AUTHORIZED DOCUMENTATION

Installation Guide

Novell®
Sentinel Log Manager 1.0.0.5

1.0.0.5

March 31, 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.
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.

About This Guide

This guide provides an overview of Novell® Sentinel™ Log Manager and its installation.

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 configuring Sentinel Log Manager, see *Sentinel Log Manager 1.0.0.4 Administration 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.

Contents

Introduction 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

1.1.1 What’s New in Novell Sentinel Log Manager 1.0.0.5

500 EPS Version of Sentinel Log Manager

The Novell Sentinel Log Manager is now available in a 500 EPS (events per second) version. The 500 EPS version is suitable for small deployments with only one Sentinel Log Manager server and a low event rate. It can also be used as a low volume node reporting to another Sentinel or Sentinel Log Manager server in a large deployment.

New End User License Agreement

The end user license agreement (EULA) terms have been updated in this release. You must accept the new terms before before proceeding to apply the latest patch. Some of the changes in the EULA are:

- Novell Sentinel Log Manager is now available in a 500 EPS version.
- Updated definition for `Non-Production Instance`.
- Updated definition for `Type I Device`.

1.1.2 What’s New in Novell Sentinel Log Manager 1.0.0.4

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 *Sentinel Log Manager 1.0.0.4 Administration Guide*.

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 *Sentinel Log Manager 1.0.0.4 Administration Guide*.

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 *Sentinel Log Manager 1.0.0.4 Administration Guide*.

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 *Sentinel Log Manager 1.0.0.4 Administration Guide*.

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 *Sentinel Log Manager 1.0.0.4 Administration Guide*.

1.1.3 Novell Sentinel Log Manager 1.0 Features

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.

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*.

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*.

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.

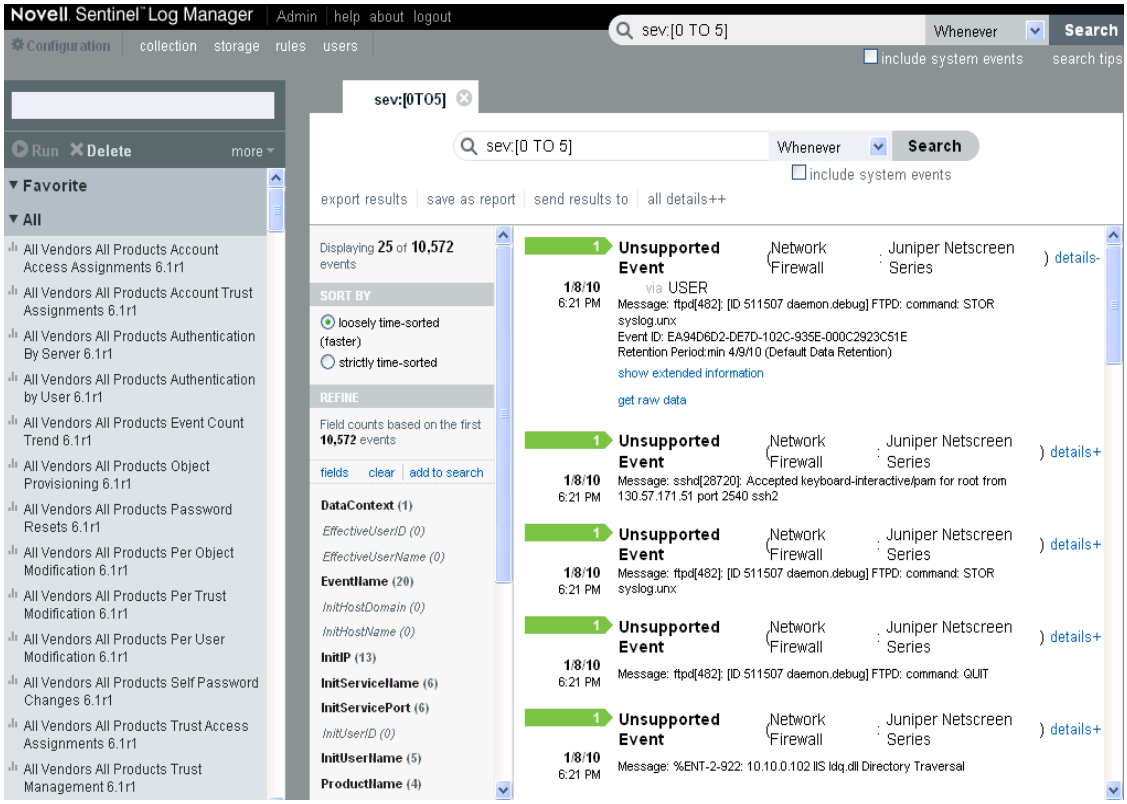
For more information about searching events and generating reports, see "Searching" (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bk76y16.html) and "Reporting" (http://www.novell.com/documentation/novelllogmanager10/novell_log_manager/data/bjxdi87.html) respectively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

1.2 Novell Sentinel Log Manager Interface

You can use the Novell Sentinel Log Manager Web interface to perform the following tasks:

- Search for events
- Save the search criteria as a report template
- View and manage reports
- Launch the Event Source Management interface to configure data collection for data sources other than Syslog and Novell applications.
- Configure data forwarding
- Download the Sentinel Collector Manager installer for remote installation
- View the health of event sources (administrators only)
- Configure data collection for Syslog and Novell data sources (administrators only)
- Configure data storage and view the health of the database (administrators only)
- Configure data archiving (administrators only)
- Configure associated actions to send matching event data to output channels (administrators only)
- Manage user accounts and permissions (administrators only)

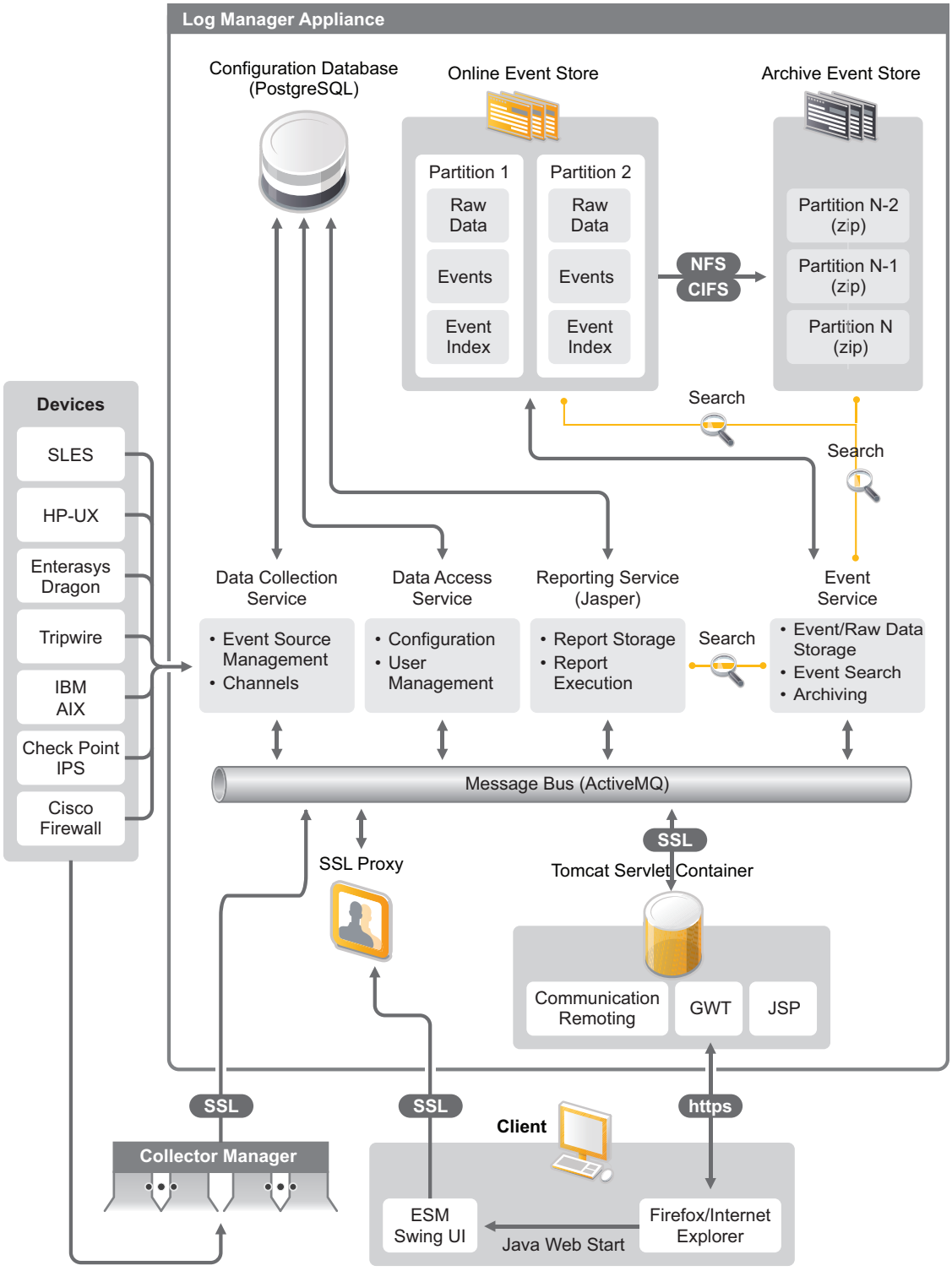
Figure 1-1 *Novell Sentinel Log Manager Interface*



1.3 Architecture

The following illustration depicts the architecture of Novell Sentinel Log Manager:

Figure 1-2 *Novell Sentinel Log Manager Architecture*



Novell Sentinel Log Manager architecture comprises of components that perform data collection, data storage, search, and reporting by using the user interfaces.

Data Collection: Novell Sentinel Log Manager collects data with the help of connectors. These connectors obtain data from device logs, and collectors parse device log data into a standardized format.

Data Storage: The data flows from data collection components to data storage components. These components use a file based data storage and indexing system to keep device log data and a PostgreSQL database to keep Novell Sentinel Log Manager configuration data. The search and reporting components access and find the requested event log data.in the file based data storage and indexing system. The data storage components also deletes data from storage location when the data retention time limit exceeds or if the available space reduces below an specified disk space value.

Searching and Reporting: The searching and reporting components search the data in both the online and archive storage locations.

User Interface: User interface functionality is provided by a Web server and a Java Web Start based graphical user interface (GUI). All user interfaces communicate with the server by using an encrypted connection.

Collector Manager Optionally, you can remotely install a collector manager from the Sentinel Log Manager server at a suitable location in your network. The collector manager provides a flexible data collection point. The remote collector manager runs the connectors and collectors, forwards the output of the collectors onto Novell Sentinel Log Manager for storage and further processing.

For information about installing collector managers, see "Installing Additional Collector Managers" on page 33.

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.

System Requirements

2

In addition to the hardware, operating system, browser, supported connectors, and event source compatibility requirements described below, the user must also have root access for some installation steps.

2.1 Hardware Requirements

2.1.1 Sentinel Log Manager

Novell® Sentinel™ Log Manager is supported on 64-bit Intel* Xeon* and AMD* Opteron* processors, but not supported on Itanium* processor.

NOTE: These requirements are for an average event size of 300 bytes.

A single server may cater different event sources. For example, a Windows server could collect data from the Windows platform and also from an SQL server database hosted on it.

Novell recommends the following hardware requirements for a production system that holds 90-days of online data:

Table 2-1 *Sentinel Log Manager Hardware Requirements*

Requirements	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
Compression	Up to 10:1	Up to 10:1	Up to 10:1
Maximum event sources	Up to 1000	Up to 1000	Up to 2000
Maximum events	500	2,500	7,500

Requirements	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
CPU	One Intel* Xeon* E5450@3 GHz (4core) CPU or Two Intel* Xeon* L5240@3 GHz (2 core) CPUs (4 cores total)	One Intel* Xeon* E5450@3 GHz (4 core) CPU or Two Intel* Xeon* L5240@3 GHz (2 core) CPUs (4 cores total)	Two Intel* Xeon* X5470@3.33 GHz (4 core) CPUs (8 cores total)
Random Access Memory (RAM)	4GB	4 GB	8 GB
Storage	2x 500 GB, 7.2k RPM drives (Hardware RAID with 256 MB cache, RAID 1	2 x 1 TB, 7.2k RPM drives (Hardware RAID with 256 MB cache, RAID 1)	6 x 450 GB, 15k RPM drives, (Hardware RAID with 512 MB cache, RAID 5)

NOTE:

- You must set up the archive location to an external multi-drive storage network area (SAN) or network-attached storage (NAS).
- The recommended steady state volume is 80% of the maximum licensed EPS. Novell recommends that you add additional Sentinel Log Manager instances if this limit is reached.

2.1.2 Collector Manager

The following are the minimum requirements for Collector Manager:

- One Intel* Xeon* L5240@3 GHz (2 core CPU)
- 256 MB RAM
- 10 GB - free disk space.

2.1.3 Estimating the Data Storage Space Requirement

Sentinel Log Manager is used to retain raw data for a long period of time to comply with legal and other requirements. Sentinel Log Manager employs compression to help you make efficient use of local and archive storage space. However, over a long period of time storage requirements might become significant.

To overcome cost constraint issues with large storage systems, you can use cost effective data storage systems to store the data for a long term. Tape-based storage systems are the most common and cost-effective solution. However, tape does not allow random access to the stored data, which is necessary to perform quick searches. Because of this, a hybrid approach to long-term data storage is desirable, where the data you need to search is available on a random-access storage system and data you need to retain, but not search, is kept on a cost-effective alternative, such as tape. Instructions for employing this hybrid approach are described in "Using Sequential-Access Storage for Long Term Data Storage" of the *Sentinel Log Manager 1.0.0.4 Administration Guide*.

To determine the amount of random-access storage space required for Sentinel Log Manager, first estimate how many day's worth of data you need to regularly perform searches or run reports on. You should have enough hard drive space either locally on the Sentinel Log Manager machine, or remotely on a CIFS, NFS, or SAN that Sentinel Log Manager can use to archive data.

You should also have additional hard drive space beyond your minimum requirements:

- To account for data rates that are higher than expected.
- To copy data from tape and back into the Sentinel Log Manager in order to perform searching and reporting on historical data.

Use the following formulas to estimate the amount of space required to store data:

- **Event Data Storage Size:** {number of days} x {events per second} x {average byte size of event} x 0.000012 = GB storage required

  Event sizes typically range from 300-1000 bytes.
- **Raw Data Storage Size:** {number of days} x {events per second} x {average byte size of raw data} x 0.000012 = GB storage required

  A typical average raw data size for syslog messages is 200 bytes.
- **Total Storage Size:** ({average byte size of event} + {average byte size of raw data}) x {number of days} x {events per second} x 0.000012 = Total GB storage required

---

NOTE:

- These numbers are only estimates and depend on the size of your event data as well as on the size of compressed data.
- The above formulas calculate the minimum storage space required to store fully compressed data on the external storage system. When local storage fills up, Sentinel Log Manager seamlessly compresses and moves data from local (partially compressed) to external (fully compressed) storage system. Therefore, estimating the external storage space requirement becomes most critical for data retention. To improve the search and reporting performance for recent data, you can increase the local storage space beyond the hardware requirements of Sentinel Log Manager; however it is not required.

You can also use the above formulas to determine how much storage space is required for long term data storage system, for example using tape.

2.1.4 Virtual Environment

Sentinel Log Manager has been extensively tested on VMWare* ESX Server, and Novell fully supports Sentinel Log Manager in this environment. Performance results in a virtual environment can be comparable to the results achieved in tests on physical machine, but the virtual environment should provide the same memory, CPU, disk space, and I/O as the physical machine recommendations.

2.2 Supported Operating Systems

2.2.1 Sentinel Log Manager

Sentinel Log Manager requires installation on 64-bit SUSE® Linux Enterprise Server 11.

Sentinel Log Manager stores event data in a compressed file system in a searchable form. So it requires a high-performing file system. All Novell testing is done with the ext3 file system.

2.2.2 Collector Manager

The Collector Manager is supported on the following platforms:

- SUSE® Linux Enterprise Server 10 SP2 (32-bit and 64-bit)
- SUSE® Linux Enterprise Server 11 (32-bit and 64-bit)
- Windows* 2003 (32-bit and 64-bit)
- Windows* 2003 SP2 (32-bit and 64-bit)
- Windows Server* 2008 (64-bit)

2.3 Supported Browsers

The following browsers are supported by Sentinel Log Manager. Other browsers might not display information as expected.

- Mozilla* Firefox* 3
- Microsoft* Internet Explorer* 8

NOTE: The Sentinel Log Manager interface is optimized for viewing at 1280 x 1024 or higher resolution.

2.3.1 Setting Browser's Internet Security Level

In Microsoft* Internet Explorer* 8, set the security level to the default level (*Medium-high*) by navigating to *Tools > Internet Options > Security tab > Security levels*. If the Internet Security Level is set to *High*, then only a blank page appears after logging in to Novell Sentinel Log Manager.

2.4 Supported Connectors

This section lists the supported connectors:

- Audit Connector
- Check Point LEA Process Connector
- Database Connector
- Data Generator Connector
- File Connector
- Process Connector
- Syslog Connector
- SNMP Connector

- SDEE Connector
- Sentinel Link Connector
- WMS Connector

NOTE: The Mainframe and SAP Connectors require a separate license.

2.5 Supported Event Sources

All event sources (devices) are supported, if there is a suitable connector to access their data. Novell Sentinel Log Manager provides collectors for many event sources. These collectors perform deep parsing of recognized events coming from the event sources. Data from event sources that have a suitable connectors, but whose data is unrecognized are processed by the Generic Event Collector. On a best-effort basis the Generic Event Collector analyses the received data and attempts to parse the information, if it was generated by a supported event source. If the Generic Event Collector does not understand the message, it does minimal parsing and places the bulk of the text in the *Message* field.

Sentinel Log Manager has enhanced support for data collection from Syslog and Novell Audit devices and the data collection can be configured by using the Sentinel Log Manager Web interface.

Sentinel Log Manager is also capable of collecting data from other devices by using many other connectors (for example: Database, File, and SNMP Connectors). Data collection from these devices can be configured by using the Event Source Management interface, which enables you to import and configure the Sentinel 6.0 and 6.1 connectors and collectors.

NOTE: Updated collectors and connectors are posted to the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/sentinel61.html) on a regular basis. Updates typically include fixes, support for additional events, and performance improvements. Always download and import the latest version of the collectors and connectors.

Collectors that support the following event sources are pre-installed with Novell Sentinel Log Manager:

- Cisco* Firewall (6 and 7)
- Cisco* Switch Catalyst 6500 Series (CatOS 8.7)
- Cisco* Switch Catalyst 6500 Series (IOS 12.2SX)
- Cisco* Switch Catalyst 5000 Series (CatOS 4.x)
- Cisco* Switch Catalyst 4900 Series (IOS 12.2SG)
- Cisco* Switch Catalyst 4500 Series (IOS 12.2SG)
- Cisco* Switch Catalyst 4000 Series (CatOS 4.x)
- Cisco* Switch Catalyst 3750 Series (IOS 12.2SE)
- Cisco* Switch Catalyst 3650 Series (IOS 12.2SE)
- Cisco* Switch Catalyst 3550 Series (IOS 12.2SE)
- Cisco* Switch Catalyst 2970 Series (IOS 12.2SE)
- Cisco* Switch Catalyst 2960 Series (IOS 12.2SE)
- Cisco* VPN 3000 (4.1.5, 4.1.7, and 4.7.2)

- Extreme Networks Summit X650 (with ExtremeXOS 12.2.2 and earlier)
- Extreme Networks Summit X450a (with ExtremeXOS 12.2.2 and earlier)
- Extreme Networks Summit X450e (with ExtremeXOS 12.2.2 and earlier)
- Extreme Networks Summit X350 (with ExtremeXOS 12.2.2 and earlier)
- Extreme Networks Summit X250e (with ExtremeXOS 12.2.2 and earlier)
- Extreme Networks Summit X150 (with ExtremeXOS 12.2.2 and earlier)
- Enterasys Dragon (7.1 and 7.2)
- Generic Event Collector
- HP HP-UX (11iv1 and 11iv2)
- IBM AIX (5.2, 5.3, and 6.1)
- Juniper* Netscreen* Series 5
- McAfee* Firewall Enterprise
- McAfee* Network Security Platform (2.1, 3.x, and 4.1)
- McAfee* VirusScan* Enterprise (8.0i, 8.5i, and 8.7i)
- McAfee* ePolicy Orchestrator (3.6 and 4.0)
- McAfee* AV Via ePolicy Orchestrator 8.5
- Microsoft Active Directory (2000, 2003, and 2008)
- Microsoft SQL Server* (2005 and 2008)
- Nortel VPN (1750, 2700, 2750, and 5000)
- 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 Privileged User Manager 2.2.1
- Novell Sentinel Link 1
- 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
- Red Hat Enterprise Linux
- Sourcefire* Snort* (2.4.5, 2.6.1, 2.8.3.2, and 2.8.4)
- Snare for Windows Intersect Alliance (3.1.4 and 1.1.1)
- Sun* Microsystems Solaris* 10
- Symantec AntiVirus Corporate Edition (9 and 10)
- TippingPoint Security Management System (2.1 and 3.0)
- Websense Web Security 7.0
- Websense Web Filter 7.0

NOTE: To enable data collection from the Novell iManager and Novell Netware 6.5 event sources, add an instance of a collector and a child connector (Audit connector) in the Event Source Management interface for each of the event sources. Once this is done, these event sources appears in the Sentinel Log Manager web console under the *Audit Server* tab.

Collectors supporting additional event sources can either be obtained from Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/sentinel61.html) or built by using the SDK plug-ins that are available on the Sentinel Plug-in SDK Web site (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

Installing and Uninstalling Novell Sentinel Log Manager

3

This section describes how to install and uninstall Novell® Sentinel™ Log Manager and Collector Managers. It also describes configuration settings for remote storage servers. These instructions assume that the minimum requirements for each system component are met. For more information on system requirements, see Chapter 2, “System Requirements,” on page 19.

The Sentinel Log Manager installation package installs the following components:

- Sentinel Log Manager server
- Communications server
- Web server and Web-based user interface
- Reporting server
- Collector Manager

Some of these components require additional configuration.

3.1 System Prerequisites

The preliminary settings listed in this section are needed to run Sentinel Log Manager.

Sentinel Log Manager should always be installed on a certified operating system. For more information on supported operating systems, see the Chapter 2, “System Requirements,” on page 19. All system testing was performed using the ext3 file system.

Install the following operating system commands:

- `mount`
- `umount`
- `id`
- `df`
- `du`
- `sudo`

Root credentials are needed for some steps in the Sentinel Log Manager installation.

3.2 Installing on an Existing Operating System

This section explains how to install Novell Sentinel Log Manager onto an existing operating system by using the compressed installer, and how to start using Sentinel Log Manager.

3.2.1 Quick Installation (as root)

To perform a simple installation of Novell Sentinel Log Manager as `root`:

1. Download or copy `sentinel_log_mgr_1.0_x86-64.tar.gz` to a temporary directory.
2. Log in as `root` to the server where you want to install Sentinel Log Manager.
3. Extract the install script from the file by using the following command:

   ```
   tar xfz sentinel_log_mgr_1.0_x86-64.tar.gz sentinel_log_mgr_1.0_x86-64/
   setup
   ```

4. Run the `root_install_all.sh` script:

   ```
   sentinel_log_mgr_1.0_x86-64/setup/root_install_all.sh
   sentinel_log_mgr_1.0_x86-64.tar.gz
   ```

   NOTE: You can log in as `root` and run the command specified above or you can use the `sudo` command to run it.

   ---

5. Choose a language by entering its number as shown in the command prompt.

   The end user license agreement is displayed in the selected language.

6. Read the end user license and enter `1` or `y`, if you agree to the terms, and to continue with the installation.

   The installation creates a novell group and novell user, if they do not already exist.

   NOTE: The novell user is created without a password. If you want to log in as the novell user later (for example, to install patches), create a password for this user after the installation is completed.

   The `/opt/novell/sentinel_log_mgr_1.0_x86-64/` installation directory is created.

7. The installer includes a 90-day evaluation license key. This license key activates the full set of product features for a 90-day trial period. At any time during or after the trial period, you can replace the evaluation license with a license key you have purchased.

   Enter `1` or `y` to use a 90-day evaluation key. Enter `2` or `n` to enter your own license key.

   For more information about license keys, see "Managing License Keys" in the *Sentinel Log Manager 1.0.0.4 Administration Guide*.

8. Specify the password for the database administrator (dbauser).
9. Confirm the password for the database administrator (dbauser).
10. Specify the password for the administrator user.
11. Confirm the password for the administrator user.

After the Sentinel Log Manager service starts, you can log in to the URL (for example: https://10.0.0.1:8443/novelllogmanager) specified in the installation output. The system starts processing the Sentinel Log Manager events immediately, and it will be fully functional after you configure event sources to send data to Sentinel Log Manager.

3.2.2 Non-root Installation

If your organizational policy does not allow you to run the full installation of Sentinel Log Manager as `root`, most of the installation steps can be run as another user. The installation scripts provided with Sentinel Log Manager and instructions in this documentation assume that the installation is run by using the *novell* user and *novell* group and that the installation directory is */opt/novell*.

1. Download or copy `sentinel_log_mgr_1.0_x86-64.tar.gz` to the `/tmp` directory.
2. Log in to the server where you want to install Sentinel Log Manager.
3. (Conditional) If the novell user and novell group do not exist on the server:
   - **3a** Extract the script to create the `novell` user and `novell` group from Sentinel Log Manager tar file.

     ```
     tar xfz sentinel_log_mgr_1.0_x86-64.tar.gz sentinel_log_mgr_1.0_x86-64/setup/root_create_novell_user.sh
     ```
   - **3b** As `root`, execute the script by using the following command:

     ```
     sentinel_log_mgr_1.0_x86-64/setup/root_create_novell_user.sh
     ```

     The `novell` user and `novell` group owns the installation and the running processes of the Sentinel Log Manager.
4. Create a directory for Sentinel Log Manager.

   ```
   mkdir -p /opt/novell
   ```
5. Set the directory to be owned by the `novell` user and `novell` group.

   ```
   chown -R novell:novell /opt/novell
   ```
6. Log in as the `novell` user:

   ```
   su - novell
   ```
7. Extract Sentinel Log Manager tar file to the directory you just created.

   ```
   cd /opt/novell
   tar xfz /tmp/sentinel_log_mgr_1.0_x86-64.tar.gz
   ```
8. Execute the installation script.

   ```
   /opt/novell/sentinel_log_mgr_1.0_x86-64/setup/install.sh
   ```
9. Choose a language by entering its number as shown in the command prompt.

   The end user license agreement is displayed in the selected language.
10. Read the end user license and enter `1` or `y` if you agree to the terms and want to continue with the installation.

    The installer includes a 90-day evaluation license key. This license key activates the full set of product features for a 90-day trial period. At any time during or after the trial period, you can replace the evaluation license with a license key you have purchased.
11. Specify the password for the database administrator (dbauser).
12. Confirm the password for the database administrator (dbauser).
13. Specify the password for the administrator user.

14 Confirm the password for the administrator user.

15 Log out and log back in as `novell`. This action loads the PATH environment variable changes made by the `install.sh` script.

16 Execute the `root_install_service.sh` script to enable Sentinel Log Manager to start up as a service. This step requires `root` level access.

```
sudo /opt/novell/sentinel_log_mgr_1.0_x86-64/setup/
root_install_service.sh
```

17 Specify the `root` password.

Novell Sentinel Log Manager is configured to start with runlevels 3 and 5 (Multi-User Mode with boot-up in console or X-Windows mode).

18 Execute the `bin/config_firewall.sh` script to enable port forwarding from ports less than 1024 (for example: Syslog port 514). This requires `root` privileges.

After the Sentinel Log Manager service starts, you can log in to the URL (for example: https://10.0.0.1:8443/novelllogmanager) specified in the installation output. The system starts processing Sentinel Log Manager events immediately, and it will be fully functional after you configure event sources to send data to Sentinel Log Manager.

3.3 Logging in to Novell Sentinel Log Manager

The administrator user created during the installation can log into the Sentinel Log Manager Web interface and configure data collection, data storage, run preloaded reports, upload new reports, perform event searches, create more users, and more.

To log into the Novell Sentinel Log Manager:

1 Open a supported Web browser. For more information, see Section 2.3, “Supported Browsers,” on page 22.

2 Log in to the Novell Sentinel Log Manager page (for example: https://10.0.0.1:8443/novelllogmanager).

If this is the first time you have logged in to the Sentinel Log Manager, you are prompted to accept a certificate.

3 Select the language for the Sentinel Log Manager interface (English, Portuguese, French, Italian, German, Spanish, Japanese, Traditional Chinese, or Simplified Chinese).

4 Specify the username as `admin`.

5 Specify the password for administrator that you configured during installation.

6 Click *Sign in*.

3.4 Configuring Archive Server Settings

Sentinel Log Manager archives data in a compressed format for the long-term storage. Several types of storage options are supported:

- **Local Storage or SAN:** The local storage or storage network area (SAN) option includes storage that is attached directly to the Sentinel Log Manager machine. This option provides the best combination of performance, security, and reliability. This is a preferable storage option in comparison to common internet file system and network file system.

- **CIFS:** The common internet file system (CIFS) protocol provides better performance and security than NFS.
- **NFS:** The network file system (NFS) protocol requires significant configuration to improve performance and security, and it is mandatory only if you already have a well-established NFS infrastructure in your environment.

If the archive destination is an NFS or CIFS server, additional configuration is necessary to ensure that the Sentinel Log Manager server has the necessary permissions. The configurations in this section are for server settings; it is also necessary to configure archiving in the Sentinel Log Manager administrator interface. For more information, see "Configuring Data Storage" in the *Sentinel Log Manager 1.0.0.4 Administration Guide*.

- Section 3.4.1, "CIFS Configuration," on page 31
- Section 3.4.2, "NFS Configuration," on page 31

3.4.1 CIFS Configuration

The configuration steps described in this section only apply in environments where the event archive destination is a CIFS server. For security reasons, you should change the following settings to limit the access to the archived data.

1. Log into the Sentinel Log Manager server as `novell`.
2. Open the `server.conf` file for editing. This file is located in the *`Install_Directory`*`/config` directory.
3. Find the `wrapper.java.additional.38` setting and modify it to:

   ```
   wrapper.java.additional.38=-
   Dnovell.sentinel.mount.options=file_mode=0660,dir_mode=0770
   ```
4. Save the file.
5. Restart the Sentinel Log Manager process by using the following command:

   ```
   Install_Directory/bin/server.sh restart
   ```

3.4.2 NFS Configuration

The configuration steps described in this section only apply in environments where the event archive destination is an NFS server. These configuration settings include configuration of both the NFS archive server and the NFS client. The exact steps can vary based on the NFS server software and operating system,. Consult with your NFS system administrator before making any changes.

- "NFS Archive Server Configuration" on page 31
- "NFS Client Configuration" on page 32

NFS Archive Server Configuration

The NFS server needs to export (share) the archive volume to the Sentinel Log Manager server so that the archive is readable by `root` user on the Sentinel Log Manager server. Following settings describe one of the method to achieve this readability:

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

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

- The archive destination directory on the NFS server must be owned by the novell user and group. In the following examples, the archive destination is `/archive`.
- The `root` user on the Sentinel Log Manager server must be mapped to the novell user and group on the NFS server.
  - **Linux** (`/etc/exports` file)

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

  - **Solaris** (`/etc/dfs/dfstab` file)

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

  - **HPUX** (`/etc/exports` file)

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

For performance reasons, you can add the async option to make the archiving process faster. However, this may increase the risk of a lost or corrupt archive, if the NFS server crashes. The following examples demonstrate the addition of the async option:

- **Linux** (`/etc/exports` file)

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

- **HPUX** (`/etc/exports` file)

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

For information about security recommendations for using NFS, see "Securing Sentinel Data" in the *Sentinel Log Manager 1.0.0.4 Administration Guide*.

NFS Client Configuration

With the default settings for mounting an NFS archive volume search requests can hang indefinitely, if the NFS server becomes unavailable. For performance reasons, you can configure a time-out setting for the search. However, after this change, restart Sentinel Log Manager process when the NFS server becomes available again to search for the archived data.

NOTE: Manual NFS client configuration is not required for Sentinel Log Manager 1.0.0.1 and later, as by default the client settings are set automatically starting from this version.

---

1. Log in to the Sentinel Log Manager server as the `novell` user.
2. Open the `server.conf` file for editing. This file is located in the *`Install_Directory`*`/config` directory.
3. Find the `wrapper.java.additional.38` setting and modify it:

   ```
   wrapper.java.additional.38=-Dnovell.sentinel.mount.options=soft,proto=tcp,retrans=1,timeo=60
   ```

4. Save the file.

5 Restart the Sentinel Log Manager process by using the following command:

```
Install_Directory/bin/server.sh restart
```

3.5 Installing Additional Collector Managers

The 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 on SUSE® Linux Enterprise Server 11 (SLES 11), but you can also install multiple collector managers in a distributed setup.

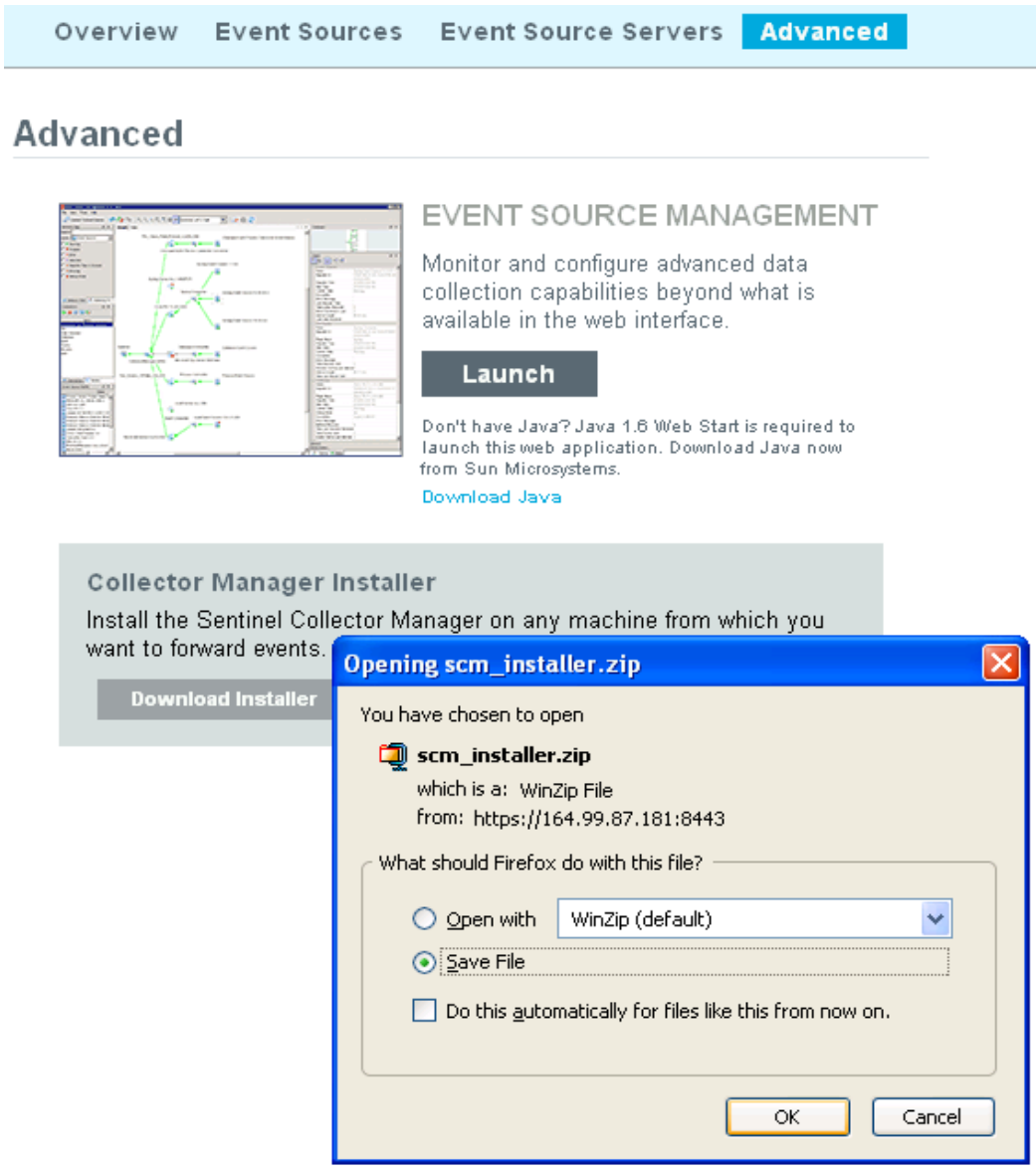
NOTE: Collector Manager requires network connectivity to the message bus port (61616) on the Sentinel Log Manager server. Before the collector manager installation, all the firewall and other network settings must be allowed to communicate over this port.

Remote collector managers provide several benefits:

- Distributed event parsing and processing to improve system performance.
- Collocation with event sources, which allows filtering, encryption, and data compression at the source. This feature provides additional data security and decreases 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 events or processing a spike in events. This feature is an advantage for protocols, such as syslog, that do not natively support event caching.

Use the following procedure to download and install the Sentinel Collector Manager installer:

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. On clicking on *Download Installer* link, an `Opening scm_installer.zip` window is displayed with the option to save the `scm_installer.zip` file on your local machine.



5 Extract the install script from the `scm_installer.zip` file and install the Sentinel Collector Manager on the machine from which you want to forward the events:

Platform	Action
Windows	Extract the `scm_installer.zip` file. The files are extracted to a directory named `disk1`.
Linux	Run the following command with root privileges: `unzip scm_installer.zip` The files are extracted to a directory named `disk1`.

6 Go to the install directory and start the installation:

Platform	Action
Windows	Run the following command: `disk1\setup.bat`
Linux	◆ **GUI mode:** `./disk1/setup.sh` ◆ **Text-based (serial console) mode:** `./disk1/setup.sh -console`

7 Select a language of your choice for installation from the drop-down list.

8 Read the Welcome screen, then click *Next* to install the Sentinel 6.1 on your system.

9 The Novell Software License Agreement wizard is displayed. Read the End User License Agreement. Select the *I accept the terms of the license agreement* option, then click *Next*.

10 Accept the default installation directory or click *Browse* to specify your installation location, then click *Next*.

NOTE: You cannot install onto a directory with special characters or non-ASCII characters. For example, when installing the collector manager on Windows x86-64, the default path is `C:\\Program Files(x86)`. You must change the default path to avoid the special characters to continue installation.

11 Specify the Sentinel administrator username and path to the corresponding home directory.

- **OS Sentinel Administrator Username:** The default is esecadm.

  This is the username of the user who owns the installed Sentinel product. If the user does not already exist, a user is created with corresponding home directory in the specified directory.
- **OS Sentinel Administrator User Home Directory:** The default is `/export/home`. If esecadm is the username, the corresponding home directory is `/export/home/esecadm`.

To log in as the esecadm user, you need to first set its password.

12 Specify the following, then click *Next*.

- **Message bus port:** The port on which the communication server is listening. Components connecting directly to the communication server uses this port.
- **Communication Server host name:** Specify the Communication Server port or host server name information.

NOTE: The port numbers must be identical on every machine in the Sentinel system to enable communications. Make a note of these ports for future installations on other machines.

13 Specify the following, then click *Next*.

- **Automatic Memory Configuration:** Select the total amount of memory to allocate to the Sentinel server. The installer automatically determines the optimal distribution of memory across components taking into account estimated operating system and database overhead.

  IMPORTANT: You can modify the-Xmx value in the `configuration.xml` file to change the RAM allocated to the Sentinel server processes. The `configuration.xml` file is placed at *`Install_Directory`*`/config` on Linux or *`Install_Directory`*`\config` on Windows.

- **Custom Memory Configuration:** Click *Configure* to fine-tune memory allocations. This option is only available if there is sufficient memory on the machine.

14 Summary screen with the features selected for installation is displayed. Click *Install* to install the Sentinel 6.1.

15 After the installation, you are prompted to enter the username and password that are used by ActiveMQ JMS strategy to connect to the broker.

You must use the `collectormanager` user and its corresponding password during the Collector Manager service installation. In this case, the `collectormanager` user will have access rights only to the required communication channels for the Collector Manager operations.

NOTE: To obtain the Collector Manager user's password, navigate to `/Install_Directory/config` directory, open the `activemqusers.properties` file. For example, in the file you may see the `collectormanager=60a25d4f67733f1074a1eafa22a50aba` text, which is the combination of alphanumeric value (such as, 60a25d4f67733f1074a1eafa22a50aba) after the equal to (=) symbol is the password.

---

16 Click *Next*. You will be prompted to accept an untrusted certificate. Select Accept Permanently. (If you do not see this certificate acceptance step, there may be something wrong with your installation. You may need to manually copy the .activemqclientkeystore.jks from the Sentinel Log Manager server.)

17 After the installation, you are prompted to reboot or re-login, and start the Sentinel services manually. Click *Finish* to reboot your system.

NOTE: If you forget the username that you have set, open a terminal console and type the command as a `root` user.

```
env | grep ESEC_USER
```

It lists down the username, if the user has already been created and the environment variable has already been set.

To start the Sentinel services manually, perform the following:

Platform	Command
On Linux	`<Install_Directory>/bin/sentinel.sh start`
On Windows	`<Install_Directory>/bin/sentinel.bat start`

To stop the Sentinel services manually, perform the following:

Platform	Command
On Linux	`<Install_Directory>/bin/sentinel.sh stop`
On Windows	`<Install_Directory>/bin/sentinel.bat stop`

18 Launch the Event Source Management interface from the Sentinel Log Manager Web page. You will see a newly installed Collector Manager.

3.6 Post-Installation Configurations

This section includes several recommendations to improve system performance.

3.6.1 Ping Timeout Setting

Novell recommends that all users must change the wait period for ping responses in the `server.conf` file to prevent issues when the Sentinel Log Manager server is heavily loaded (in an high traffic setup).

1. Log in to the Sentinel Log Manager server as `novell`.
2. Open the `server.conf` file for editing. This file is located in the *`Install_Directory`*`/config` directory.
3. Find the `wrapper.ping.timeout=60` setting and modify it to:

   ```
   wrapper.ping.timeout=0
   ```
4. Save the file.
5. Restart the Sentinel Log Manager process by using the following command:

   ```
   Install_Directory/bin/server.sh restart
   ```

3.7 Uninstalling Novell Sentinel Log Manager

To uninstall Sentinel Log Manager, run the uninstall script and then perform the manual cleanup steps given below:

1. Log in to the Sentinel Log Manager server as `root`.
2. To stop the Sentinel Log Manager service, execute the following command:

   ```
   /etc/init.d/sentinel_log_mgr stop
   ```
3. To run the uninstallation script, execute the following command:

   ```
   /opt/novell/sentinel_log_mgr_1.0_x86-64/setup/root_uninstall_service.sh
   ```
4. Delete the Sentinel Log Manager home directory and its contents.

   ```
   rm -rf /opt/novell/sentinel_log_mgr_1.0_x86-64
   ```

   If you want to retain or remove any information related to the novell user and group, use the following steps:
5. (Conditional) If you do not want to retain any information related to the novell user, run the following command to remove the user, its home directory, and the group:

   ```
   userdel -r novell && groupdel novell
   ```
6. (Conditional) If you want to retain the `novell` user and its home directory, then perform these steps to cleanup the Sentinel Log Manager settings that are stored in novell users home directory:

   6a Remove the following environment variable entries from the novell users profile in `~novell/.bashrz`:

   ```
   APP_HOME=/opt/novell/sentinel_log_mgr_1.0_x86-64
   export PATH=$APP_HOME/bin:$PATH
   ```

   6b Remove the dbauser entry from the PostgreSQL file:

`~novell/.pgpass`. `*:*:*:dbauser:`*`password`*

The dbauser password is shown in clear text, but the contents of this file are only visible to the `novell` and `root` users, who already have full access to all functions on the Sentinel Log Manager server.