Novell Sentinel Log Manager 1.0.0.4 Release Notes

Novell.

February 08, 2010

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 What's New in Novell Sentinel Log Manager

The following sections list the new and enhanced features of Novell Sentinel Log Manager.

1.1 What's New in Novell Sentinel Log Manager 1.0.0.4

1.1.1 New Data Collection User Interface

The new and enhanced data collection user interface enables you to perform several new tasks:

- Refine all the event sources by using the new *Event Sources* screen.

- Start and stop the audit and syslog event source server by using the new *Event Source Server*s tab.
- Set the time zone for event sources.
- Search for events that are coming from one or many event sources.

For more information about data collection configuration, see "Configuring Data Collection" in the *Novell Sentinel Log Manager 1.0.0.4 Administration Guide*.

1.1.2 LDAP Authentication

Sentinel Log Manager now supports LDAP authentication in addition to the database authentication.

A new *Authentication Type* option has been added in the *user* > *Add a user* window of the Sentinel Log Manager, which enables you to create user accounts that use LDAP authentication.

For more information about configuring the Sentinel Log Manager server for LDAP authentication, see "User Administration" in the *Novell Sentinel Log Manager 1.0.0.4 Administration Guide*.

1.1.3 Enhancements to the Search Result User Interface

The enhanced search result interface enables you to perform several new tasks:

- Export search report results.
- Send search results to an action.
- Download the raw data files for the selected event result's event source by using the *get raw data* link.
- View new event fields information in the search results.

  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.
- View all the event fields information for the event source by using the *show all fields* link.

For more information about searching events and generating reports, see "Searching" in the *Novell Sentinel Log Manager 1.0.0.4 Administration Guide*.

1.1.4 New User Interface for Actions

The new user interface for actions allows you to create multiple action instances that you can also use while configuring rules. You can also view the number of rules that are associated with an action.

For more information about configuring rules and actions, see "Configuring Rules" in the *Novell Sentinel Log Manager 1.0.0.4 Administration Guide*.

1.1.5 Enhancement to the Admin User Interface

The new admin user interface enables you to assign new permissions for a user:

- You can now allow users to view all reports that are stored on the server
- Enable Sentinel Log Manager configuration reporting
- You can now set a filter for the events a user can view.

For more information about configuring users, see "User Administration" in the *Novell Sentinel Log Manager 1.0.0.4 Administration Guide*.

1.2 Novell Sentinel Log Manager 1.0 Features

- "Installation and Deployment" on page 3
- "Data Collection" on page 3
- "Data Storage and Management" on page 4
- "Reporting and Searching" on page 4
- "Architecture Options" on page 5

1.2.1 Installation and Deployment

Novell Sentinel Log Manager is easy to install and deploy for data collection, storage, reporting, and searching of log data. Installation of Novell Sentinel Log Manager includes installation of the Sentinel Log Manager server, Web server, reporting server, and configuration database.

1.2.2 Data Collection

Novell Sentinel Log Manager can collect and manage data from event sources that generate logs to syslog, windows event log, files, databases, SNMP, Novell Audit, SDEE, Check Point OPSEC, and other storage mechanisms and protocols.

Novell Sentinel Log Manager contains enhanced web-based user interface support for Syslog and Novell Audit connectivity to make it even easier to start collecting logs from event sources. You can direct all the logs to Sentinel Log Manager.

Messages from recognized data sources are parsed into fields such as target IP address and source username. Messages from unrecognized data sources are placed intact into a single field for storage, search, and reporting. All data can be filtered to drop unwanted events.

For a complete list of supported event sources, see "Supported Event Sources" (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bhmwq0w.html) in the *Novell Sentinel Log Manager Guide*.

Novell Sentinel Log Manager collects data using a wide variety of connection methods:

- Syslog Connector automatically accepts and configures syslog data sources that send data over the standard user datagram protocol (UDP), reliable transmission control protocol (TCP), or secure transport layer system (TLS).
- Audit Connector automatically accepts and configures audit-enabled Novell data sources.
- File Connector reads log files.
- SNMP Connector receives SNMP traps.
- JDBC* Connector reads from database tables.
- WMS Connector accesses Windows* event logs on desktops and servers.
- SDEE Connector for Cisco* devices.
- LEA Connector for Check Point* devices.

- Sentinel Link Connector accepts data from other Novell Sentinel Log Manager servers.
- Process Connector accepts data from custom-written processes that output event logs.

You can also purchase an additional license to download connectors for SAP* and mainframe operating systems.

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

For more information about configuring the connectors, see the connector documents at Sentinel Content Web site (http://support.novell.com/products/sentinel/sentinel61.html).

For more information about data collection configuration, see "Configuring Data Collection" (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bjxe7z1.html) in the *Novell Sentinel Log Manager Guide*.

1.2.3 Data Storage and Management

Novell Sentinel Log Manager stores all of the log data in a compressed file format. Data can be archived locally or on a remotely-mounted CIFS or NFS share. You can set up data retention policies to configure the system to keep some data for longer time periods and other data for shorter time periods.

For more information about system requirements, see "System Requirements" (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bjx8zq7.html) in the *Novell Sentinel Log Manager Guide*.

For more information about data storage configuration, see "Configuring Data Storage" (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bjxe7z1.html) in the *Novell Sentinel Log Manager Guide*.

1.2.4 Reporting and Searching

Novell Sentinel Log Manager can perform full text searches of all the stored event data or perform focused searches against particular event fields, such as source username. Such searches can be further refined, saved for future review, filtered, and formatted by applying a report template to the results.

Sentinel Log Manager has pre-installed reports and also has the ability to upload additional reports. Reports can be run as per a planned scheduled or for an unplanned requirement.

For more information on list of default reports, see "Sentinel Log Manager Reports" (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bl5jfoz.html) in the *Novell Sentinel Log Manager Guide*.

Searches and reports can run against both online and archived data.

For more information about searching events and generating reports, see "Searching" (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bk76y16.html) and "Reporting" (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bjxdi87.html) respectively in the *Novell Sentinel Log Manager Guide*.

1.2.5 Architecture Options

Collector managers for Sentinel Log Manager manage all of the data collection processes and data parsing. A Collector Manager is included in the Sentinel Log Manager server installation, but you can also install multiple collector managers throughout your enterprise. Remote collector managers provide several benefits:

- Distributed event parsing and processing to improve system performance.
- Co-location with event sources, which allows filtering, encryption, and data compression at the source. This can provide additional data security and decrease network bandwidth requirements.
- Installation on additional operating systems (for example, installation on Microsoft* Windows* to enable data collection using the WMI protocol).
- File caching, which enables the remote collector manager to cache large amounts of data while the server is temporarily busy performing archiving or processing a spike in events. This is an advantage for protocols, such as syslog, that do not natively support event caching.

Sentinel Link can be used to forward event data from one Sentinel Log Manager to another. With a hierarchical set of Sentinel Log Managers, complete logs can be retained at multiple regional locations while more important events are forwarded to a single Sentinel Log Manager for centralized search and reporting.

In addition, Sentinel Link can forward important events to Novell Sentinel, a full Security Information Event Management (SIEM) system, for advanced correlation, incident remediation, and injection of high-value contextual information such as server criticality or identity information from an identity management system.

1.3 New Plug-Ins

A new Generic Forwarder Action 6.1r2 plug-in has been added to send search results to an action instance.

2 System Requirements

For a detailed information on hardware requirements and supported operating systems, browsers, and event sources, see “System Requirements” (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bjx8zq7.html) in the *Novell Sentinel Log Manager Guide*.

3 Prerequisite

The Sentinel Log Manager Hot fix 4 (1.0.0.4) should be installed on top of an existing Sentinel Log Manager 1.0.0.0 or 1.0.0.1 or 1.0.0.2 or 1.0.0.3 installation.

4 Installation

IMPORTANT: The Sentinel Log Manager Hot fix 4 (1.0.0.4) must be installed on the Sentinel Log Manager server and all the Collector Managers running on remote machines. This hotfix does not update the Collector Manager installer script that you can download from the Sentinel Log Manager web server. Hence, regardless of whether you have installed a Collector Manager before or after applying the hotfix on the Sentinel Log Manager server, it is mandatory to apply this hotfix to all the Collector Managers.

- Section 4.1, "On a Sentinel Log Manager Server," on page 6
- Section 4.2, "On a Remote Collector Manager," on page 6

4.1 On a Sentinel Log Manager Server

To perform a quick and simple installation of Novell Sentinel Log Manager 1.0.0.4 on a Sentinel Log Manager server:

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

   The `novell` user is created during the Sentinel Log Manager installation process and does not have a password by default. Therefore, you can create a password in order to log in as this user, or you can su - to this user.
2. Download or copy the installer `SENTINEL_LOG_MANAGER_1.0.0.4.zip` to a temporary directory.
3. Change to the temporary directory.
4. Unzip the install package by using the following command:
   ```
   unzip SENTINEL_LOG_MANAGER_1.0.0.4.zip
   ```
5. Change to the unzipped directory.
   ```
   cd SENTINEL_LOG_MANAGER_1.0.0.4
   ```
6. (Optional) Stop the Sentinel Log Manager services by using the following command:
   ```
   Installation_Directory/bin/server.sh stop
   ```
7. Run the hotfix installer and follow the prompts.
   ```
   ./service_pack.sh
   ```

4.2 On a Remote Collector Manager

- "Installing on Unix" on page 6
- "Installing on Windows" on page 7

4.2.1 Installing on Unix

1. Log in to the Sentinel Log Manager as the `root` user.
2. Download or copy the installer `SENTINEL_LOG_MANAGER_1.0.0.4.zip` to a temporary directory.
3. Change to the temporary directory.
4. Unzip the install package by using the following command:
   ```
   unzip SENTINEL_LOG_MANAGER_1.0.0.4.zip
   ```
5. Change to the unzipped directory.
   ```
   cd SENTINEL_LOG_MANAGER_1.0.0.4
   ```
6. (Optional) Stop the Collector Manager by using the following command:
   ```
   Installation_Directory/bin/sentinel.sh stop
   ```

7. Run the hotfix installer and follow the prompts.

```
./service_pack.sh
```

4.2.2 Installing on Windows

1. Log in to the Sentinel Log Manager as an `Administrator`.
2. Download or copy the installer `SENTINEL_LOG_MANAGER_1.0.0.4.zip` to a temporary directory.
3. Change to the temporary directory.
4. Unzip the installer package.
5. Change to the unzipped directory.

   ```
   cd SENTINEL_LOG_MANAGER_1.0.0.4
   ```
6. (Optional) Stop the Collector Manager by using the following command:

   ```
   Installation_Directory/bin/sentinel.bat stop
   ```
7. Go to the installation directory.
8. Execute the `service_pack.bat` from the command window and follow the prompt.

5 Issues Fixed

- Section 5.1, "Issues Fixed in Sentinel Log Manager 1.0.0.4 Release," on page 7
- Section 5.2, "Issues Fixed in Sentinel Log Manager 1.0.0.3 Release," on page 9
- Section 5.3, "Issues Fixed in Sentinel Log Manager 1.0.0.2 Release," on page 11
- Section 5.4, "Issues Fixed in Sentinel Log Manager 1.0.0.1 Release," on page 11

5.1 Issues Fixed in Sentinel Log Manager 1.0.0.4 Release

This section lists the issues fixed in Novell Sentinel Log Manager 1.0.0.4 Release.

Table 1 *Issues fixed in Sentinel Log Manager 1.0.0.4 Release*

Issues Fixed	Description
551079	Issue: In the report details, if the time range is not set to custom date range, then the time shown reflect the actual times the report had been run. Fixed: After the report is run, the date range is being displayed appropriately in the report details.
545195	Issue: When there are many event sources in the Operating System section of syslog server user interface, the browser reports an `unresponsive script` error. As a result Sentinel Log Manager user interface also becomes unusable. Fixed: A new Data Collection user interface with Sentinel Log Manager hotfix 4 properly manages the event sources.

Issues Fixed	Description
532421	Issue: The e-mails received from Sentinel Log Manager has Novell Identity Audit Event text in the subject line. Fixed: The Subject field is now user configurable.
549330	Issue: The Device Event Time field is appearing as searchable field in the search tips popup. Fixed: The Device Event Time field is not a searchable field. It is now deleted from the search tips popup.
523499	Issue: Passwords with both backward and forward slashes and single quote characters are not accepted while login. Fixed: Now the passwords with escape characters (\, /, and ‘) are allowed.
499349	Issue: When executing a search from the search toolbar on the upper right hand corner of the user interface, it would intermittently open a search tab with the search criteria of a previous search rather than the currently typed in search. Fixed: The new search tab now always has the most recently typed in search criteria.

5.1.1 Enhancement

This section lists the enhancements in Novell Sentinel Log Manager 1.0.0.4 Release.

Table 2 *Enhancements in Sentinel Log Manager 1.0.0.4 Release*

Issues Fixed	Description
553146	Issue: A raw data link is required next to each search result entry that will take you to the unparsed raw data on the Raw Data Download page. The event will display the data originated from the event source. Fixed: A *get raw data* link is added to each search result. Clicking on this link opens a Raw Data Download page in a new tab and points to the appropriate event source.
509882	Issue: An option to export the report results option should be included. Fixed: Sentinel Log Manager interface now provides you an option to export the report results.
508992	Issue: An option needs to be provided to know the number of events the user has scrolled through. Fixed: The left pane of the search result displays the number of events the user has scrolled through.
504105	Issue: LDAP authentication option should be added for Sentinel Log Manager. Fixed: Sentinel Log Manager now supports the LDAP authentication option.

Issues Fixed	Description
557632	Issue: The exported results `.csv` file should display the important fields columns at the beginning. Fixed: Important fields are placed in the beginning of csv report. The fields are ordered as dt, port, sev, evt, msg, rv42, shn, sip, rv35, sun, rv41, dhn, dip, rv45, dun, sp, isvcc, dp, tsvcc, ttd, ttn, rv36, and fn followed by other fields as long as field has valid value.
542187	Issue: Exported search results were unreadable with too many empty columns, which was causing it to throw some errors while opening in open office. Fixed: The empty columns are removed from the search results to make it more readable and compact.
547204	Issue: Subject was not configurable in the Send an Email action user interface and all the mails had default subject value. Fixed: Now you can specify a subject line using the *Subject* field in the *Send an Email* action user interface.
530183	Issue: The number of records value that went into a collector should be displayed in the Collector status details pane of the Event Source Management interface. Fixed: The *Total Records Sent* and *Records Sent in Last Interval* fields are included in the Collector status details pane of the Event Source Management interface.
495806	Issue: Export search result has the same event count limit as search refinement (50,000). Fixed: The 50,000 limit for exporting results has been removed. Now the user will be prompted to enter the number of results they want to export.

5.2 Issues Fixed in Sentinel Log Manager 1.0.0.3 Release

This section lists the issues fixed in Novell Sentinel Log Manager 1.0.0.3 Release.

Table 3 *Issues fixed in Sentinel Log Manager 1.0.0.3 Release*

Issues Fixed	Description
563948	Issue: A message stating that no events have been found by the search is displayed even before the search is completed. Fixed: The `no events found` message only appears if no events are found after the completion of a search.
560580	Issue: Occasional searches run from the search tool bar used the previous search string instead of the new search string. Fixed: A new search run from the search tool bar uses the new search string.

Issues Fixed	Description
556411	Issue: Squashfs indexes that were mounted by a previous running instance of the server are not cleaned up when the server starts, resulting is failed searches. Fixed: The server now detects if old mounts need to be cleaned up and cleans them up allowing searches to complete normally.
552519	Issue: The softwarekey.sh script was not included in the install, making it difficult to reset the license key with the server turned off. Fixed: The softwarekey.sh script is now included.
549582	Issue: An event is not searchable by its original timestamp if it arrives more than a day late. Fixed: The event is searchable by its original timestamp no matter how late it arrives.
546324	Issue: A rule or data retention policy configured with a filter that is just a full text search (i.e., no field such as `sev:5` is specified) results in an error on the server that prevents any users from logging into the Web interface or ESM user interface. Fixed: The bug is fixed so that all valid filters are now accepted and evaluated properly. Filter validation is also done before allowing a user to save a filter to prevent an invalid filter from being saved that would cause logins to fail.
545837	Issue: The Event Source Management (ESM) user interface is not able to read the maxclausecount property in the `SentinelPreferences.properties` file. Fixed: The Event Source Management (ESM) user interface works fine with a high number (>=~1000) event sources and does not log any `max clause count exceeded` exceptions.
545197	Issue: When many event sources are configured (for example, 2000+), the Event Source Management (ESM) user interface consumes lot of memory on webstart (for example, 1GB) and also becomes unusable. Fixed: The ESM user interface now works fine if there are many event sources are configured.
527007	Issue: To turn on or off the data logging for all of the operating system event sources and all of the Application collectors, a *Data logging (All) On and Off* option is required for the *APPLICATIONS* and *OS* tables under the *Collection* > *Syslog Server* tab. Fixed: To turn on or off the data logging for all of the operating system event sources and all of the Application collectors, a *Data logging (All) On and Off* option is provided for the *APPLICATIONS* and *OS* tables under the *Collection* > *Syslog Server* tab.

5.2.1 Enhancement

Top N type reports are now supported. A Top N type report named `All Vendors All Products Top 10 Report` is installed with this hotfix and is available as a Visualization from the Search Save As Report dialog as well from the main report list. This report provides an easy way to view a dashboard of the most frequent activity being monitored by Sentinel Log Manager.

5.3 Issues Fixed in Sentinel Log Manager 1.0.0.2 Release

This section lists the issues fixed in Novell Sentinel Log Manager 1.0.0.2 Release.

Table 4 *Issues fixed in Sentinel Log Manager 1.0.0.2 Release*

Issues Fixed	Description
537273	Issue: Non-admin user is able to log in to the Event Source Management interface by using a cached ESM jnlp file. Fixed: Only authorized admin user can log in to the Event Source Management interface.
536377	Issue: Lucene indexes are not being committed on a timely basis. Fixed: Lucene indexes are now being committed on a timely basis - once a minute.
535736	Issue: The Rule user interface does not perform the filter validation. Fixed: The specified filter value is validated by the Rule user interface.
536589	Issue: IndexedLogComponent can get stuck on deactivate when shutting down under heavy load (high EPS). Fixed: IndexedLogComponent will now shutdown gracefully under heavy load.
540119	Issue: When the Sentinel Log Manager Server runs for many days (for example, 25-40 days), it stores huge amount of EPS data, which is generated over time. This eps information is transferred to the tomcat server in a verbose format so it consumes a lot of memory and also while parsing the eps data it causes out of memory at the tomcat server. Fixed: The eps data information will now be transferred in a more compact format from the Sentinel Log manager server to the Tomcat server.
541858	Issue: A few events that are generated on a remote Collector Manager do not get displayed on the Sentinel Log Manager server. Fixed: All the events that are generated on a remote Collector Manager will be displayed on the Sentinel Log Manager server as expected.
543029	Issue: When one Sentinel Log Manager is configured with multiple Collector Managers. On changing a Collector for an event source under the *Collection* > *Syslog Server* tab, the Collector and the event source gets assigned to the wrong Collector Manager. Fixed: On changing a Collector for an event source under the *Collection* > *Syslog Server* tab, the Collector and the event source will be assigned to their respective Collector Manager.

5.4 Issues Fixed in Sentinel Log Manager 1.0.0.1 Release

This section lists the issues fixed in Novell Sentinel Log Manager 1.0.0.1 Release.

***Table 5** Issues fixed in Sentinel Log Manager 1.0.0.1 Release*

Issues Fixed	**Description**
527031	Issue: If the browser and the server are running in different time zones, the dates in the search results are not displaying correctly. Fixed: The dates in the search results are now displayed in the local timezone of the browser, regardless of which timezone the server is running in.
527006	Issue: The values in all of the drop down boxes in the raw data download page should be sorted alphabetically. Fixed: The values in the drop-down box appears in the alphabetical order.
526143	Issue: The communication links between the Sentinel Log Manager server and either Tomcat or Collector Managers do not always recover when the link is dropped temporarily. The link may get dropped temporarily due to network outage, system load, or a variety of other reasons. If this occurs to the link with Tomcat, the Web Server becomes unresponsive. If this occurs to the link with Collector Managers, data from the Collector Managers no longer flows to the Sentinel Log Manager, although the data is cached on the Collector Manager file system. Fixed: The communication links between the Sentinel Log Manager server and either Tomcat or Collector Managers recovers even when the link is dropped temporarily.
526119	Issue: Online data storage graphs are not displayed when the nfs archive location is unshared. Fixed: The Online data storage graphs are being displayed even if the archive location is not accessible.
524994	Issue: In Internet Explorer 8 browser, an error message is displayed on entering a search criteria and hitting enter instead of clicking on Search button. Fixed: The search results appear as expected.
525099	Issue: Sentinel Log Manager does not need to listen on port 1099. Fixed: Sentinel Log Manager does not listen on port 1099.
525075	Issue: On the Firefox browser if you log in to Sentinel Log Manager with the Administrator or Report Administrator credentials, perform a self edit and save the user details twice, then by default it takes the Auditor permission. Fixed: On performing a self edit of the Administrator or Report Administrator user accounts, the settings will not change to Auditor permission.
524606	Issue: The scheduled report is getting deleted when it is edited and invalid start time is entered. Fixed: After editing the scheduled report and giving invalid start time, the scheduled report will not get deleted.

Issues Fixed	Description
524453	Issue: The Data Archive user interface always reports the following error when setting the archive location, even if the save succeeded: ◆ Failed Data Archive Configuration Save. ◆ Archive could not be configured, as archive was already configured. Fixed: No error message is displayed when archive location is set successfully.
523873	Issue: If archiving is configured to use NFS and the connection to the NFS server is lost, the archiving process will stop working and the storage graphs on the user interface will not be displayed. Fixed: The issue has partially been fixed in the code. However, the other half of it needs to be fixed manually. Since the hotfix contains code to automatically set the NFS mount options automatically to the correct value, remove the `-Dnovell.sentinel.mount.options` property from the server.conf and restart the Sentinel Log Manager service to correct the problem. The code will automatically use the NFS mount options `soft,proto=tcp,timeo=60,retrans=1`. To restart the Sentinel Log Manager service, execute the following command: `<Installation_Directory>/bin/server.sh restart`
522907	Issue: On deleting a data retention policy an unnecessary exception is logged if the policy has events that match the specified filter criteria. The exception should not be logged because no real error actually occurred. Fixed: The exception is no longer logged.
509112	Issue: On performing a search that returns more than 50,000 results. the event fields that were selected (by default) in the Select Event Fields window are not displayed in the user interface on scrolling through the search results. Fixed: All the events fields are being displayed.
529773	Issue: Event router server is not executing an action to send events from remote Collector Managers to the Sentinel Machine. Fixed: Event router server is now able to send events to the Sentinel machine from the remote collector manager.
528049	Issue: On the data collection page, the *data logging* on/off buttons are not working for the Syslog server event sources. Fixed: The data logging on/off buttons now correctly turn the event source on/off and reflect the proper current state of the event source.
524998	Issue: On the Internet Explorer 8 browser, the scroll bar to view the license is disabled. Fixed: The license key can be viewed by using the scroll bar.

Issues Fixed	Description
527023	Issue: An exception log message appears when archiving is disabled. Fixed: The exception message has been changed to an INFO level log message `Archive location is not configured` when archiving is disabled.
527306	Issue: server.sh script is not automatically correcting the permissions of the postgresql data directory before startup. Fixed: server.sh script automatically corrects the permissions of the `data` folder. The permissions of `data` folder reverts back to the old permissions.
532219	Issue: In some cases, an Out of Memory occurs in the Tomcat server related to the Data Collector Events Per Second chart. Fixed: The out of memory issue conditions has been fixed when generating this chart.
501503	Issue: The `start_tomcat.sh` script selects the wrong IP if there are multiple interfaces returned by `/sbin/ifconfig`. Fixed: The script now excludes ipv6 addresses from its search for the best address to use and, therefore, does a better job at choosing the right IP address.

6 Known Issues

- Section 6.1, "Known Issues in Sentinel Log Manager 1.0," on page 14
- Section 6.2, "Known Issues in Sentinel Plug-ins," on page 17

6.1 Known Issues in Sentinel Log Manager 1.0

This section lists the known issues in Novell Sentinel Log Manager 1.0 Release.

Table 6 *Known Issues in Sentinel Log Manager 1.0 Release*

Issue Number	Description
523007	*Issue: Export Result* and *Save as Report* links are not visible after performing search operation using custom option in search result page. Workaround: To view all the links, set the screen resolution to 1280 x 1024.
503808	Issue: The Event Source Management (ESM) application fails to launch in the first attempt when it is installed on a server where it has never been installed before. Workaround: Re-launch the application.
524575	On Microsoft Internet Explorer* 8, all javascript pop-up windows display error when French (fr) or Italian (it) or Spanish (es) languages are selected on login page. Workaround: Use the Firefox 3 web browser instead.

Issue Number	**Description**
510824	Issue: After clicking the *details++* link for the individual search results, the all details++ and all details-- link does not work as intended. Workaround: Avoid using the *all details* link until this issue is fixed.
524473	Issue: The prompt for using the 90 day evaluation license is not localized in non-English versions of the product.
521942	Issue: If many reports are run within a sort period of time (for example, 40-50 reports within 5-10 minutes), you may experience the following error: `java.lang.OutOfMemoryError: PermGen space` Workaround: This is a temporary error due to the number of reports being run. Try running the report again later.

Issue Number	Description

525753	Issue: If the command `hostname -f` did not return a valid hostname during Sentinel Log Manager installation, the user is unable to accept a certificate when Collector Manager is installed.
	Workaround: To avoid the issue, before installing the Log Manager server, test the `hostname -f` command to make sure it returns a valid hostname. This needs to be tested on the Log Manager server machine, not the machine where the Collector Manager is going to be installed.
	If you get stuck in a loop during the Collector Manager install, the workaround is the following:
	1. There is no need to exit the Collector Manager install. Instead, perform the following steps while the Collector Manager install remains at the user/password prompt.
	2. Log in to the Log Manager server as the `novell` user.
	3. Run the following command:
	`server.sh stop`
	4. Specify the command to change directory: `cd /opt/novell/sentinel_log_mgr_1.0_x86-64/config`
	5. hostname -f (make sure a valid hostname is returned - if not, fix hostname)
	NOTE: All passwords must remain set to `password` in the following commands.
	◆ `../jre/bin/keytool -delete -alias broker -keystore .activemqkeystore.jks -storepass password`
	◆ `../jre/bin/keytool -genkey -alias broker -keyalg RSA -keystore .activemqkeystore.jks -storepass password -keypass password -dname "CN=`hostname -f`, O=broker"`
	◆ `../jre/bin/keytool -list -keystore .activemqkeystore.jks -v -storepass password`
	◆ `../jre/bin/keytool -export -alias broker -keystore .activemqkeystore.jks -storepass password -file .activemq.cer`
	◆ `../jre/bin/keytool -delete -alias broker -keystore .activemqclientkeystore.jks -storepass password`
	◆ `../jre/bin/keytool -import -noprompt -alias broker -keystore .activemqclientkeystore.jks -storepass password -file .activemq.cer`
	6. Run the following command:
	`server.sh start`
	7. Return to the Collector Manager install and enter the user/pass/accept cert. You should see a valid issuer name and the acceptance of the certificate should proceed normally.

6.2 Known Issues in Sentinel Plug-ins

The collectors supporting the following event sources that are bundled with Sentinel Log Manager have known issues. These issues are fixed in the latest version of the collectors available on the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/sentinel61.html).

- Novell Access Manager 3.1
- Novell Identity Manager 3.6.1
- Novell Netware 6.5
- Novell Modular Authentication Services 3.3
- Novell Open Enterprise Server 2.0.2
- Novell SUSE® Linux Enterprise Server
- Novell eDirectory™ 8.8.3 with the eDirectory instrumentation patch found on the Novell Support Web Site (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~)
- Novell iManager 2.7
- McAfee* VirusScan* Enterprise (8.0i, 8.5i, and 8.7i)

The following table lists known issues that still exist in other Sentinel Plug-ins:

Table 7 Known Issues in Sentinel Plug-ins

Issue Number	Description
524664	Issue: Queue full condition might cause unpredictable behavior. If a queue size limit is set for the Integrator, and the queue is full, and the Integrator configuration specifies that the oldest messages are to be dropped, it is possible that the thread which attempts to drop the oldest message has a conflict with the thread that is reading data from the queue to send it over the wire. One or both threads might incorrectly modify the queue read pointer, or other unexpected behaviors may occur such as exceptions, etc. Workaround: Do not specify a queue limit. or Specify that the newest message should be dropped instead of the oldest.
522544	Issue: Collector stops requesting data from the Database Connector if the event source is restarted but the collector is not also restart. Workaround: Stop the collector, then start the event source. Starting the event source causes the collector to start.
504507	Issue: When configuring a File event source, the browse button does not work properly when running the Event Source Management Interface on some operating systems (for example, Windows XP). Workaround: Type in the file or directory path in the text field.

Issue Number	Description

524671	Issue: Integrators threads are not started when server starts.
	Currently, the Sentinel Link Integrator is not initialized and started until they receive their first event from an action. This is because it may have events stored in its queue that should be forwarded. When the Integrator starts, a background thread is also started to process this.
	Workaround: If Integrator is not sending events, either because no events are happening or events are being filtered by rules, you must generate a fake event that does not get filtered in order to get your Integrator started.
	To determine if the Integrator thread is started, search for a message in the log that indicates that the Integrator has started. It will be logged by the StoreAndForward logger (esecurity.ccs.comp.Integrator.slink.StoreAndForward), and will have a message similar to the following:
	`Thread processing messages from store and forward queue starting up.`
	or
	`SentinelLinkStoreAndForward thread starting up.`
	NOTE: The actual message might change, so search for messages logged by the StoreAndForward logger.

526364	Issue: Some connector documentation has the wrong version of the connector stated in the documentation. For example, the documentation may say 6r5 when the version of the connector is really 6r6. Workaround: This is a typo. To determine the correct version of the connector, open the Event Source Manager Interface, select the connector from the list of connectors on the left hand side of the interface, and click the *info* button.

7 Documentation Conventions

In this 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

8 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.