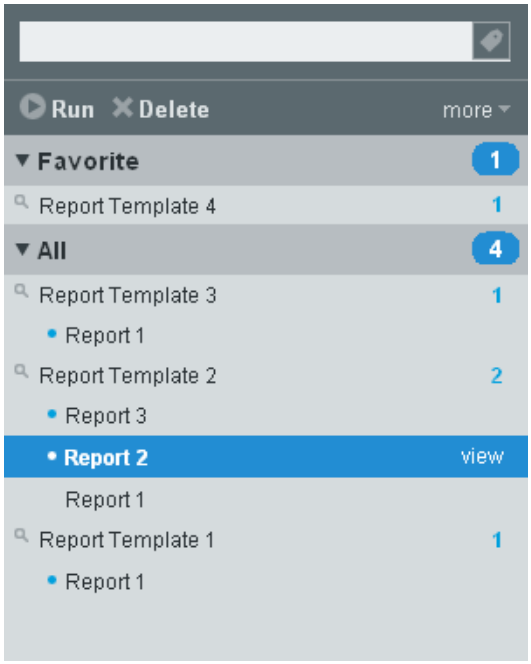
When a report result is created under a report definition, the report result is in unread state. An unread report result appears with a blue dot next to the report result in the Report Viewer. When you view a report result, the blue dot is removed to indicate that the report has been read. You can also manually mark a report result as read or unread without viewing it.

In the Report Viewer, each of the report template or definition 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.

6.8.1 Marking a Single Report Result as Read

1 Select an unread report result (report result with a blue dot next to it) under a report definition in the Report Viewer pane of the page.

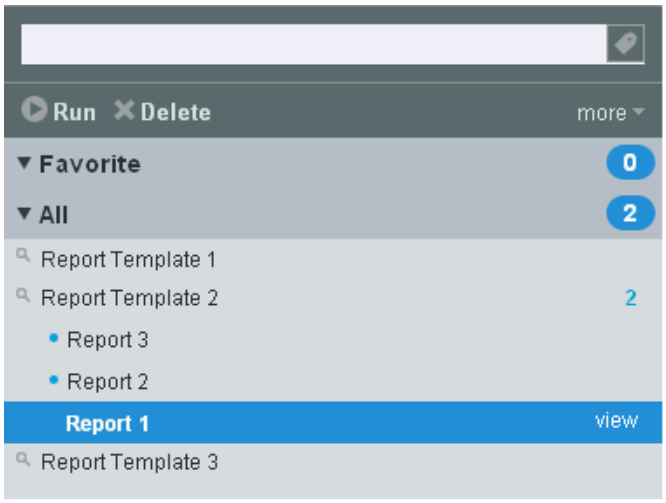


2 Click the *more* drop-down list in the Report Viewer pane and click *Mark Read*.

The report result changes to the read state without a blue dot next to the report result.

6.8.2 Marking Single Report Result as Unread

1 Select a read report result without a blue dot next to it under a report definition in the Report Viewer pane.

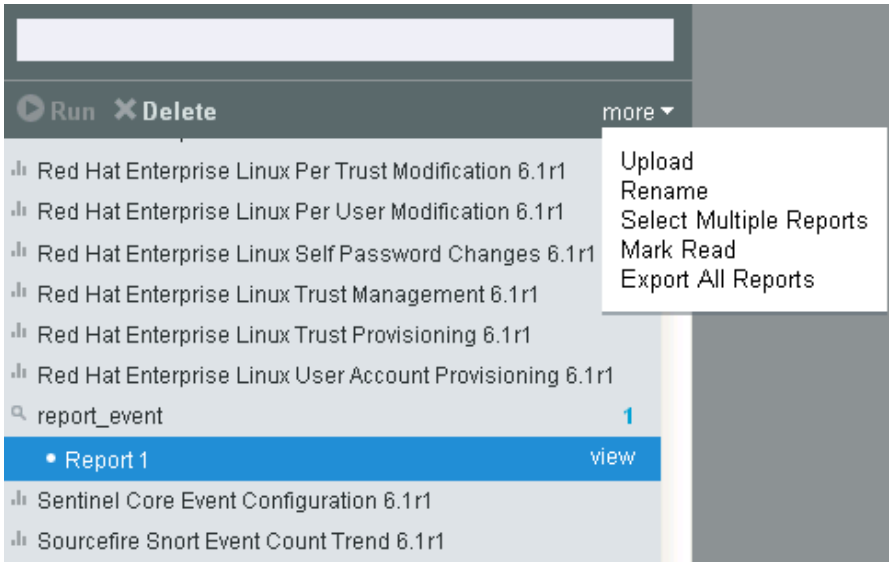


2 Click the *more* drop-down list in the Report Viewer pane and click *Mark Unread*.

The report result changes to the Unread state with a blue dot next to the report result.

6.8.3 Marking Multiple Report Results as Read

1 Click the *more* drop-down list in the Report Viewer pane and click *Select Multiple Reports*.

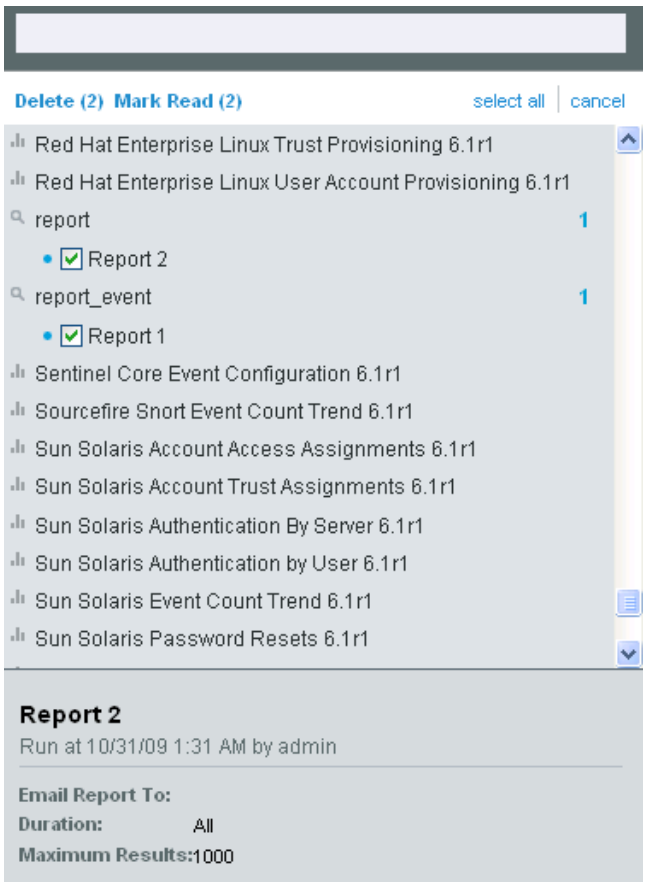


2 A check box is displayed next to each report result in the Report Viewer pane. Click the check boxes to select one or more report results.

You can also use the *select all* link to select all the available report results. To deselect all the selected reports, click the *unselect all* link.

If the report results are not selected, the *Mark Read* link is disabled.

If the selected report results are all Unread or a mixture of Read and Unread report results, the *Mark Read (x)* link is displayed in the Report Viewer pane, where *x* is the number of selected report results.

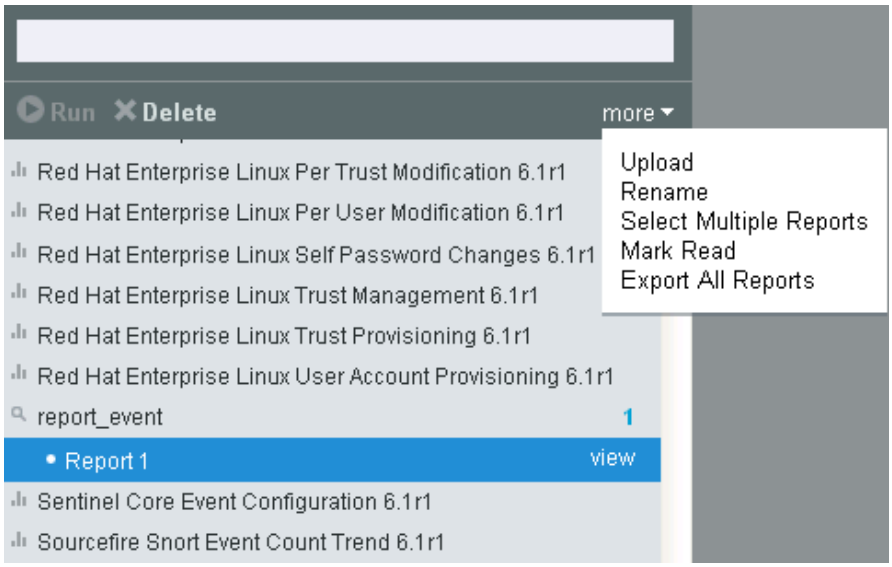


3 Click the *Mark Read (x)* link.

The selected report results change to the Read state without a blue dot next to the report results.

6.8.4 Marking Multiple Report Results as Unread

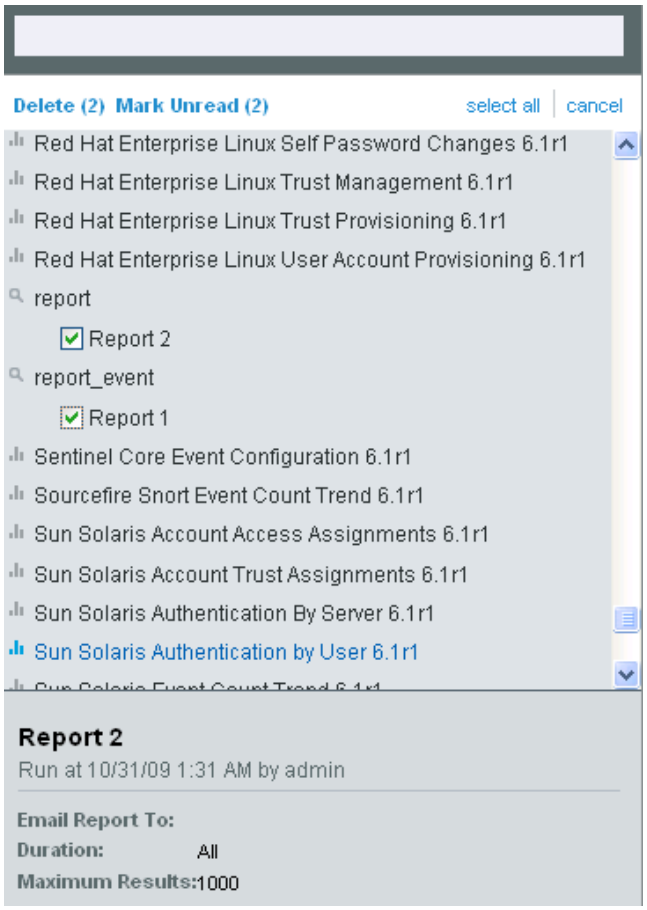
1 Click the *more* drop-down list in the Report Viewer pane and click *Select Multiple Reports*.



2 A check box is displayed next to each report result in the Report Viewer pane. Click the check boxes to select one or more report results.

You can also use the *select all* link to select all the available report results. To deselect all the selected reports, click the *unselect all* link.

If the selected report results are Read, the *Mark Unread (x)* link is displayed in the Report Viewer, where x is the number of selected report results.



3 Click the *Mark Unread (x)* link.

The selected report results changes to unread state with a blue dot next to the report results.

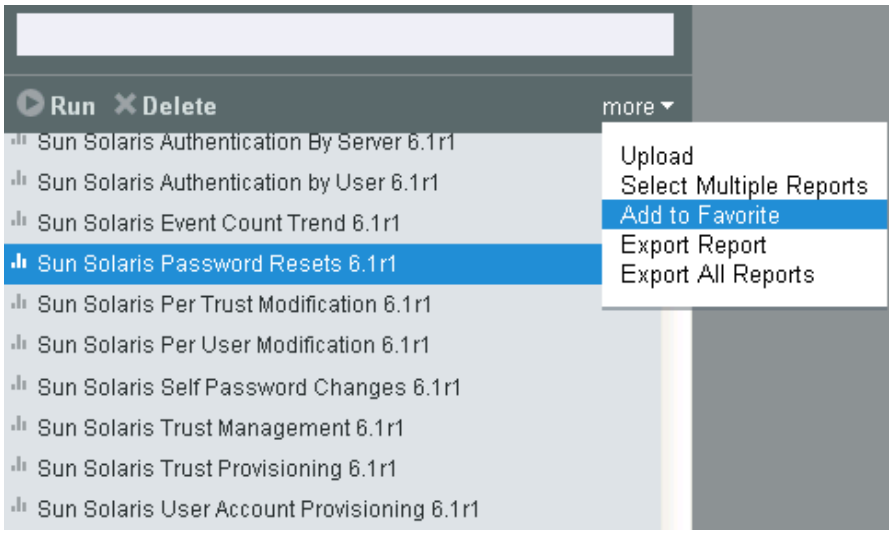
6.9 Managing Favorite Reports

6.9.1 Adding Reports as Favorites

You can mark individual report definitions as Favorite.

1 Select a report definition from the All node.

2 Click the *more* drop-down list in the Report Viewer pane and click *Add to Favorite*.

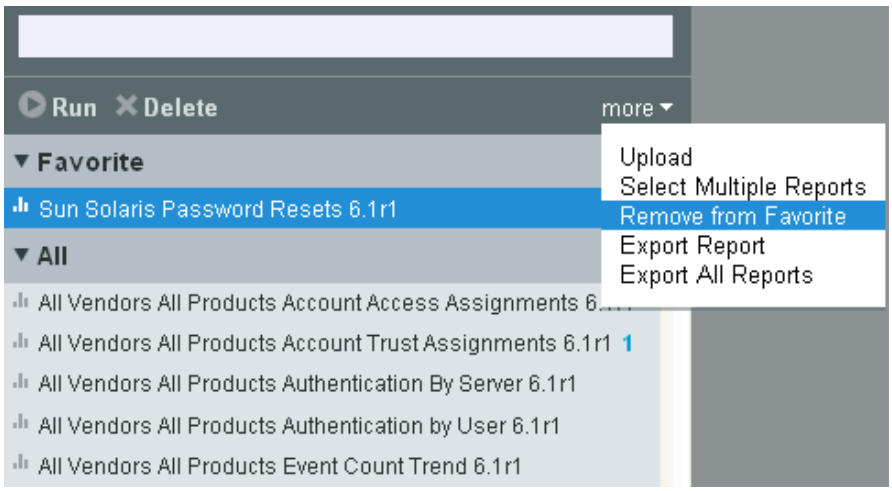


The selected report definition is displayed under the Favorite node in the Reports Viewer pane.

NOTE: The reports marked as favorites are on a per-user basis. Each user can have a different set of favorite reports.

6.9.2 Removing Favorite Reports

1. Select a report definition from the Favorite node.
2. Click the *more* drop-down list in the Report Viewer pane and click *Remove from Favorite*.



3. The selected report definition is removed from the Favorite list and added to the All list in the Report Viewer pane.

6.10 Exporting Report

NOTE: When exporting a report definition or all report definitions, only the report definitions (and their associated resources) are exported. None of the report results are exported.

6.10.1 Exporting a Single report

You can use the *Export Report* option to export the selected report as a `.zip` file. The *Export Report* option is only available when a report definition is selected.

1. Log in to Novell Sentinel Log Manager.
2. Select a report definition from the Report Viewer pane.
3. Click the *more* drop-down list in the Report Viewer pane and select the *Export Report*.

   The report is zipped into a file and provided to you for download.
4. The *Opening <Selected Report Name>.zip* dialog box provides the option to save the `<Selected Report Name>.zip` file on your local machine.

6.10.2 Exporting All Reports

You can use the *Export All Reports* option to export all reports as a `.zip` file.

1. Log in to Novell 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 Reports*.

   All reports are zipped into a file and provided to you for download.
4. The *Opening reportexport.zip* dialog box is displayed with the option to save the `reportexport.zip` file on your local machine.

6.11 Exporting a Report Result

You can export the report result of a report definition.

1. Log in to Novell Sentinel Log Manager.
2. Select a report definition from the Report Viewer pane.

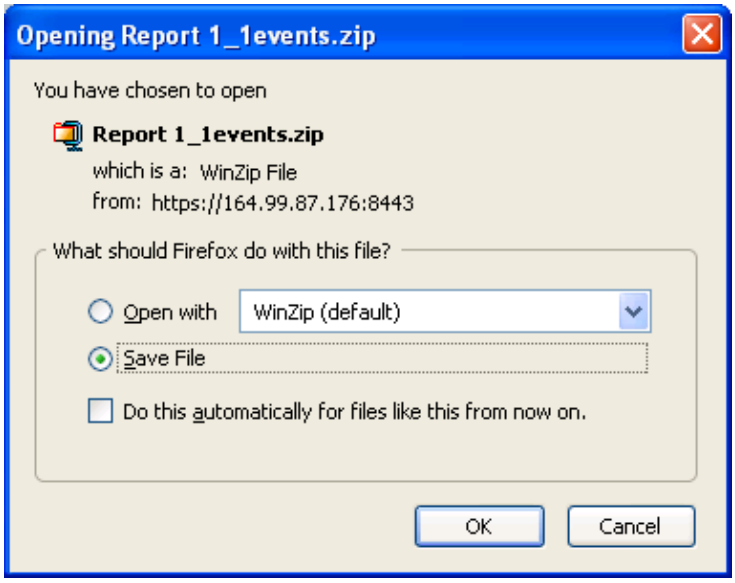
   A list of available report results appear.
3. Select the report result.

   The *View* button is displayed next to the report result.
4. Click the *View* button.

   The report results appear in the right pane of the Search Dashboard.

   The *export results* link is displayed at the top of the report result after you click a report result. You can use this report result as a reference in the future.

5 On clicking on *export results* link, an *Opening <report_result_name>_xevents.zip* window is displayed with the option to save the `<report_result_name>_xevents.zip` file on your local machine.



6 Click *OK* to save the `<report_result_name>_xevents.zip` file.

This zip file has the report result of the event source.

6.12 Deleting Reports

You can delete either a report definition or a report result. If a report definition is deleted, all associated report results are also deleted.

- Section 6.12.1, “Deleting a Report Definition,” on page 108
- Section 6.12.2, “Deleting a Report Result,” on page 109
- Section 6.12.3, “Deleting Multiple Report Results,” on page 109

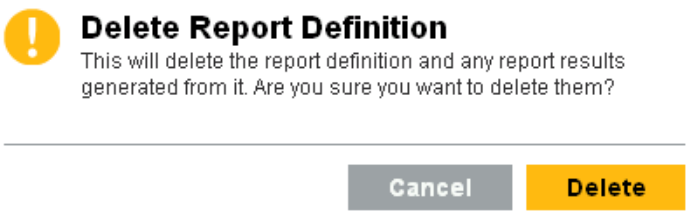
6.12.1 Deleting a Report Definition

1 Log in to Novell Sentinel Log Manager.

2 Select a report definition from the Report Viewer pane.

3 Click the *Delete* button in the Report Viewer pane.

4 The following confirmation message is displayed.



5 Click *Delete* to delete the selected report definition.

The selected report definition is deleted from the Report Viewer pane.

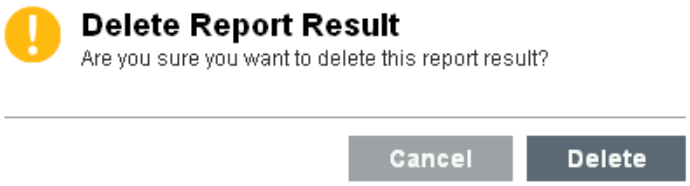
6.12.2 Deleting a Report Result

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.

4 The following confirmation message is displayed.



5 Click *Delete* to delete the selected report result.

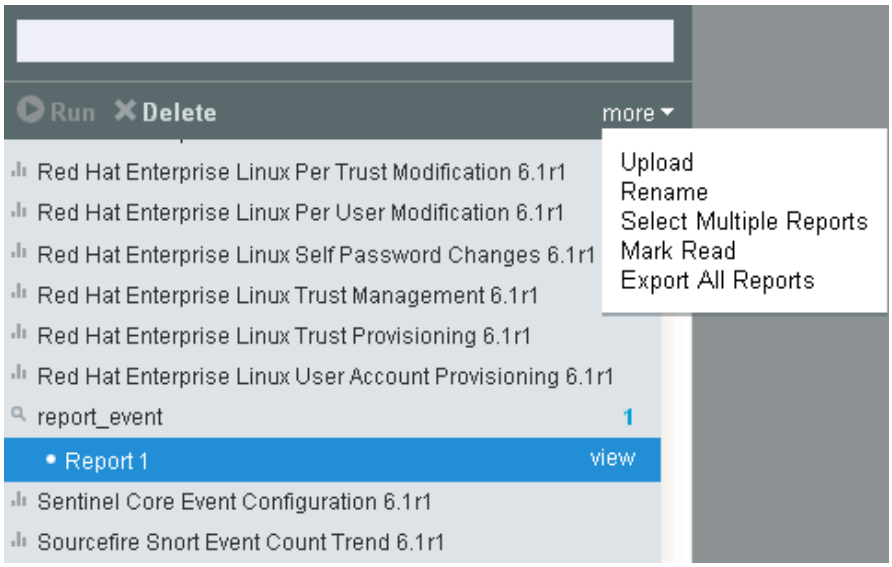
The selected report result under the report definition is deleted from the Report Viewer pane.

6.12.3 Deleting Multiple Report Results

You can select multiple report results and delete all of them.

1 Log in to Novell Sentinel Log Manager.

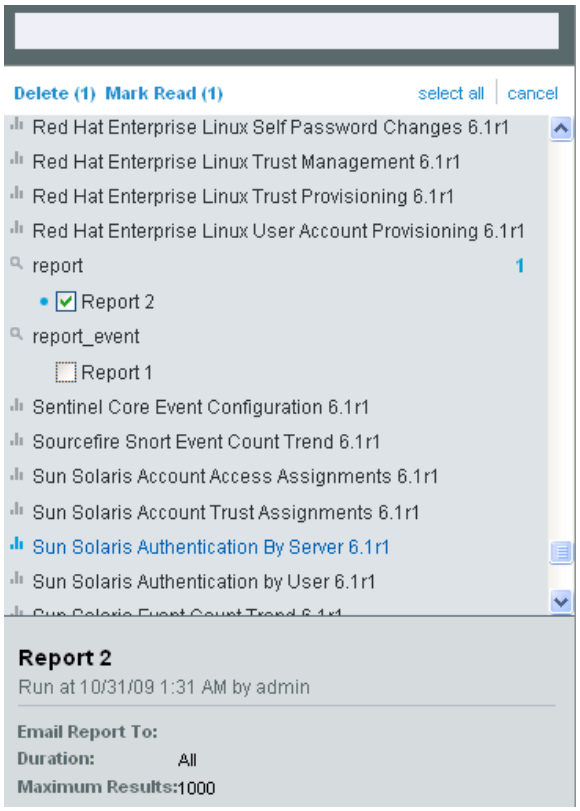
2 Click the *more* drop-down list in the Report Viewer pane and select *Select Multiple Reports*.



3 A check box is displayed next to each report result in the Report Viewer pane. Click the check boxes to select the report results.

You can also use the *select all* link to select all the available report results. To deselect all the selected reports, click the *unselect all* link.

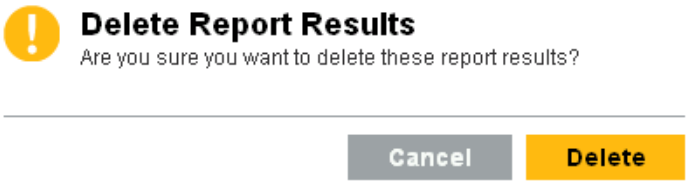
If the report results are not selected, the *Delete* and *Mark Read* links are disabled.



4 The *Delete(x)* in the Report Viewer pane shows the number of selected report results, where *(x)* is the number of selected report results.

5 Click *Delete(x)*.

6 The following confirmation message is displayed.



7 Click *Delete*.

The selected report results are deleted from the Report Viewer pane.

Configuring Rules

7

You can configure rules to evaluate and filter all incoming events and deliver selected events to designated output channels. For example, each severity 5 event can be e-mailed to a security analyst distribution list or to an administrator.

This section describes the event channels and rules that can be used to send events from Novell® Sentinel™ Log Manager to another system.

7.1 Configuring Rules

Sentinel Log Manager rules can be configured 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.

7.1.1 Filter Criteria

Rules can be based on any searchable event field. 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.

7.1.2 Adding a Rule

You can add a filter-based rule and then define one or more channels where you want to output the events that meet the rule criteria.

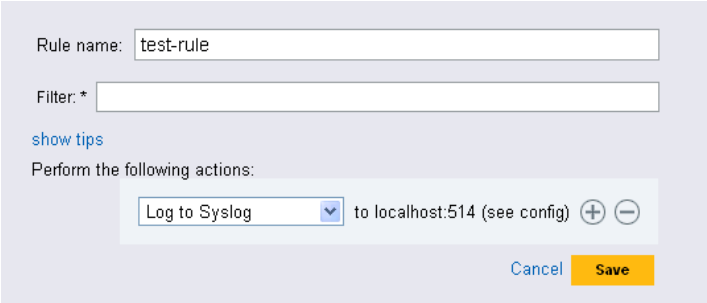
1. Log in to the Sentinel Log Manager as an administrator.
2. Click *rules* in the upper left corner of the page.

   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.

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 114.

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 under the *Rules* tab.

7.1.3 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.

7.1.4 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.

The created 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.

7.1.5 Deleting a Rule

1 Log in to the Sentinel Log Manager as an administrator.

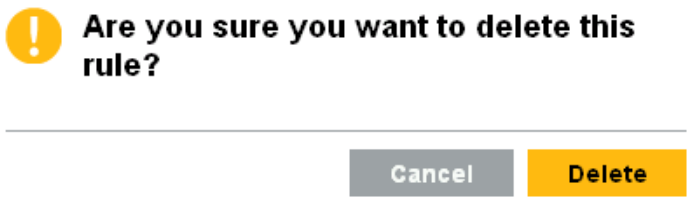
2 Click *rules* in the upper left corner of the page.

3 The *Rules* tab is displayed on the right pane of the page.

The created rule appears 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.

7.1.6 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.

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 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.

7.2 Configuring Actions

An event is delivered to one or more channels 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. Before the events can be output to a channel, an action to send the events to that channel should be configured.

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).

There may be many actions, but each action will be one of the following six action types:

Execute a Script: This type of action executes a specified script on a Sentinel Log Manager server by passing events to it as argument.

Log to File: This type of action writes the event to a specified file on a Sentinel Log Manager server.

Log to Syslog: This type of action forwards the event to a configured syslog server.

Send an Email: This type of 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 type of action sends the SNMP traps.

Send to Sentinel Link: This type of action uses Sentinel Link to forward events to another Sentinel Log Manager, Sentinel, or Sentinel RD system.

For more information on how to configure these actions, see “Adding Actions” on page 115.

NOTE: Events are processed by the associated actions one at a time. You should therefore consider performance implications when selecting the output channel to which events are sent. For example, the Write 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), 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"}
```

The following sections describe how you can add, edit, and delete the actions:

- Section 7.2.1, “Adding Actions,” on page 115

- Section 7.2.2, “Editing an Action,” on page 123
- Section 7.2.3, “Deleting an Action,” on page 124

7.2.1 Adding Actions

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.

This section describes how you can add actions of the following action types:

- “Executing a Script” on page 115
- “Writing the Events to a File” on page 116
- “Sending the Events to Syslog” on page 116
- “Sending the Events by an E-Mail” on page 117
- “Sending the SNMP Traps” on page 118
- “Sending the Events to a Sentinel Link” on page 119

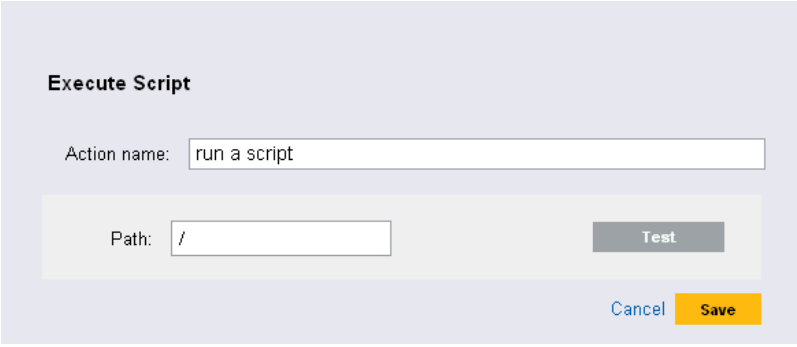
Executing a Script

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. 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. Click the *Add Action* link on the right side of the screen.
6. Select the Execute a Script action type.

   The *Execute Script* screen appears.



7. Specify an action name. The action name should be unique.
8. 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 application’s home directory.

If required, click *Test* to test if script exists and novell user has the required permissions.

9 Click *Save*. If the action is configured, a `Successfully Added Action` message is displayed.

The newly created action appears under the *Actions* tab.

Writing the Events to a File

All Sentinel Log Manager events that meet the filter criteria for which the Write to File action is defined are written to the specified file.

To configure the Write to File action, you need the name and path of the file onto which the events will 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 Click *rules* in the upper left corner of the page.

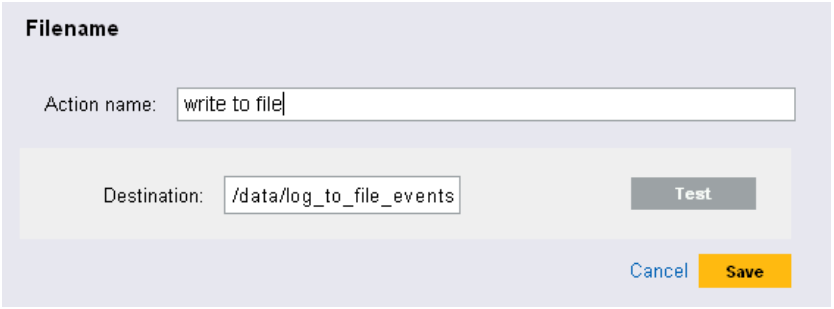
3 The *Rules* tab is displayed on the right pane of the page.

4 Select the *Actions* tab.

5 Click the *Add Action* link on the right side of the screen.

6 Select the Log to File action type.

The *Filename* screen appears.



7 Specify an action name. The action name should be unique.

8 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 application's home directory.

If required, click *Test* to test permissions and create a zero-byte file to hold the data.

9 Click *Save*. If the action is configured, a `Successfully Added Action` message is displayed.

The newly created action appears under the *Actions* tab.

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 Click *rules* in the upper left corner of the page.

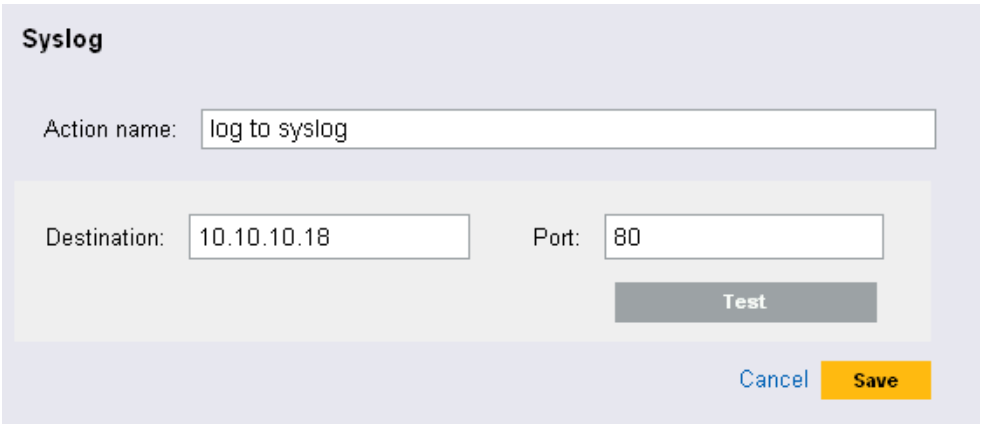
3 The *Rules* tab is displayed on the right pane of the page.

4 Select the *Actions* tab.

5 Click the *Add Action* link on the right side of the screen.

6 Select the Log to Syslog action type.

The *Syslog* screen appears.



7 Specify an action name. The action name should be unique.

8 Specify a name or IP address and the open UDP port of a syslog server.

If required, click *Test* to test if the destination server and port are specified correctly.

9 Click *Save*. If the action is configured, a `Successfully Added Action` message is displayed.

The newly created action appears under the *Actions* tab.

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 Click *rules* in the upper left corner of the page.

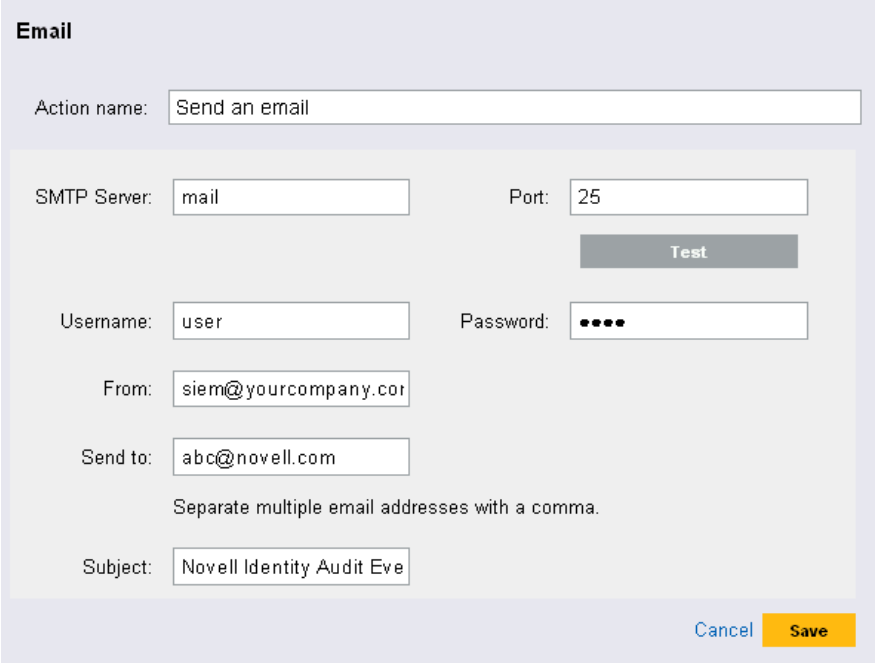
3 The *Rules* tab is displayed on the right pane of the page.

4 Select the *Actions* tab.

5 Click the *Add Action* link on the right side of the screen.

6 Select the Send an Email action type.

The *Email* screen appears.



7 Specify an action name. The action name should be unique.

8 Specify the hostname or IP address of an available SMTP server.

9 Specify the port number of an available SMTP server.

10 If the SMTP server requires authentication, specify a username and password.

If required, click *Test* to validate the hostname or IP address, port, username, and password fields.

11 Specify an address from where the e-mail messages are sent.

12 Specify one or more e-mail addresses for recipients, separated by commas.

13 Specify the subject line for the e-mail.

14 Click *Save*. If the action is configured, a `Successfully Added Action` message is displayed.

The newly created action appears under the *Actions* tab.

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 Click *rules* in the upper left corner of the page.

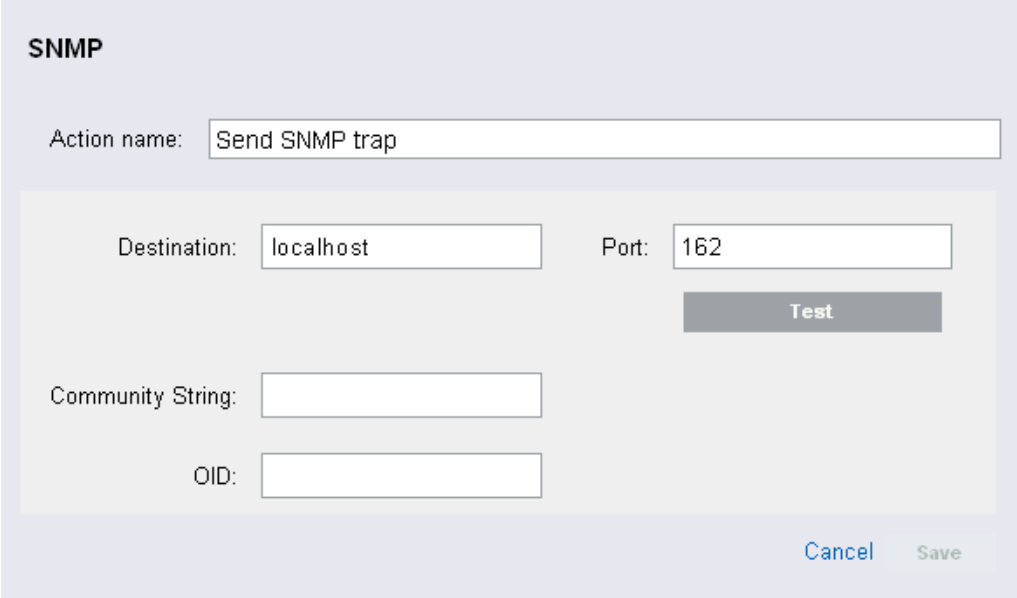
3 The *Rules* tab is displayed on the right pane of the page.

4 Select the *Actions* tab.

5 Click the *Add Action* link on the right side of the screen.

6 Select the Send SNMP Trap action type.

The *SNMP* screen appears.



7 Specify an action name. The action name should be unique.

8 Specify the IP address or hostname of the SNMP server you want to send the trap.

9 Specify the port number for the SNMP server. The default port is 162.

If required, click *Test* to validate the hostname or IP address and port number.

10 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.

11 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).

12 Click *Save*. If the action is configured, a `Successfully Added Action` message is displayed.

The newly created action appears under the *Actions* tab.

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.

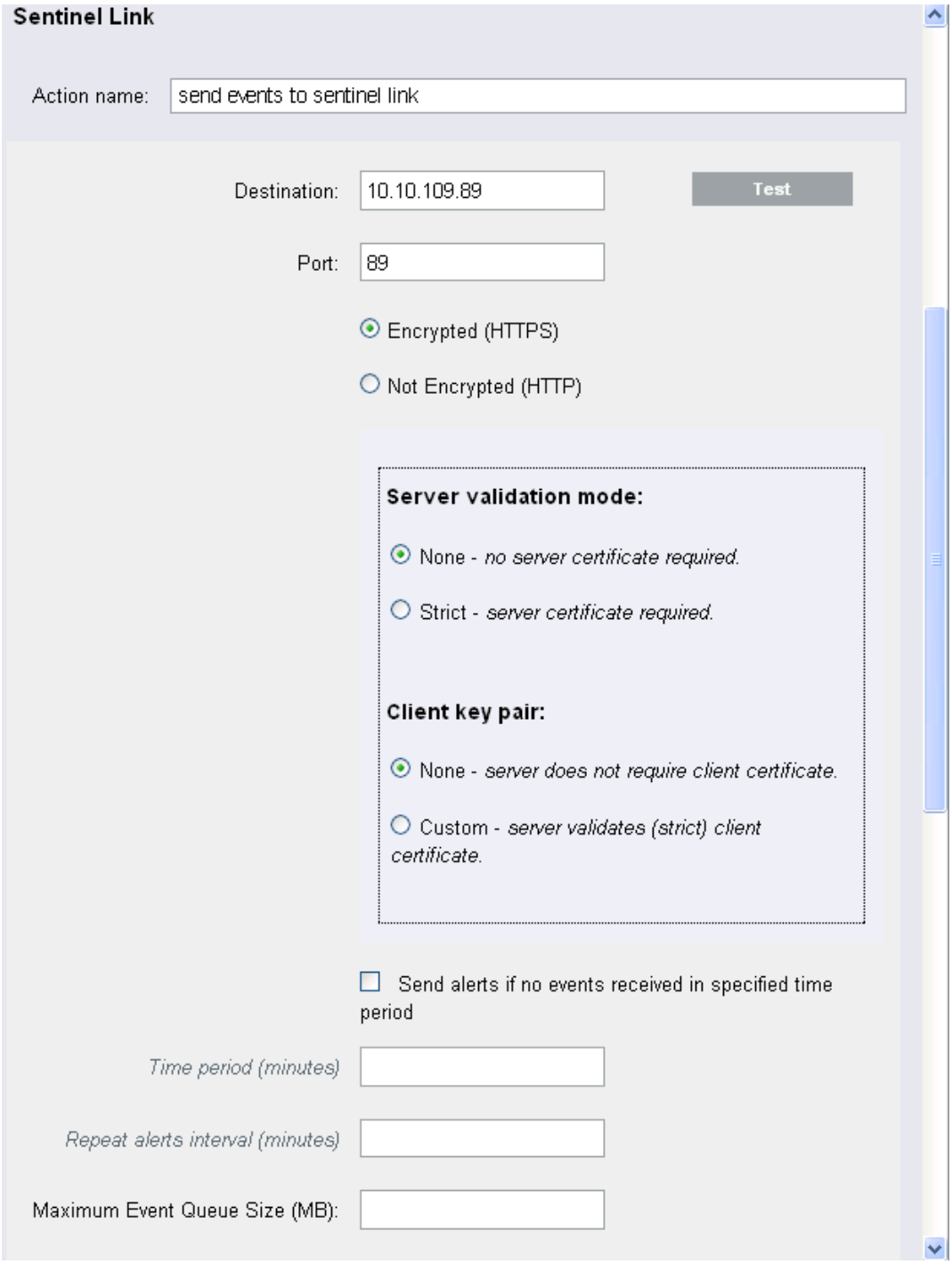
- One or more Sentinel Log Managers can forward important data to either Sentinel or Sentinel RD, which are SIEM (Security Information Event Management) systems. These systems provide real-time visualization of data, advanced correlation and actions, workflow management, and integration with identity 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).
2. Log in to the Sentinel Log Manager as an administrator.
3. Click *rules* in the upper left corner of the page.
4. The *Rules* tab is displayed on the right pane of the page.
5. Select the *Actions* tab.
6. Click the *Add Action* link on the right side of the screen.
7. Select the Send to Sentinel Link action type.

   The *Sentinel Link* screen appears.



8 Specify an action name. The action name should be unique.

9 Specify the IP address or hostname of the destination Sentinel system where a Sentinel Link connector is configured.

10 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.

11 Select either 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
Server Validation Mode	Select either of the following: ◆ **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.
Integrator Key Pair	Select either of the following: ◆ **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 *Open*. ◆ **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 *Strict*. 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 *Import Key Pair* 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.

12 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.

13 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.

14 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`.

15 Specify the maximum data rate value in kilobytes per second. The value must be between 0 and 2147483647.

16 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.

17 Click *Save*. If the action is configured, a `Successfully Added Action` message is displayed.

The newly created action appears under the *Actions* tab.

7.2.2 Editing an Action

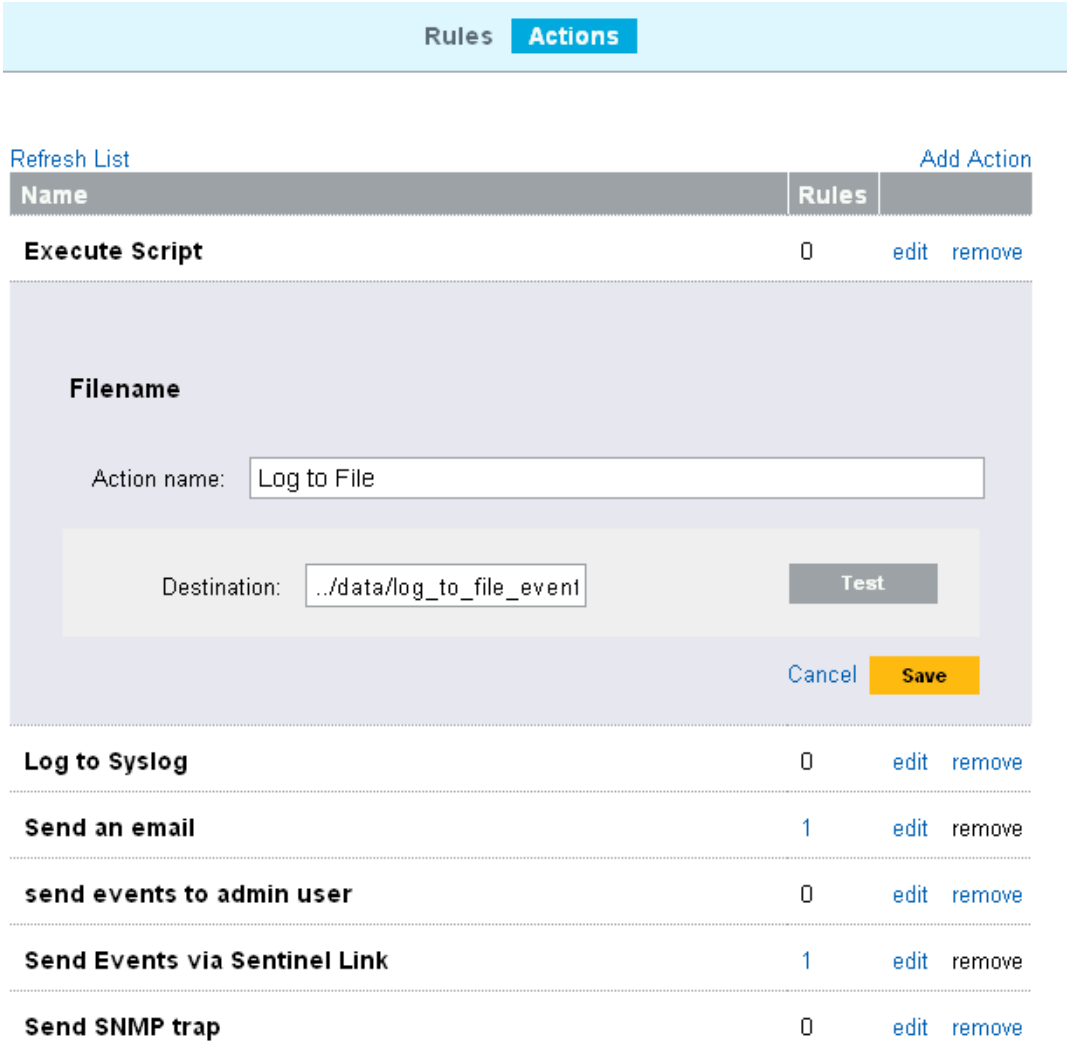
1 Log in to the Sentinel Log Manager as an administrator.

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 change the action settings, click the *edit* link next to the action.



6 Edit the parameter values for the action.

7 Click *Save* to save the settings.

If the action settings are changed, a `Successfully Saved Action` message is displayed.

7.2.3 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.

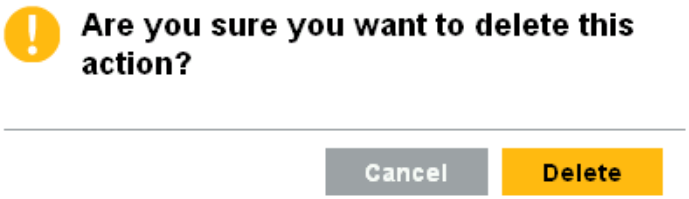
3 The *Rules* tab is displayed on the right pane of the page.

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.

7.3 Configuring E-Mail Notification of 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. It 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 e-mail address that is configured for the Send an email action.

- Section 7.3.1, “Activating the Event Source Created with Unspecified Timezone Rule,” on page 125
- Section 7.3.2, “Configuring Settings for Sending E-Mail,” on page 126

7.3.1 Activating the Event Source Created with Unspecified Timezone Rule

By default, the Event Source Created With Unspecified Timezone rule is installed with Sentinel Log Manager, but it is in the inactive (off) state. To send an e-mail, the rule must be activated, and the e-mail notification settings for the Send an email action must be configured.

Use the following procedure to activate the rule:

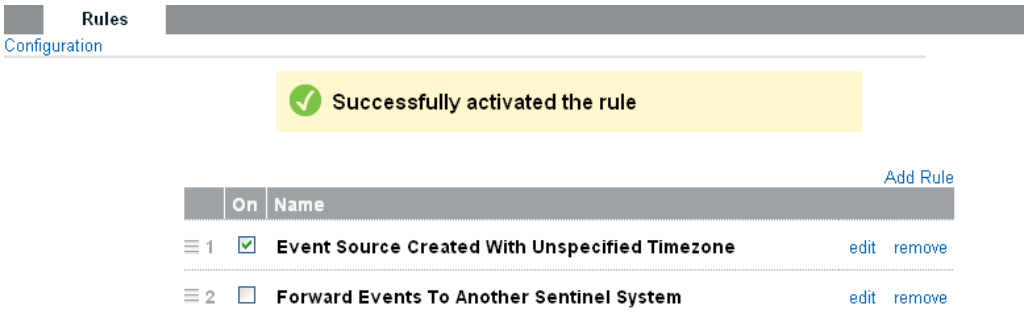
1 Log in to the Sentinel Log Manager as an administrator.

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 Event Source Created With Unspecified Timezone rule is displayed under the *Rules* tab.

4 To activate the Event Source Created With Unspecified Timezone rule, click the check box next to the rule.



If the rule is activated a `Successfully activated the rule` message is displayed.

7.3.2 Configuring Settings for Sending E-Mail

In addition to activating the Event Source Created With Unspecified Timezone rule, you should also configure the settings to receive the e-mail notifications for event sources that are auto-created without a time zone.

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 Click the *Add Action* link on the right side of the screen.

6 Select the Send an Email action type.

The *Email* screen appears.

7 Use the following table to specify the field values:

Fields	Description
Action name	Specify an action name. The action name should be unique.
SMTP Server	Specify the hostname or IP address of the SMTP server.
Port	Specify the port of the SMTP server. The default port value is 25. **NOTE:** Do not change the port value unless your SMTP server uses a different port.
Test	Click *Test* to validate the SMTP server and port.
Username	Specify a username to log in to the SMTP server.
Password	Specify a password to log in to the SMTP server.
From	Specify an e-mail address that the e-mail messages comes from.
Send To	Specify an e-mail address to receive the e-mail notifications for event sources that are auto-created without a time zone. **NOTE:** Specify multiple e-mail addresses by separating them with commas.

8 Click *Save*.

7.4 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.

- Section 7.4.1, “Activating the Forward Events To Another Sentinel System Rule,” on page 128
- Section 7.4.2, “Configuring Sentinel Link Integrator Settings,” on page 128

7.4.1 Activating the Forward Events To Another Sentinel System Rule

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.

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, click the check box next to the rule.

   If the rule is activated, a `Successfully activated the rule` message is displayed.

7.4.2 Configuring Sentinel Link Integrator Settings

In addition to activating the Forward Events To Another Sentinel System rule, you must also configure the Sentinel Link Integrator settings.

Configuring the Send to Sentinel Link settings is same as configuring the Sentinel Link Integrator settings. The Send to Sentinel Link settings configures the Sentinel Link Integrator instance that is pre-installed on Sentinel Log Manager.

To configure the Send to Sentinel Link settings, refer to “Sending the Events to a Sentinel Link” on page 119.

User Administration

8

This section describes the user administration feature of Novell® Sentinel™ Log Manager. You can add, edit, delete, and grant different user level permissions. You can edit the details of your own user profiles.

8.1 Adding a User

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 a user*.
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.
5. Specify one of the following options to give more granular permissions for the user to control the Sentinel Log Manager system.

   Only an administrator can provide these permissions to a user.

   Administrator: Selecting this option gives administrative rights to the user in the Sentinel Log Manager system. Administrator rights include the ability to perform the following functions:

   - User administration
   - Data collection
   - Data storage
   - Rules management
   - Report management
   - Search operations
   - License management

   Report Administrator: Selecting this option allows the user to have administrative rights for reports, which also includes the Auditor rights. Report administrator rights include the ability to perform the following functions:

   - Search reports
   - Run reports

- View reports
- Add and delete Report Templates and Report results
- Export all reports
- Export results
- Save as report

NOTE: A user who has Report Administrator rights cannot access the *collections*, *storage*, *rules*, and *users* configuration links.

Auditor: Selecting this option gives the auditor rights to the users in Sentinel Log Manager system. Auditor rights include the ability to perform the following functions:

- Search reports
- Run reports
- View reports
- Delete report results
- Rename report results
- Select multiple reports

NOTE: A user who has Auditor rights cannot delete report templates, cannot access the *Export All Reports*, *export results*, and *save as report* links, and cannot access the *collections*, *storage*, *rules*, and *users* configuration links.

---

6 The following options appear only when the Auditor option is selected:

View reports created by all users: Select this option to allow access to all the reports available on the Sentinel Log Manager server.

Enable Sentinel Log Manager configuration reporting: Select this option to run the reports if you are using SQL queries in the report definition.

7 Select the authentication type.

Local: By default, the *Local* option is selected.

Directory: The *Directory* option is enabled only if the user has configured LDAP authentication. For more information about configuring LDAP authentication, see "Configuring Sentinel Log Manager Server for LDAP Authentication" on page 132.

If you select *Directory* option, specify the same username as the eDirectory username or Active Directory sAMAccountName in the *Username* field. The user's password is authenticated with the LDAP credentials.

8 Specify a filter value in the *Security Filter* field to filter the events that a user can view.

To allow a user to view all the events select the *Allow all events* radio button.

To set a filter, click the *Tips* link to use the tag names defined in the table.

For example, if you set the filter value to `sev:5`, the user can view only events of severity five for a search.

For more information on each of these event fields, see Appendix C, "Event Fields," on page 149.

9 Specify a user name in the *Username* field.

If this is a directory user, the name must match the eDirectory user name (if the directory is eDir) or the sAMAccountName (if the directory is Active Directory).

10 Specify a password in the *Password* field.

11 Re-enter the password in the *Verify* field.

12 The *Title*, *Office #*, *Mobile #*, *Fax #*, and *Ext.* 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.

13 Click *Save*.

The created user appears under the *Users* tab.

8.2 Editing the 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.

8.2.1 Editing Your Own Profile

To edit a profile:

1 Click the logged in user name in the upper left corner of the page.

2 The *Users* tab is displayed on the right pane of the page.

3 Click *Edit* link under the *Users* tab, to edit the user profile.

4 Click *Save*.

8.2.2 Changing Your Own Password

You can change your own password, if you know the current password. Otherwise, an administrator can reset the password.

To change the password:

1 Click the logged in user name in the upper left corner of the page.

2 The *Users* tab is displayed on the right pane of the page.

3 Click *Edit* link under the *Users* tab.

4 Specify your current password.

5 Specify your new password.

6 Confirm your new password.

7 Click *Save*.

8.2.3 Editing 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.
3. Click *Edit* under the user you want to edit.
4. Edit any fields (except the username).
5. Click *Save*.

NOTE: Changes to *User Rights (Administrator/Report Administrator/Auditor)* take effect the next time the user logs in.

8.2.4 Resetting Another User's Password (admin only)

To reset another user's password, see "Editing Another User's Profile (admin only)" on page 132.

8.3 Deleting a User

Administrators can delete a user from the system.

1. Log in to the Sentinel Log Manager as an administrator.
2. Click *user* in the upper left corner of the page.
3. Click *Edit* under the *Users* tab.
4. Click *Delete this user* in the upper right corner of the *Users* tab.
5. To delete the user permanently, click *Delete*.

8.4 Configuring Sentinel Log Manager Server for LDAP Authentication

You can enable users to log in to Sentinel Log Manager by using their Novell eDirectory™ username or Microsoft Active Directory* sAMAccountName and password. You do this by configuring a Sentinel Log Manager server for LDAP authentication.

NOTE: LDAP authentication is currently supported only on Linux systems that have Sentinel Log Manager 1.0.0.4 or later installed.

8.4.1 Configuring the Server

To configure a Sentinel Log Manager server for LDAP authentication:

1. Log in to the Sentinel Log Manager server as the `novell` user:

   ```
   su - novell
   ```

2. Change to the following directory:

   ```
   Install_Directory/bin
   ```

3 Run the ldap_auth_config.sh script:

```
./ldap_auth_config.sh
```

4 Specify the following information:

Press Enter to accept the default value suggested in the brackets [ ] or enter a new value to override the default value.

Parameter	Description
Sentinel Log Manager install location	The default location of Sentinel Log Manager server installation directory is `/opt/novell/Sentinel_log_mgr_1.0_x86-64`
LDAP directory	The value is 1 for Novell eDirectory or 2 for Active Directory. The default value is 1.
LDAP server hostname or IP address	The hostname or the IP address of the machine where the LDAP server is installed. The default value is localhost.

Parameter	Description
Use SSL/TLS (secured or non-secured LDAP connection port)	Enter one of the following: ◆ `y` to use the secured connection port and perform the below steps: 1. Login as the `root` user. 2. Export the self-signed certificate of the Certificate Authority (CA) for the eDirectory/Active Directory tree to a Base64-encoded file. **eDirectory:** For exporting an eDirectory CA certificate in iManager, the Novell Certificate Server plug-ins for iManager must be installed. For more information on installing an iManager plug-in, see Downloading and Installing Plug-in Modules (http://www.novell.com/documentation/imanager27/imanager_admin_273/?page=/documentation/imanager27/imanager_admin_273/data/hk42s9ot.html). For more information on exporting an eDirectory CA certificate, see Exporting an Organizational CA's Self-Signed Certificate (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html). **Active Directory:** For more information on exporting an Active Directory CA certificate, see How to enable LDAP over SSL (http://support.microsoft.com/kb/321051). For the Sentinel LDAP authentication, the ANONYMOUS LOGON user object must be given read access to `sAMAccountName` and `objectclass` attributes. For more information, see Configuring Active Directory to Allow Anonymous Queries (http://support.microsoft.com/kb/320528). For Windows Server 2003, you must perform additional configuration. For more information, see Configuring Active Directory on Windows Server 2003 (http://support.microsoft.com/kb/326690/en-us). 3. Copy the certificate file to the following directory on Sentinel Log Manager server: *Install_Directory*/config 4. Set the ownership and permissions of the certificate file as follows: `chown novell:novell Install_Directory/config/<cert-file>` `chmod 400 Install_Directory/config/<cert-file>` ◆ `n` to use the non-secured connection port. ◆ `q` to quit the configuration.
LDAP server port	The default port number for a secured LDAP connection is 636. The default port number for a non-secured LDAP connection is 389.

Parameter	Description
LDAP subtree to search for users	The subtree in the directory that has the user objects. The following are examples for specifying subtree in eDirectory and Active Directory: ◆ eDirectory: `ou=users, o=novell` For eDirectory, if no subtree is specified, the search is run on the entire directory. ◆ Active Directory: `CN=users, DC=TEST AD, DC=provo, DC=novell, DC=com` For Active Directory, the subtree cannot be blank.
Filename of the LDAP server certificate This parameter is displayed only if you have specified 'y' for Use SSL/TLS.	The filename of the eDirectory/Active Directory CA certificate that you have copied in Step 4.

5 Enter one of the following:

- `y` to accept the values.
- `n` to enter new values.
- `q` to quit the configuration.

6 Enter `y` to restart the Sentinel Log Manager server.

7 Log in to Sentinel Log Manager as `admin`. Create a Directory user and select the directory authentication type to authenticate with an existing user's LDAP credentials.

For more information about creating a user, see "Adding a User" on page 129.

You have successfully configured Sentinel Log Manager server for LDAP authentication, and users can log in to Sentinel Log Manager by using an eDirectory username or Active Directory sAMAccountName and password.

8.4.2 Modifying the LDAP Authentication Configuration

To modify an existing LDAP authentication configuration for a Sentinel Log Manager server:

1 Log in to a Sentinel Log Manager server as the `novell` user:

```
su - novell
```

2 Change to the *`Install_Directory`*`/config` directory:

```
cd Install_Directory/config
```

3 Modify the `LdapLogin` entry in the `auth.login` file of the *`Install_Directory`*`/config` directory.

4 Modify the `.activemqkeystore.jks` file in the *`Install_Directory`*`/config` directory.

5 Perform Step 1 through Step 7 in Section 8.4, "Configuring Sentinel Log Manager Server for LDAP Authentication," on page 132.

IMPORTANT: Modifying the `auth.login` or `.activemqkeystore.jks` incorrectly causes LDAP authentication to fail. The user can also modify the `.activemqkeystore.jks` file with the java `keytool` utility available in the *`Install_Directory`*`/jre/bin` directory.

Managing License Keys

9

This section describes the License feature of the Novell® Sentinel™ Log Manager. You can add a license key and also view the details of the added licenses. By default, Sentinel Log Manager comes with the Embedded Database Licensed Feature. Licenses are categorized as Application licenses and EPS licenses. The Application licenses monitor each application. The EPS licenses check against the EPS of the incoming events.

9.1 License Categories

The following sections describe the each type of licenses:

9.1.1 Application Licenses

Licenses are generated based on the plug-in type, vendor, and device name.

For example, the Collector.Novell.eDirectory license allows Sentinel Log Manager to collect events only from the eDirectory application, where Collector is the plug-in type, Novell is the Vendor, and eDirectory™ is the device name.

You can also create a more generalized license such as Collector.Novell, which allows Sentinel Log Manager to collect events from all applications with the Vendor name Novell.

If you configure and start the Collector without any license, the Collector shows a red cross and the `Collector is not licensed to run` message is displayed in the status details of the Event Source Management interface.

9.1.2 EPS Licenses

Licenses are also generated based on EPS (events per second). The incoming EPS is checked against the licensed EPS installed on Sentinel Log Manager. If the incoming EPS exceeds the licensed EPS value, then an audit event and a log message are generated. The log message is logged in the server log file. The Sentinel Log Manager continues with the events collection.

9.2 Managing License Keys

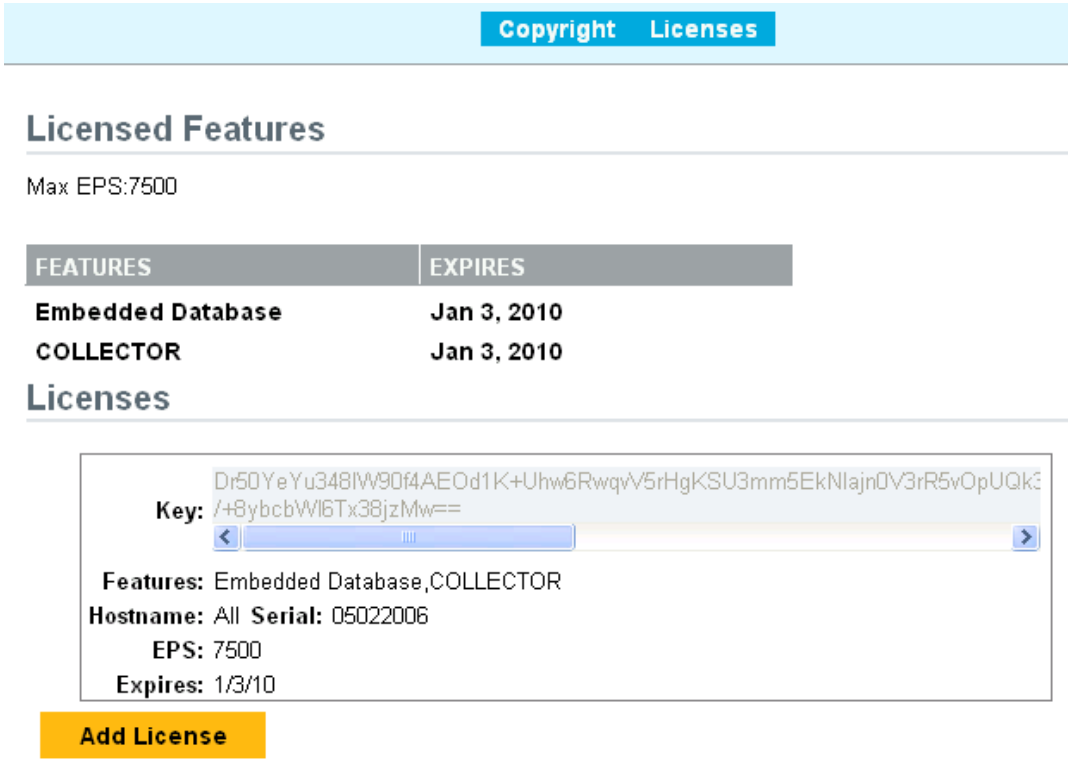
The following sections describe how you can add, view, and delete the license keys:

NOTE: To add, view, or delete a license, you must have admin rights.

- Section 9.2.2, “Viewing License Features,” on page 138
- Section 9.2.3, “Deleting a License Key,” on page 139

9.2.1 Adding a License Key

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.
4. In the *License* section, click *Add License*.



The *Enter License Key* field is displayed.

To purchase the license keys, either call 1-800-529-3400 or contact Novell Technical Support (http://support.novell.com).

5. Paste the license key in the *Enter License Key* field.

   If you paste the license key, the preview of the license is displayed immediately.
6. Click *Save*.

9.2.2 Viewing License Features

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 1500, 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.

9.2.3 Deleting a License Key

NOTE: You can only delete an expired license.

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 *License*s 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. The *delete license* link is displayed only when a license expires.
4. Click the *delete license* link. A confirmation message is displayed.
5. Click *Delete*.

Command Line Utilities

10

The command line utilities included with Novell® Sentinel™ Log Manager are useful for managing and configuring many lower level functions of the system.

10.1 Managing the Sentinel Log Manager Services

10.1.1 Starting the Sentinel Log Manager

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 *Install_Directory*/bin directory.
3. To start Sentinel Log Manager, run the following command:

   ```
   ./server.sh start
   ```

10.1.2 Stopping the Sentinel Log Manager

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 *Install_Directory*/bin directory.
3. To stop Sentinel Log Manager, run the following command:

   ```
   ./server.sh stop
   ```

10.1.3 Checking the Sentinel Log Manager Service Status

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 *Install_Directory*/bin directory.

3 To check Sentinel Log Manager service status, run the following command:

```
./server.sh status
```

10.1.4 Checking the Sentinel Log Manager Version

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 *Install_Directory*/bin directory.

3 To check Sentinel Log Manager version, run the following command:

```
./server.sh version
```

10.1.5 Restarting the Sentinel Log Manager

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 *Install_Directory*/bin directory.

3 To restart Sentinel Log Manager, run the following command:

```
./server.sh restart
```

10.1.6 Starting the Database

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 *Install_Directory*/bin directory.

3 To start database, run the following command:

```
./server.sh startdb
```

10.1.7 Stopping the Database

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 *Install_Directory*/bin directory.

3 To stop database, run the following command:

```
./server.sh stopdb
```

10.2 Sentinel Scripts

The *Install_Directory*/bin (on UNIX) 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.

10.2.1 Operational Scripts

The scripts below can be used during the normal operation of Sentinel Log Manager.

Table 10-1 *Operational Scripts*

Script File:	Description:
dbconfig	Configures the database connection settings. For more information, see "Reconfiguring Database Connection Properties" on page 143.
config_firewall.sh	For more information, see "Listening on Ports Below 1024" on page 52.

10.3 Getting Sentinel Log Manager .jar Version Information

The following procedure describes how to gather the version information of `Sentinel Log Manager .jar` files:

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 *`Install_Directory`*`/bin` directory.
3. At the command line, specify the `./versionreader.sh <path/jar file name>`.

10.4 Reconfiguring Database Connection Properties

The primary settings in these 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 these 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 *`Install_Directory`*`/bin` directory.
3. Enter the following command:

For UNIX:

```
dbconfig -a Install_Directory/config [-u username] [-p password] [-h
hostname] [-t portnum] [-d database] [-s server] [-help] [-version]
```

Other settings in the files that can be adjusted manually (without using `dbconfig`) are:

- maxConnections
- batchSize
- loadSize

Changing these settings might affect database performance and should be done with caution.

Managing Data

A

A.1 Data Expiration Policy

This section lists the order in which Sentinel Log Manager chooses to delete data from the archive 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 online and archive) are deleted as soon as the *keep at most* time limit of their retention policy completes.
2. Partitions that are successfully archived (oldest first until none-left or the desired amount of space is available).
3. Partitions that are not yet archived, 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 archived 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).

A.2 Database Users

The installer creates and configures a PostgreSQL database with users.

There are several users created by default:

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.

Truststore

B

If you are using strict authentication for the connection between Log Manager and the Novell® applications, a truststore can improve data security.

A truststore can be created using the Java* “keytool” executable, which comes with any JRE* installation. This truststore holds a public and private keypair that can be used to replace the default certificate that comes with Sentinel Log Manager. There are basic instructions below, but for more information on keytool, see the Sun* Web site (http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html).

1. Go to the `/bin` directory for Java (for example, `$JAVA_HOME/bin`).
2. Run the following command:

   ```
   keytool -genkey -alias alias -keystore .keystore
   ```

3. Specify a password for the truststore. This password is used when you import the truststore.
4. Specify the following information:
   - First and last name
   - Organizational unit
   - Organization
   - City or locality
   - State or province
   - Two-digit country code
5. Verify the information.
6. Press Enter to use the same password as the keystore password.

   A `.keystore` file is created with a private key and corresponding public key (certificate).

Event Fields

C

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).

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 C-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		
CorrelatedEventUuids	ceu	List of event UUIDs associated with this correlated event. Only relevant for correlated events.			

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
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 (`root` using `su`, 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
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
ObserverIP	obsip	The IP address of the observer (sensor) that detected the event.			Y

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
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		
TargetDataName	fn	The name of the data object (file, database table, directory object, etc) that was affected by this event.			Y
TargetFunction	rv47	Target function.	Y		

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
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		
TargetServiceComp	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

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
TargetUserIdentity	tuident	The internal UUID of the identity associated with the target account.			
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.			

Field	Short Name	Description	Tokenized	Visible in Basic View	Visible in Detailed View
XDASIdentifier	xdasid	The XDAS Event Identifier; refer to XDAS specification.			
XDASOutcome	xdasoutcome	The XDAS major outcome; success, failure, or denial.			
XDASOutcomeName	xdasoutcome name	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	

Sentinel Log Manager Reports

D

This section lists all the pre-installed reports that are bundled with Novell® Sentinel™ Log Manager.

- All Vendors All Products Account Access Assignments
- All Vendors All Products Account Trust Assignments
- All Vendors All Products Authentication By Server
- All Vendors All Products Authentication by User
- All Vendors All Products Event Count Trend
- All Vendors All Products Object Provisioning
- All Vendors All Products Password Resets
- All Vendors All Products Per Object Modification
- All Vendors All Products Per Trust Modification
- All Vendors All Products Per User Modification
- All Vendors All Products Self Password Changes
- All Vendors All Products Trust Access Assignments
- All Vendors All Products Trust Management
- All Vendors All Products Trust Provisioning
- All Vendors All Products User Account Provisioning
- Cisco Firewall Authentication By Server
- Cisco Firewall Authentication by User
- Cisco Firewall Event Count Trend
- Cisco Firewall Password Resets
- Cisco Firewall Per User Modification
- Cisco Firewall Self Password Changes
- Cisco Firewall Trust Provisioning
- Cisco Firewall User Account Provisioning
- Cisco Switch Authentication By Server
- Cisco Switch Authentication by User
- Cisco Switch Event Count Trend
- Cisco VPN 3000 Authentication By Server
- Cisco VPN 3000 Authentication by User
- Cisco VPN 3000 Event Count Trend
- Enterasys Dragon Event Count Trend
- Extreme Networks Summit Series Authentication By Server
- Extreme Networks Summit Series Authentication by User
- Extreme Networks Summit Series Event Count Trend

- Extreme Networks Summit Series Password Resets
- Extreme Networks Summit Series Per Object Modification
- Extreme Networks Summit Series Per User Modification
- Extreme Networks Summit Series Self Password Changes
- Extreme Networks Summit Series User Account Provisioning
- Generic Event Collector Event Count Trend
- HP HP UX Account Access Assignments
- HP HP UX Account Trust Assignments
- HP HP UX Authentication By Server
- HP HP UX Authentication by User
- HP HP UX Event Count Trend
- HP HP UX Password Resets
- HP HP UX Per Trust Modification
- HP HP UX Per User Modification
- HP HP UX Self Password Changes
- HP HP UX Trust Management
- HP HP UX Trust Provisioning
- HP HP UX User Account Provisioning
- IBM AIX Account Access Assignments
- IBM AIX Account Trust Assignments
- IBM AIX Authentication By Server
- IBM AIX Authentication by User
- IBM AIX Event Count Trend
- IBM AIX Password Resets
- IBM AIX Per Trust Modification
- IBM AIX Per User Modification
- IBM AIX Self Password Changes
- IBM AIX Trust Management
- IBM AIX Trust Provisioning
- IBM AIX User Account Provisioning
- Juniper Netscreen Series Account Access Assignments
- Juniper Netscreen Series Account Trust Assignments
- Juniper Netscreen Series Authentication By Server
- Juniper Netscreen Series Authentication by User
- Juniper Netscreen Series Event Count Trend
- Juniper Netscreen Series Object Provisioning
- Juniper Netscreen Series Password Resets
- Juniper Netscreen Series Per Object Modification

- Juniper Netscreen Series Per Trust Modification
- Juniper Netscreen Series Per User Modification
- Juniper Netscreen Series Self Password Changes
- Juniper Netscreen Series Trust Access Assignments
- Juniper Netscreen Series Trust Management
- Juniper Netscreen Series Trust Provisioning
- Juniper Netscreen Series User Account Provisioning
- McAfee ePolicy Orchestrator Event Count Trend
- McAfee Firewall Enterprise Authentication By Server
- McAfee Firewall Enterprise Authentication by User
- McAfee Firewall Enterprise Event Count Trend
- McAfee Firewall Enterprise Password Resets
- McAfee Firewall Enterprise Per User Modification
- McAfee Firewall Enterprise Self Password Changes
- McAfee Firewall Enterprise User Account Provisioning
- McAfee Network Security Platform Event Count Trend
- McAfee VirusScan Enterprise Event Count Trend
- Microsoft Active Directory Account Access Assignments
- Microsoft Active Directory Account Trust Assignments
- Microsoft Active Directory Authentication By Server
- Microsoft Active Directory Authentication by User
- Microsoft Active Directory Event Count Trend
- Microsoft Active Directory Object Provisioning
- Microsoft Active Directory Password Resets
- Microsoft Active Directory Per Object Modification
- Microsoft Active Directory Per Trust Modification
- Microsoft Active Directory Per User Modification
- Microsoft Active Directory Self Password Changes
- Microsoft Active Directory Trust Access Assignments
- Microsoft Active Directory Trust Management
- Microsoft Active Directory Trust Provisioning
- Microsoft Active Directory User Account Provisioning
- Microsoft SQL Server Authentication By Server
- Microsoft SQL Server Authentication by User
- Microsoft SQL Server Event Count Trend
- Microsoft SQL Server Object Provisioning
- Microsoft SQL Server Password Resets
- Microsoft SQL Server Per Object Modification

- Microsoft SQL Server Per Trust Modification
- Microsoft SQL Server Self Password Changes
- Microsoft SQL Server Trust Access Assignments
- Microsoft SQL Server Trust Management
- Microsoft SQL Server Trust Provisioning
- Nortel VPN Authentication By Server
- Nortel VPN Authentication by User
- Nortel VPN Event Count Trend
- Nortel VPN Trust Access Assignments
- Novell Access Manager Event Count Trend
- Novell eDirectory Account Access Assignments
- Novell eDirectory Account Trust Assignments
- Novell eDirectory Authentication By Server
- Novell eDirectory Authentication by User
- Novell eDirectory Event Count Trend
- Novell eDirectory Object Provisioning
- Novell eDirectory Password Resets
- Novell eDirectory Per Object Modification
- Novell eDirectory Per Trust Modification
- Novell eDirectory Per User Modification
- Novell eDirectory Self Password Changes
- Novell eDirectory Trust Access Assignments
- Novell eDirectory Trust Management
- Novell eDirectory Trust Provisioning
- Novell eDirectory User Account Provisioning
- Novell Identity Manager Account Access Assignments
- Novell Identity Manager Account Trust Assignments
- Novell Identity Manager Authentication By Server
- Novell Identity Manager Authentication by User
- Novell Identity Manager Event Count Trend
- Novell Identity Manager Object Provisioning
- Novell Identity Manager Password Resets
- Novell Identity Manager Per Object Modification
- Novell Identity Manager Per Trust Modification
- Novell Identity Manager Per User Modification
- Novell Identity Manager Self Password Changes
- Novell Identity Manager Trust Access Assignments
- Novell Identity Manager Trust Management

- Novell Identity Manager Trust Provisioning
- Novell Identity Manager User Account Provisioning
- Novell iManager Authentication By Server
- Novell iManager Authentication by User
- Novell iManager Event Count Trend
- Novell iManager Per Trust Modification
- Novell iManager Trust Management
- Novell Modular Authentication Services Event Count Trend
- Novell NetWare Account Access Assignments
- Novell NetWare Account Trust Assignments
- Novell NetWare Authentication By Server
- Novell NetWare Authentication by User
- Novell NetWare Event Count Trend
- Novell NetWare Object Provisioning
- Novell NetWare Per Object Modification
- Novell Open Enterprise Server Event Count Trend
- Novell Open Enterprise Server Object Provisioning
- Novell Open Enterprise Server Per Object Modification
- Novell Privileged User Manager Event Count Trend
- Novell Sentinel Link Event Count Trend
- Novell SUSE Linux Enterprise Server Account Access Assignments
- Novell SUSE Linux Enterprise Server Account Trust Assignments
- Novell SUSE Linux Enterprise Server Authentication By Server
- Novell SUSE Linux Enterprise Server Authentication by User
- Novell SUSE Linux Enterprise Server Event Count Trend
- Novell SUSE Linux Enterprise Server Object Provisioning
- Novell SUSE Linux Enterprise Server Password Resets
- Novell SUSE Linux Enterprise Server Per Object Modification
- Novell SUSE Linux Enterprise Server Per Trust Modification
- Novell SUSE Linux Enterprise Server Per User Modification
- Novell SUSE Linux Enterprise Server Self Password Changes
- Novell SUSE Linux Enterprise Server Trust Management
- Novell SUSE Linux Enterprise Server Trust Provisioning
- Novell SUSE Linux Enterprise Server User Account Provisioning
- Red Hat Enterprise Linux Account Access Assignments
- Red Hat Enterprise Linux Account Trust Assignments
- Red Hat Enterprise Linux Authentication By Server
- Red Hat Enterprise Linux Authentication by User

- Red Hat Enterprise Linux Event Count Trend
- Red Hat Enterprise Linux Password Resets
- Red Hat Enterprise Linux Per Trust Modification
- Red Hat Enterprise Linux Per User Modification
- Red Hat Enterprise Linux Self Password Changes
- Red Hat Enterprise Linux Trust Management
- Red Hat Enterprise Linux Trust Provisioning
- Red Hat Enterprise Linux User Account Provisioning
- Sourcefire Snort Event Count Trend
- Sun Solaris Account Access Assignments
- Sun Solaris Account Trust Assignments
- Sun Solaris Authentication By Server
- Sun Solaris Authentication by User
- Sun Solaris Event Count Trend
- Sun Solaris Password Resets
- Sun Solaris Per Trust Modification
- Sun Solaris Per User Modification
- Sun Solaris Self Password Changes
- Sun Solaris Trust Management
- Sun Solaris Trust Provisioning
- Sun Solaris User Account Provisioning
- Symantec Endpoint Protection Event Count Trend
- TippingPoint Security Management System Event Count Trend
- Websense Web Security Event Count Trend

Collector Scripts

E

Copy_SAVCE_Log_Files.bat and Copy_SEP_Log_Files.bat: These scripts are used by the Symantec Endpoint Protection Collector. Instructions on how to use them are included in that Collector documentation. The scripts are located in the `setup` directory of the Sentinel Log Manager installation directory.

oes2sentinelsetup.sh: This script is used in conjunction with the Novell Open Enterprise Server Collector. The script is located in the `setup` directory of the Sentinel Log Manager installation directory.

NOTE: Always download and use the latest version of `oes2sentinelsetup.sh` script.

---

wtmpsetup: This script enables following two important capabilities on UNIX operating systems:

- Enables the Syslog Connector auto-detection capability by injecting into the syslog stream a message that contains an identifier. The identifier allows the Syslog Connector to select and use the best collector for the operating system where the script is installed. For parsing the data, the identifier matches the most appropriate UniqueMatchingRule in the connection mode property of the Collector. If this script is not used, you can still configure the system to route data to the right Collector by manually reconfiguring the event source to send data by using the Web console or the Event Source Management Interface.
- Enables proper logging of user login events. Without this script, user logins are not logged by the operating system to the syslog stream. This script is designed to be used in conjunction with the following Collectors:
  - HP HP-UX (11iv1 and 11iv2)
  - Sun* Microsystems Solaris* 10
  - Novell SUSE® Linux Enterprise Server
  - Red Hat Enterprise Linux

  The script is located in the `setup` directory of the Sentinel Log Manager installation directory.

NOTE: The collector setup is performed through the Event Source Management interface. For device configuration or setup scripts, see the Sentinel 6.1 content Web site (http://support.novell.com/products/sentinel/sentinel61.html).

Syslog Collector Package Policy

F

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