

Installation Guide

Sentinel Log Manager 1.2.2

July 2014



Legal Notice

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

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

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

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

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

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

© 2014 NetIQ Corporation. All Rights Reserved.

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

Contents

About This Guide	7
1 Introduction	9
1.1 Product Overview	9
1.1.1 Event Sources	11
1.1.2 Event Source Management	11
1.1.3 Data Collection	12
1.1.4 Collector Manager	13
1.1.5 Data Storage	13
1.1.6 Searching and Reporting	13
1.1.7 Sentinel Link	14
1.1.8 Web-Based User Interface	14
1.2 Installation Overview	14
2 System Requirements	17
2.1 Hardware Requirements	17
2.1.1 Sentinel Log Manager Server	17
2.1.2 Collector Manager System	18
2.1.3 Data Storage Requirement Estimation	19
2.1.4 Disk I/O Utilization Estimation	20
2.1.5 Network Bandwidth Utilization Estimation	21
2.1.6 Virtual Environment	21
2.2 Supported Operating Systems	21
2.2.1 Sentinel Log Manager	21
2.2.2 Collector Manager	21
2.3 Supported Browsers	22
2.3.1 Linux	22
2.3.2 Windows	22
2.4 Supported Virtual Environment	22
2.5 Supported Connectors	23
2.6 Supported Event Sources	23
2.7 Recommended Limits	25
2.7.1 Collector Manager Limits	25
2.7.2 Reports Limits	26
2.7.3 Actions EPS Limits	26
2.7.4 SLES Open Files Limits	27
2.8 Search and Reports Performance	27
2.8.1 Search Response and Completion Speed	27
2.8.2 Report Generation Speed	28
3 Installing on an Existing SLES 11 SP1 System	29
3.1 Before You Begin	29
3.2 Standard Installation	30
3.3 Custom Installation	32
3.4 Silent Installation	34
3.5 Non-Root Installation	34

4	Installing the Appliance	37
4.1	Before You Begin	37
4.2	Ports Used	37
4.2.1	Ports Opened in the Firewall	38
4.2.2	Ports Used Locally	38
4.3	Installing the VMware Appliance	39
4.4	Installing the Xen Appliance	40
4.5	Installing the Appliance on Hardware	42
4.6	Post-Installation Setup for the Appliance	43
4.6.1	Installing VMware Tools	43
4.6.2	Logging in to the Appliance Web Interface	43
4.7	Configuring WebYaST	43
4.8	Configuring the Appliance with SMT	44
4.8.1	Prerequisites	45
4.8.2	Configuring the Appliance	46
4.8.3	Upgrading the Appliance	46
4.9	Stopping and Starting the Appliance by Using Web UI	46
4.10	Registering for Updates	47
5	Upgrading Sentinel Log Manager	49
5.1	Prerequisites	49
5.2	Upgrading the Sentinel Log Manager Server	50
5.3	Upgrading the Collector Manager	51
5.4	Upgrading the Appliance	52
5.4.1	Upgrading the Appliance through WebYast	52
5.4.2	Upgrading the Appliance by Using Zypper	53
5.4.3	Upgrading the Appliance by Using SMT	53
5.5	Upgrading Sentinel Plug-Ins	54
6	Logging In to the Web Interface	55
7	Installing Additional Collector Managers	57
7.1	Before You Begin	57
7.2	Advantages of Additional Collector Managers	58
7.3	Installing Additional Collector Managers	58
8	Uninstallation	61
8.1	Uninstalling the Appliance	61
8.2	Uninstalling Sentinel Log Manager	61
8.3	Uninstalling the Collector Manager	62
8.3.1	Uninstalling the Linux Collector Manager	62
8.3.2	Uninstalling the Windows Collector Manager	62
8.3.3	Manual Cleanup of Directories	63
A	Troubleshooting Installation	65
A.1	Sentinel Log Manager Upgrade Fails if the dbauser Password does not Match the dbauser Password Stored in the .pgpass File	65
A.2	Failed Installation Because of an Incorrect Network Configuration	66
A.3	Trouble Configuring the Network with VMware Player 3 on SLES 11	66
A.4	Collector Manager Throws Exception on Windows 2008 When UAC is Enabled	67

A.5	Upgrading Log Manager installed as a Non-Root User Other Than Novell User.	68
A.6	UUID Does Not get Created for Imaged Collector Managers	68
	Sentinel Terminology	69

About This Guide

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

- ◆ Chapter 1, “Introduction,” on page 9
- ◆ Chapter 2, “System Requirements,” on page 17
- ◆ Chapter 3, “Installing on an Existing SLES 11 SP1 System,” on page 29
- ◆ Chapter 4, “Installing the Appliance,” on page 37
- ◆ Chapter 5, “Upgrading Sentinel Log Manager,” on page 49
- ◆ Chapter 6, “Logging In to the Web Interface,” on page 55
- ◆ Chapter 7, “Installing Additional Collector Managers,” on page 57
- ◆ Chapter 8, “Uninstallation,” on page 61
- ◆ Appendix A, “Troubleshooting Installation,” on page 65
- ◆ “Sentinel Terminology” on page 69

Audience

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

Feedback

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

Additional Documentation

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

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

For additional documentation about configuring Sentinel Log Manager, see the *Sentinel Log Manager 1.2.2 Administration Guide*.

Contacting Novell

- ◆ [Novell Web site \(http://www.novell.com\)](http://www.novell.com)
- ◆ [Novell Technical Support \(http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup\)](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)

- ♦ Novell Self Support (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- ♦ Patch Download Site (<http://download.novell.com/index.jsp>)
- ♦ Novell 24x7 Support (<http://www.novell.com/company/contact.html>)
- ♦ Sentinel TIDS (<http://support.novell.com/products/sentinel>)
- ♦ Sentinel Community Support Forum (<http://forums.novell.com/novell-product-support-forums/sentinel/>)

1 Introduction

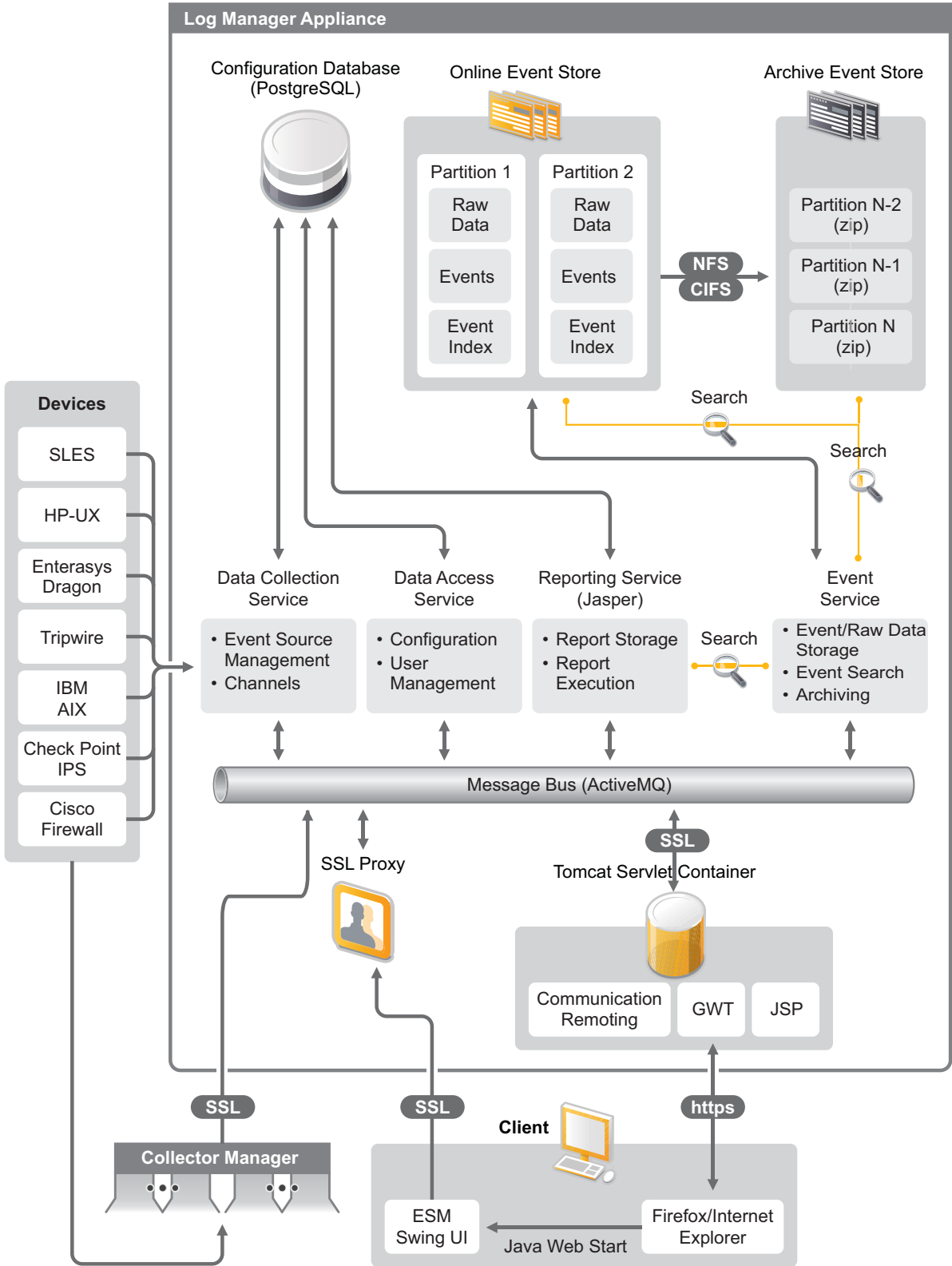
Novell Sentinel Log Manager collects and manages data from a variety of devices and applications, including intrusion detection systems, firewalls, operating systems, routers, Web servers, databases, switches, mainframes, and antivirus event sources. Novell Sentinel Log Manager provides high event-rate processing, long-term data retention, policy-based data retention, regional data aggregation, and simple searching and reporting functionality for a variety of applications and devices.

- ♦ [Section 1.1, “Product Overview,” on page 9](#)
- ♦ [Section 1.2, “Installation Overview,” on page 14](#)

1.1 Product Overview

Novell Sentinel Log Manager 1.2 provides a flexible and scalable log management solution to organizations. Novell Sentinel Log Manager is a log management solution that addresses basic log collection and management challenges and also delivers a complete solution focused on reducing the cost and complexity of managing risk and simplifying compliance requirements.

Figure 1-1 Novell Sentinel Log Manager Architecture



Novell Sentinel Log Manager has the following features:

- ◆ Distributed search capabilities allow customers to search collected events not only on the local Sentinel Log Manager server but also on one or more Sentinel Log Manager servers from one centralized console
- ◆ Pre-built compliance reports to simplify the task of generating compliance reports for audit or forensic analysis
- ◆ By utilizing non-proprietary storage technology, customers can leverage their existing infrastructure to further manage cost.
- ◆ Enhanced browser-based user interface supporting collection, storage, reporting and searching of log data to greatly simplify monitoring and management tasks.
- ◆ Granular and efficient controls and customization for IT administrators through new group and user permissions capabilities to provide increased transparency into IT infrastructure activities.

This section has the following information:

- ◆ [Section 1.1.1, “Event Sources,” on page 11](#)
- ◆ [Section 1.1.2, “Event Source Management,” on page 11](#)
- ◆ [Section 1.1.3, “Data Collection,” on page 12](#)
- ◆ [Section 1.1.4, “Collector Manager,” on page 13](#)
- ◆ [Section 1.1.5, “Data Storage,” on page 13](#)
- ◆ [Section 1.1.6, “Searching and Reporting,” on page 13](#)
- ◆ [Section 1.1.7, “Sentinel Link,” on page 14](#)
- ◆ [Section 1.1.8, “Web-Based User Interface,” on page 14](#)

1.1.1 Event Sources

Novell Sentinel Log Manager collects data from event sources that generate logs to syslog, Windows event log, files, databases, SNMP, Novell Audit, Security Device Event Exchange (SDEE), Check Point Open Platforms for Security (OPSEC), and other storage mechanisms and protocols.

Sentinel Log Manager supports all event sources if there are suitable Connectors to parse data from those event sources. Novell Sentinel Log Manager provides Collectors for many event sources. The Generic Event Collector collects and processes data from unrecognized event sources that have suitable connectors.

You can configure the event sources for data collection by using the Event Source Management interface.

For a complete list of supported event sources, see [Section 2.6, “Supported Event Sources,” on page 23](#).

1.1.2 Event Source Management

The Event Source Management interface enables you to import and configure the Sentinel 6.0 and 6.1 Connectors and Collectors.

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

- ◆ Add or edit connections to event sources by using Configuration wizards.
- ◆ View real-time status of connections to event sources.

- ◆ Import or export configuration of event sources to or from the Live View.
- ◆ View and configure Connectors and Collectors installed with Sentinel.
- ◆ Import or export Connectors and Collectors from or to a centralized repository.
- ◆ Monitor data flowing through the configured Collectors and Connectors.
- ◆ View the raw data information.
- ◆ Design, configure, and create the components of the Event Source hierarchy, and execute required actions by using these components.

For more information, see to the Event Source Management section of the *Sentinel User Guide* (<http://www.novell.com/documentation/sentinel61/#admin>).

1.1.3 Data Collection

Novell Sentinel Log Manager collects data from configured event sources with the help of Connectors and Collectors.

Collectors are scripts that parse the data from a variety of event sources into the normalized Sentinel event structure, or in some cases collect other forms of data from external data sources. Each Collector should be deployed with a compatible Connector. Connectors facilitate the connectivity between Sentinel Log Manager Collectors and event or data sources.

Novell Sentinel Log Manager provides enhanced Web-based user interface support for syslog and Novell Audit to easily collect logs from different event sources.

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

- ◆ The Syslog Connector automatically accepts and configures syslog data sources that send data over the User Datagram Protocol (UDP), the Transmission Control Protocol (TCP), or the secure Transport Layer System (TLS).
- ◆ The Audit Connector automatically accepts and configures audit-enabled Novell data sources.
- ◆ The File Connector reads log files.
- ◆ The SNMP Connector receives SNMP traps.
- ◆ The JDBC Connector reads from database tables.
- ◆ The WMS Connector accesses Windows event logs on desktops and servers.
- ◆ The SDEE Connector connects to devices that support the SDEE protocol such as the Cisco devices.
- ◆ Check Point Log Export API (LEA) Connector facilitates integration between Sentinel Collectors and Check Point firewall servers.
- ◆ The Sentinel Link Connector accepts data from other Novell Sentinel Log Manager servers.
- ◆ The 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) (<http://support.novell.com>).

For more information on configuring Connectors, see the Connector documents at the [Sentinel Plugins Web site](http://support.novell.com/products/sentinel/secure/sentinelplugins.html) (<http://support.novell.com/products/sentinel/secure/sentinelplugins.html>).

For more information on configuring data collection, see “[Configuring Data Collection](#)” in the *Sentinel Log Manager 1.2.2 Administration Guide*.

NOTE: You must always download and import the latest version of the Collectors and Connectors. Updated Collectors and Connectors are posted to the [Sentinel 6.1 Plug-ins Web site \(http://support.novell.com/products/sentinel/secure/sentinelplugins.html\)](http://support.novell.com/products/sentinel/secure/sentinelplugins.html) on a regular basis. Updates to Connectors and Collectors include fixes, support for additional events, and performance improvements.

1.1.4 Collector Manager

The Collector Manager provides a flexible data collection point for Sentinel Log Manager. The Novell Sentinel Log Manager installs a Collector Manager by default during installation. However, you can remotely install Collector Managers at suitable locations in your network. These remote Collector Managers run Connectors and Collectors and forward the collected data to Novell Sentinel Log Manager for storage and processing.

For information on installing additional Collector Managers, see [“Installing Additional Collector Managers” on page 58](#).

1.1.5 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 the collected device log data, and a PostgreSQL database to keep Novell Sentinel Log Manager configuration data.

The data is stored in a compressed format on the server file system and then stored in a configured location for long-term storage. The data can be stored either locally or on a remotely mounted SMB (CIFS) or NFS share. Data files are deleted from the local and networked storage locations based on the schedule configured in the data retention policy.

You can configure data retention policies to delete data from the storage location if the data retention time limit exceeded for that particular data or if the available space is reduced below a specified disk space value.

For more information on configuring data storage, see [“Configuring Data Storage”](#) in the *Sentinel Log Manager 1.2.2 Administration Guide*.

1.1.6 Searching and Reporting

The searching and reporting components help you to search and report the event log data in both local and networked data storage and indexing systems. The stored event data can be searched either generically or against specific event fields such as source username. These search results can be further refined or filtered and saved as a report template for future use.

The Sentinel Log Manager comes with preinstalled reports. You can also upload additional reports. You can run reports on a schedule or whenever it is necessary.

For information on list of default reports, see [“Reporting”](#) in the *Sentinel Log Manager 1.2.2 Administration Guide*.

For information on searching events and generating reports, see [“Searching Events”](#) and [“Reporting”](#) in the *Sentinel Log Manager 1.2.2 Administration Guide*.

1.1.7 Sentinel Link

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-fledged 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.

1.1.8 Web-Based User Interface

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

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. (administrators only)
- ◆ Configure data forwarding (administrators only)
- ◆ Download the Sentinel Collector Manager installer for remote installation (administrators only)
- ◆ 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)

1.2 Installation Overview

Novell Sentinel Log Manager can be installed either as an appliance or on an existing SUSE Linux Enterprise Server (SLES) 11 SP1 operating system. When Sentinel Log Manager is installed as an appliance, the Log Manager server is installed on a SLES 11 SP1 operating system.

The Novell Sentinel Log Manager installs the following components by default:

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

Some of these components require additional configuration.

The Novell Sentinel Log Manager installs a Collector Manager by default. If you want additional Collector Managers, you can install them separately on remote machines. For more information, see [Chapter 7, "Installing Additional Collector Managers,"](#) on page 57.

2 System Requirements

The following sections describe the hardware, operating system, browser, supported Connectors, and event source compatibility requirements for Novell Sentinel Log Manager.

- ◆ [Section 2.1, “Hardware Requirements,” on page 17](#)
- ◆ [Section 2.2, “Supported Operating Systems,” on page 21](#)
- ◆ [Section 2.3, “Supported Browsers,” on page 22](#)
- ◆ [Section 2.4, “Supported Virtual Environment,” on page 22](#)
- ◆ [Section 2.5, “Supported Connectors,” on page 23](#)
- ◆ [Section 2.6, “Supported Event Sources,” on page 23](#)
- ◆ [Section 2.7, “Recommended Limits,” on page 25](#)
- ◆ [Section 2.8, “Search and Reports Performance,” on page 27](#)

2.1 Hardware Requirements

- ◆ [Section 2.1.1, “Sentinel Log Manager Server,” on page 17](#)
- ◆ [Section 2.1.2, “Collector Manager System,” on page 18](#)
- ◆ [Section 2.1.3, “Data Storage Requirement Estimation,” on page 19](#)
- ◆ [Section 2.1.4, “Disk I/O Utilization Estimation,” on page 20](#)
- ◆ [Section 2.1.5, “Network Bandwidth Utilization Estimation,” on page 21](#)
- ◆ [Section 2.1.6, “Virtual Environment,” on page 21](#)

2.1.1 Sentinel Log Manager Server

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

The following table lists the hardware requirements that are recommended for a production system that holds 90 days of online data. The recommended requirements are for an average event size of 300 bytes.

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

Requirements	Sentinel Log Manager (500 EPS)	Sentinel Log Manager (2500 EPS)	Sentinel Log Manager (7500 EPS)
Maximum Event Rate	500	2500	7500
CPU	One Intel Xeon E5450 3-GHz (4 core) CPU or Two Intel Xeon L5240 3-(2 core) CPUs (4 cores total)	One Intel Xeon E5450 3-GHz (4 core) CPU or Two Intel Xeon L5240 3-(2 core) CPUs (4 cores total)	Two Intel Xeon X5470 3.33-GHz (4 core) CPUs (8 cores total)
Random Access Memory (RAM)	4 GB	4 GB	8 GB
Local Storage (30 days)	2 x 500 GB, 7.2k RPM drives (Hardware RAID with 256 MB cache, RAID 1)	4 x 1 TB, 7.2k RPM drives (Hardware RAID with 256 MB cache, RAID 10)	16 x 600 GB, 15k RPM drives, (Hardware RAID with 512 MB cache, RAID 10) or an equivalent storage area network (SAN)
Networked Storage (90 days)	600 GB	2 TB	5.8 TB

Follow these guidelines for optimal system performance:

- ◆ The local storage should have enough space to hold at least 5 days worth of data, which includes both event data and raw data. For more details on calculating the data storage requirements, see [Section 2.1.3, “Data Storage Requirement Estimation,” on page 19](#).
- ◆ Networked storage contains all 90 days worth of data, including a fully compressed copy of the event data in local storage. A copy of the event data is kept on local storage for search and reporting performance reasons. The local storage size can be decreased if storage size is a concern. However, due to decompression overhead, there will be an estimated 70% decrease in searching and reporting performance on data that would otherwise be in local storage.
- ◆ You must set up the networked storage location to an external multi-drive SAN or network-attached storage (NAS).
- ◆ One machine can include more than one event source. For example, a Windows server can include two Sentinel event sources because you want to collect data from the Windows operating system and also the SQL Server database hosted on that machine.
- ◆ 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.
- ◆ Maximum event source limits are not hard limits, but, are recommendations based on the performance testing done by Novell and assume a low average events rate per second per event source (less than 3 EPS). Higher EPS rates result in lower sustainable maximum event sources. You can use the equation (maximum event sources) × (average EPS per event source) = maximum event rate to arrive at the approximate limits for your specific average EPS rate or number of event sources, as long as the maximum number of event sources does not exceed the limit indicated above.

2.1.2 Collector Manager System

- One Intel Xeon X5570 2.93-GHz (4 CPU cores)

- ❑ 4 GB RAM
- ❑ 10 GB free disk space

2.1.3 Data Storage Requirement Estimation

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 networked storage space. However, storage requirements might become significant over a long period of time.

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. For instructions on employing this hybrid approach, see [“Using Sequential-Access Storage for Long Term Data Storage”](#) in the *Sentinel Log Manager 1.2.2 Administration Guide*.

To determine the amount of random-access storage space required for Sentinel Log Manager, first estimate how many days 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 the Server Message Block (SMB) protocol or CIFS protocol, the network file system (NFS), or a SAN for Sentinel Log Manager to use for archiving data.

You should also have the following 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:

- ◆ **Local event storage (partially compressed):** {average byte size per event} x {number of days} x {events per second} x 0.00007 = Total GB storage required

Event sizes typically range from 300-1000 bytes.

- ◆ **Networked event storage (fully compressed):** {average byte size per event} x {number of days} x {events per second} x 0.00002 = Total GB storage required
- ◆ **Raw Data Storage (fully compressed on both local and networked storage):** {average byte size per raw data record} x {number of days} x {events per second} x 0.000012 = Total GB storage required

A typical average raw data size for syslog messages is 200 bytes.

- ◆ **Total local storage size (with networked storage enabled):** {Local event storage size for desired number of days} + {Raw data storage size for one day} = Total GB storage required

If networked storage is enabled, event data is moved to networked storage when local storage fills up. Raw data, however, is located on the local storage only temporarily before it is moved to networked storage. It typically takes less than a day to move the raw data from local storage to networked storage.

- ◆ **Total local storage size (with networked storage disabled):** {Local event storage size for retention time} + {Raw data storage size for retention time} = Total GB storage required

- ◆ **Total networked storage size:** {Networked event storage size for retention time} + {Raw data storage size for retention time} = Total GB storage required

NOTE:

- ◆ The coefficients in each formula represent ((seconds per day) x (GB per byte) x compression ratio).
 - ◆ These numbers are only estimates and depend on the size of the event data as well as on the size of compressed data.
 - ◆ Partially compressed means that the data is compressed, but the index of the data is not compressed. Fully compressed means that both the event data and index data is compressed. Event Data compression rates are typically 10:1. Index compression rates are typically 5:1. The index is used to optimize searching through the data.
-

You can also use the above formulas to determine how much storage space is required for a long-term data storage system such as tape.

2.1.4 Disk I/O Utilization Estimation

Use the following formulas to estimate the amount of disk utilization on the server at various EPS rates.

- ◆ **Data written to Disk (Kilobytes per second):** (average event size in bytes + average raw data size in bytes) x (events per second) x .004 compression coefficient = data written per second to disk

For example, at 500 EPS, for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, data written to disk is determined as follows:

$$(464 \text{ bytes} + 300 \text{ bytes}) \times 500 \text{ EPS} \times .004 = 1558 \text{ KB}$$

- ◆ **Number of I/O request to the Disk (transfers per second):** (average event size in bytes + average raw data size in bytes) x (events per second) x .00007 compression coefficient = I/O requests per second to disk

For example, at 500 EPS, for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, number of I/O requests per second to the disk is determined as follows:

$$(464 \text{ bytes} + 300 \text{ bytes}) \times 500 \text{ EPS} \times .00007 = 26 \text{ tps}$$

- ◆ **Number of blocks written per second to the disk:** (average event size in bytes + average raw data size in bytes) x (events per second) x .008 compression coefficient = Blocks written per second to disk

For example, at 500 EPS, for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, number of blocks written per second to the disk is determined as follows:

$$(464 \text{ bytes} + 300 \text{ bytes}) \times 500 \text{ EPS} \times .008 = 3056$$

- ◆ **Data read per second from disk when performing a Search:** (average event size in bytes + average raw data size in bytes) x (number of events matching query in millions) x .013 compression coefficient = kilobytes read per second from disk

For example, at 3 millions of events matching the search query, for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, data read per second from disk is determined as follows:

$$(464 \text{ bytes} + 300 \text{ bytes}) \times 3 \times .013 = 300 \text{ KB}$$

2.1.5 Network Bandwidth Utilization Estimation

Use the following formulas to estimate the network bandwidth utilization on the server at various EPS rates:

{average event size in bytes + average raw data size in bytes} x {events per second} x .0003
compression coefficient = network bandwidth in Kbps (kilobits per second)

For example, at 500 EPS for an average event size of 464 bytes and an average raw data size of 300 bytes in the log file, the network bandwidth utilization is determined as follows:

$(464 \text{ bytes} + 300 \text{ bytes}) \times 500 \text{ EPS} \times .0003 = 115 \text{ Kbps}$

2.1.6 Virtual Environment

Sentinel Log Manager is extensively tested and fully supported on a VMware ESX server. To achieve comparable performance results to the physical-machine testing results on ESX or in any other virtual environment, the virtual environment should provide the same memory, CPUs, disks pace, and I/O as the physical machine recommendations.

For information on physical machine recommendations, see [Section 2.1, "Hardware Requirements," on page 17](#).

2.2 Supported Operating Systems

Novell supports Sentinel Log Manager on the operating systems described in this section. Novell also supports Sentinel Log Manager on systems with minor updates to these operating systems, such as security patches or hotfixes. However, running Sentinel Log Manager on systems with major updates to these operating systems is not supported until Novell has tested and certified those updates.

- ♦ [Section 2.2.1, "Sentinel Log Manager," on page 21](#)
- ♦ [Section 2.2.2, "Collector Manager," on page 21](#)

2.2.1 Sentinel Log Manager

- 64-bit SUSE Linux Enterprise Server 11 SP3.
- A high-performing file system.

NOTE: All Novell testing is done with the ext3 file system.

2.2.2 Collector Manager

You can install additional Collector Managers on the following operating systems:

- ♦ ["Linux" on page 21](#)
- ♦ ["Windows" on page 22](#)

Linux

- SUSE Linux Enterprise Server 11 SP3 (64-bit)

Windows

- Windows Server 2003 (32-bit and 64-bit)
- Windows Server 2003 SP2 (32-bit and 64-bit)
- Windows Server 2003 R2 (32-bit and 64-bit)
- Windows Server 2008 (64-bit)
- Windows Server 2008 R2 (64-bit)

2.3 Supported Browsers

The Sentinel Log Manager interface is optimized for viewing at 1280 x 1024 or higher resolution in the following supported browsers:

- ♦ [Section 2.3.1, "Linux," on page 22](#)
- ♦ [Section 2.3.2, "Windows," on page 22](#)

2.3.1 Linux

- Mozilla Firefox 5 and later

2.3.2 Windows

- Mozilla Firefox 5 and later
- Microsoft Internet Explorer 8 and 11*

* See ["Prerequisites for Internet Explorer" on page 22](#).

Prerequisites for Internet Explorer

- ♦ If the Internet Security Level is set to High, only a blank page appears after logging in to Sentinel Log Manager. To work around this issue, navigate to *Tools > Internet Options > Security tab > Trusted Sites*. Click the *Site* button and add the Sentinel Log Manager Web site to the list of trusted sites.
- ♦ Make sure that the *Tools > Compatibility View* option is not selected.
- ♦ If the *Automatic Prompting for File Downloads* option is not enabled, the file download pop-up might be blocked by the browser. To work around this issue, navigate to *Tools > Internet Options > Security tab > Custom Level*, then scroll down to the download section and select *Enable* to enable the *Automatic Prompting for File Downloads* option.

2.4 Supported Virtual Environment

- VMware ESX/ESXi 3.5/4.0 or higher
- VMPlayer 3 (for demo only)
- Xen 3.1.1

2.5 Supported Connectors

The Sentinel Log Manager supports all Connectors that are supported by Sentinel and Sentinel RD.

- 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
- Mainframe Connector
- SAP Connector

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

2.6 Supported Event Sources

Sentinel Log Manager supports a variety of devices and applications, including intrusion detection systems, firewalls, operating systems, routers, Web servers, databases, switches, mainframes, and antivirus event sources. The data from these event sources is parsed and normalized to varying degrees depending on whether the data is processed by using the generic event Collector that puts the entire payload of the event into a common field, or by using a device-specific Collector that parses the data into individual fields.

The following event sources are supported by 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 \(http://download.novell.com/Download?buildid=RH_B5b3M6EQ~\)](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. When this is done, these event sources appear in the Sentinel Log Manager Web interface > *collection* > *Event Sources*.

Collectors supporting additional event sources can either be obtained from the [Sentinel Plug-ins Web site](http://support.novell.com/products/sentinel/secure/sentinelplugins.html) (<http://support.novell.com/products/sentinel/secure/sentinelplugins.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) (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

2.7 Recommended Limits

The limits mentioned in this section are recommendations based on the performance testing done at Novell or at customer sites. They are not hard-limits. The recommendations are approximations. In highly dynamic systems, it is a good practice to build in buffers and allow room for growth.

- ♦ [Section 2.7.1, “Collector Manager Limits,” on page 25](#)
- ♦ [Section 2.7.2, “Reports Limits,” on page 26](#)
- ♦ [Section 2.7.3, “Actions EPS Limits,” on page 26](#)
- ♦ [Section 2.7.4, “SLES Open Files Limits,” on page 27](#)

2.7.1 Collector Manager Limits

Unless otherwise specified, Collector Manager limits assume 4 CPU cores at 2.2 GHz each, 4 GB of RAM, running on SLES 11.

Table 2-2 *Collector Manager Performance Numbers*

Attribute	Limits	Comments
Maximum number of Collector Managers	20	This limit assumes each Collector Manager is running at low EPS (e.g, less than 100 EPS). The limit decreases as the events per second increase.
Maximum number of Connectors (fully utilized) on a single Collector Manager	1 per CPU core, with at least 1 CPU core reserved for the operating system and other processing	A fully utilized Connector is one that is running at the highest EPS possible for that type of Connector.
Maximum number of Collectors (fully utilized) on a single Collector Manager	1 per CPU core, with at least 1 CPU core reserved for the operating system and other processing	A fully utilized Collector is one that is running at the highest EPS possible for that type of Collector.

Attribute	Limits	Comments
Maximum number of event sources on a single Collector Manager	2000	The limit of the Sentinel Log Manager server is either 1000 or 2000, depending on the hardware. If the server limit is reached on a single Collector Manager, then the limit of event sources for the overall Sentinel system has been reached with that single Collector Manager.
Maximum number of event sources per Sentinel Log Manager server instance	2000	

2.7.2 Reports Limits

Table 2-3 Reports Performance Numbers

Attribute	Limits	Comments
Maximum number of saved reports	200	
Maximum number of reports running simultaneously	3	The limit assumes that the server is not already highly utilized performing data collection or other tasks.

2.7.3 Actions EPS Limits

Unless otherwise specified, the Actions EPS limits assume that one action is configured per rule.

Table 2-4 Actions Performance Numbers

Action	EPS per Action
Sentinel Link	300
Log to File	30 - 50
Send an email	40
Log to Syslog	5 - 10
Execute Script	5 - 10

2.7.4 SLES Open Files Limits

In systems with a large number of event sources (for example, more than 75), with the majority using the File Connector and the offset set to the beginning of the file, the SLES open files limit might not be the same as the number of files currently open in the system. This might lead to performance issues on Sentinel Log Manager.

To avoid this issue, you can set the soft and hard limits for the maximum number of open files based on the number of files that are open.

Perform the following steps to set the open file limits:

- 1 Log in to the system as novell user.
- 2 View the number of files that are open for the sentinel (novell) user.

```
lsof | wc -l
```

- 3 View the hard and soft limits:

```
ulimit -Hn
```

```
ulimit -Sn
```

Based on the number of open files, the file descriptor limits in the `/etc/security/limits.conf` file can be set. For example, if the number of open files is 1000, the limits can be set to 2000.

NOTE: Only the root user can edit the `/etc/security/limits.conf` file.

- 4 Ensure that root user sets the file descriptor limits as follows:

```
novell soft nofile 2000
```

```
novell hard nofile 2000
```

NOTE: Setting the soft limits is optional, however, setting the hard limits is mandatory.

- 5 Save the changes.

2.8 Search and Reports Performance

The performance of Sentinel Log Manager can vary depending on your environment, configuration, and hardware. Novell has done in depth performance testing on the Sentinel Log Manager system to validate and verify the quality attributes of the system, such as scalability, reliability, and resource usage.

- ♦ [Section 2.8.1, “Search Response and Completion Speed,” on page 27](#)
- ♦ [Section 2.8.2, “Report Generation Speed,” on page 28](#)

2.8.1 Search Response and Completion Speed

Several tests were carried out with the following configuration to determine the duration taken for a search to return initial data:

- ♦ **Hardware:** 4 CPU cores at 2.93GHz each, 4 GB of RAM, running on SLES 11
- ♦ **EPS rate:** Incoming EPS rate while performing the search is at 2000
- ♦ **Data Storage:** All the event data in time range is in the local storage

The following are the observations:

Table 2-5 Search Performance Results

Total events	Number of events matching the Search query	Time for Initial Search Results
10,000,000	1,000 - 10,000,000	5 - 10 seconds
100,000,000	20,000,000 - 100,000,000	10 – 30 seconds
200,000,000	110,000,000 - 200,000,000	1 – 5 minutes

2.8.2 Report Generation Speed

Several tests were carried out with the following configuration to determine the duration taken for report generation.

- ♦ **Hardware:** 4 CPU cores at 2.93GHz each, 4 GB of RAM, running on SLES 11
- ♦ **EPS rate:** Incoming EPS rate while performing the search is at 2000
- ♦ **Location of the data:** All the event data in time range is in the local storage

The following are the observations:

Table 2-6 Reports Performance Results

Total events	Number of events matching the Search query	Time for Report Generation
10,000,000	1,000 - 10,000,000	1 - 2 minutes
100,000,000	20,000,000 - 100,000,000	10 – 50 minutes
200,000,000	110,000,000 - 200,000,000	1 – 3 hours

NOTE: For reports with large number of events and large number of fields, such as the Event Details report, the report generation might take a long time and the system might run out of memory. To improve the reports performance results, you can increase the RAM in your system.

3 Installing on an Existing SLES 11 SP1 System

The section describes the procedure to install Sentinel Log Manager on an existing SUSE Linux Enterprise Server (SLES) 11 SP1 system by using the application installer. You can install the Sentinel Log Manager server in several ways: the standard installation procedure, the custom installation procedure, or the silent installation procedure where the installation proceeds without user input and uses the default values. You can also install Sentinel Log Manager as a non-root user.

If you choose the custom installation method, you have the option to install the product with a license key and also select an authentication option. You can set up LDAP authentication for Sentinel Log Manager in addition to the database authentication. When you configure Sentinel Log Manager for LDAP authentication, users can log in to the server by using their Novell eDirectory or Microsoft Active Directory credentials.

If you want to install multiple Sentinel Log Manager servers in your deployment, you can record the installation options in a configuration file and then use the file to run an unattended installation. See [Section 3.4, “Silent Installation,” on page 34](#) for more information.

- ◆ [Section 3.1, “Before You Begin,” on page 29](#)
- ◆ [Section 3.2, “Standard Installation,” on page 30](#)
- ◆ [Section 3.3, “Custom Installation,” on page 32](#)
- ◆ [Section 3.4, “Silent Installation,” on page 34](#)
- ◆ [Section 3.5, “Non-Root Installation,” on page 34](#)

3.1 Before You Begin

- ◆ Make sure that your hardware and software meet the minimum requirements mentioned in [Chapter 2, “System Requirements,” on page 17](#).
- ◆ Ensure that the `libstdc++33-32-bit` rpm is installed. You can install this rpm either by using Ya ST or by using the `zypper` command:

```
zypper in libstdc++33-32bit
```

- ◆ For Sentinel Log Manager 1.2 and later to work successfully on SLES 11 SP1, the following RPMs or a later version must be installed:
 - ◆ **Kernel patches:**
 - ◆ `kernel-default-2.6.32.29-0.3.1.x86_64.rpm`
 - ◆ `kernel-default-base-2.6.32.29-0.3.1.x86_64.rpm`
 - ◆ **Linux util RPMs:**
 - ◆ `libblkid1-2.16-6.11.1.x86_64.rpm`
 - ◆ `libuuid1-2.16-6.11.1.x86_64.rpm`

- ◆ util-linux-2.16-6.11.1.x86_64.rpm
- ◆ util-linux-lang-2.16-6.11.1.x86_64.rpm
- ◆ uuid-runtime-2.16-6.11.1.x86_64.rpm

Sentinel Log Manager 1.1.0.x uses squashfs version 3.4-35.1; however SLES 11 SP1 supports squashfs 4.0 and later, which is not backward compatible and cannot open a squashed file system created with previous squashfs versions. Installing these RPMs fixes the incompatibility issue between the squashfs versions of Sentinel Log Manager 1.1.0.x and SLES 11 SP1.

These RPMs are available through the SLES 11 online update channel. For more information on updating the SLES system, see “YaST Online Update” (http://www.novell.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html) in the *SLES 11 SP1 Administration Guide* (http://www.novell.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html).

NOTE: The installation does not proceed unless the above mentioned kernel patches and Linux util rpms are installed.

- ◆ Configure the operating system in such a way that the `hostname -f` command returns a valid hostname.
- ◆ Obtain your license key from the [Novell Customer Care Center](https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22) (https://secure-www.novell.com/center/ICSLogin/?%22https://secure-www.novell.com/center/regadmin/jsps/home_app.jsp%22), to install the licensed version.
- ◆ Synchronize time by using the Network Time Protocol (NTP).
- ◆ Install the following operating system commands:
 - ◆ mount
 - ◆ umount
 - ◆ id
 - ◆ df
 - ◆ du
 - ◆ sudo
- ◆ Make sure that the following ports are opened on the firewall:
TCP 8080, TCP 8443, TCP 61616, TCP 10013, TCP 1289, TCP 1468, TCP 1443, and UDP 1514
For more information on what these ports are used for, see [Section 4.2, “Ports Used,” on page 37](#).

3.2 Standard Installation

The standard installation procedure installs Sentinel Log Manager with a 60-day evaluation license and installs all the features except the Data Restoration feature.

- 1 Download and copy the install files from the Novell Download site.
- 2 Log in as `root` to the server where you want to install Sentinel Log Manager.
- 3 Specify the following command to extract the install files from the tar file:

```
tar xfz <install_filename>
```

Replace `<install_filename>` with the actual name of the install file.

- 4 Change to the directory where the install file is extracted.
- 5 Specify the following command to run the `install-slm` script to install Sentinel Log Manager:

```
./install-slm
```

If you want to install Sentinel Log Manager on more than one system, you can record your installation options in a file. You can use this file to install Sentinel Log Manager on other systems unattended. To record your installation options, specify the following command:

```
./install-slm -r responseFile
```

- 6 To proceed with a language of your choice, select the number specified next to the language. The end user license agreement is displayed in the selected language.
- 7 Read the end user license and enter *yes* or *y* to accept the license and continue with the installation.
The installation starts installing all RPM packages. This installation might take a few seconds to complete.
The installation creates a *novell* group and a *novell* user, if they do not already exist.
- 8 When prompted, specify the option to proceed with standard installation.
Installation proceeds with the 60-day evaluation license key included with the installer. This license key activates the full set of product features for a 60-day trial period except for the Data Restoration feature. At any time during or after the trial period, you can add the evaluation license with a license key you have purchased.
- 9 Specify the password for the administrator user.
- 10 Confirm the password for the administrator user.
The installer selects the *Authenticate to database only* method and proceeds with the installation.
The Sentinel Log Manager installation completes and the server starts. It might take about 5-10 minutes for all services to start up after installation as the system performs a one time initialization. Wait for this duration before you log in to the server.
- 11 To log in to the Sentinel Log Manager server, use the URL specified in the installation output. The URL is similar to `https://10.0.0.1:8443/novelllogmanager`.
For more information on logging in to the server, see [Chapter 6, "Logging In to the Web Interface,"](#) on page 55.
- 12 To configure event sources to send data to Sentinel Log Manager, see ["Configuring Data Collection"](#) in the *Sentinel Log Manager 1.2.2 Administration Guide*.

NOTE: When you start the system for the first time after installation, it might take approximately five minutes for the system to initialize before you can start using it. This delay only occurs when you start the system for the first time after the installation or an update.

3.3 Custom Installation

If you choose the custom installation method, you have the option to install the product with a license key and also select an authentication option. You can set up LDAP authentication for Sentinel Log Manager in addition to the database authentication. When you configure Sentinel Log Manager for LDAP authentication, users can log in to the server by using the LDAP directory credentials.

If you do not configure the Sentinel Log Manager for LDAP authentication during the installation process, you can configure authentication after the installation, if necessary. To set up LDAP authentication after installation, see “[LDAP Authentication](#)” in the *Sentinel Log Manager 1.2.2 Administration Guide*.

- 1 Download and copy the install files from the Novell Download site.
- 2 Log in as `root` to the server where you want to install Sentinel Log Manager.
- 3 Specify the following command to extract the install files from the tar file:

```
tar xfz <install_filename>
```

Replace `<install_filename>` with the actual name of the install file.

- 4 Change to the directory where the install file is extracted.
- 5 Specify the following command to run the `install-slm` script to install Sentinel Log Manager:

```
./install-slm
```

- 6 To proceed with a language of your choice, select the number specified next to the language. The end user license agreement is displayed in the selected language.

- 7 Read the end user license and enter `yes` or `y` to accept the license and continue with the installation.

The installation starts installing all RPM packages. This installation might take a few seconds to complete.

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

- 8 When prompted, specify the option to proceed with the custom installation.
- 9 When prompted to specify the license key option, enter `2` to specify the license key for the purchased product.
- 10 Specify the license key, then press Enter.

For more information about license keys, see “[License Information](#)” in the *Sentinel Log Manager 1.2.2 Administration Guide*.

- 11 Specify the password for the administrator user.
- 12 Confirm the password for the administrator user.
- 13 Specify the password for the database administrator (`dbauser`).
- 14 Confirm the password for the database administrator (`dbauser`).
- 15 You can configure any valid port number within the specified range for the following services:
 - ♦ Web Server
 - ♦ Java Message Service
 - ♦ Client Proxy Service
 - ♦ Database Service
 - ♦ Agent Internal Gateway

If you want to proceed with the default ports, enter option 6 to continue with the custom installation.

- 16 Specify the option to authenticate users through an external LDAP directory.
- 17 Specify the IP address or the hostname of the LDAP server.

The default value is localhost. However, you should not install the LDAP server on the same machine as the Sentinel Log Manager server.
- 18 Select one of the following LDAP connection types:
 - ◆ **SSL/TSL LDAP connection:** Establishes a secured connection between the browser and the server for the authentication. Enter 1 to specify this option.
 - ◆ **Unencrypted LDAP connection:** Establishes an unencrypted connection. Enter 2 to specify this option.
- 19 Specify the LDAP server port number. The default SSL port is 636 and the default non SSL port is 389.
- 20 (Conditional) If you selected SSL/TSL LDAP connection, specify whether the LDAP server certificate is signed by a well known CA.
- 21 (Conditional) If you specified `n`, specify the filename of the LDAP server certificate.
- 22 Select whether you want to perform anonymous searches on the LDAP directory:
 - ◆ **Perform anonymous searches on the LDAP directory:** Sentinel Log Manager server performs an *anonymous search* on the LDAP directory based on the specified user name to fetch the corresponding LDAP user distinguished name (DN). Enter 1 to specify this method.
 - ◆ **Do not perform anonymous searches on the LDAP directory:** Enter 2 to specify this option.
- 23 (Conditional) If you selected anonymous search, specify the search attribute and move to [Step 26](#).
- 24 (Conditional) If you did not select anonymous search in [Step 22](#), specify whether you are using Microsoft Active Directory.

For Active Directory, the `userPrincipalName` attribute whose value is of the form `userName@domainName` can be optionally used to authenticate the user before searching for the LDAP user object, with out the need to enter user DN.
- 25 (Conditional) If you want to use the above approach for Active Directory, specify the domain name.
- 26 Specify the Base DN.
- 27 Press `y` to specify that the options provided are correct, else press `n` and change the configuration.
- 28 To log in to the Sentinel Log Manager server, use the URL specified in the installation output. The URL is similar to `https://10.0.0.1:8443/novelllogmanager`.

For more information on logging in to the server, see [Chapter 6, “Logging In to the Web Interface,”](#) on page 55.
- 29 To configure event sources to send data to Sentinel Log Manager, see [“Configuring Data Collection”](#) in the *Sentinel Log Manager 1.2.2 Administration Guide*.

NOTE: When you start the system for the first time after installation, it might take approximately five minutes for the system to initialize before you can start using it. This delay only occurs when you start the system for the first time after the installation or an update.

3.4 Silent Installation

The silent or unattended installation of Sentinel Log Manager is useful if you need to install more than one Sentinel Log Manager servers in your deployment. In such a scenario, you can record the installation parameters during the first installation and then run the recorded file on all the other servers.

- 1 Download and copy the install files from the Novell Download site.
- 2 Log in as `root` to the server where you want to install Sentinel Log Manager.
- 3 Specify the following command to extract the install files from the tar file:

```
tar xfz <install_filename>
```

Replace `<install_filename>` with the actual name of the install file.

- 4 Change to the directory where the install file is extracted.
- 5 Specify the following command to run the `install-slm` script to install Sentinel Log Manager in a silent mode:

```
./install-slm -u responseFile
```

For information on creating the response file, see [Section 3.2, “Standard Installation,” on page 30](#). The installation proceeds with the values stored in the response file.

- 6 To log in to the Sentinel Log Manager server, use the URL specified in the installation output. The URL is similar to `https://10.0.0.1:8443/novelllogmanager`.

For more information on logging in to the server, see [Chapter 6, “Logging In to the Web Interface,” on page 55](#).

- 7 To configure event sources to send data to Sentinel Log Manager, see [“Configuring Data Collection” in the “Sentinel Log Manager 1.2.2 Administration Guide”](#).

NOTE: When you start the system for the first time after installation, it might take approximately five minutes for the system to initialize before you can start using it. This delay only occurs when you start the system for the first time after the installation or an update.

3.5 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 non-root (`novell`) user.

- 1 Download and copy the install files from the Novell Download site.
- 2 Specify the following command to extract the install files from the tar file:

```
tar xfz <install_filename>
```

Replace `<install_filename>` with the actual name of the install file.

- 3 Log in as `root` to the server where you want to install Sentinel Log Manager as `root`.
- 4 Change to the directory where the install file is extracted.
- 5 Specify the following command:

```
./bin/root_install_prepare
```

A list of commands to be executed with root privileges is displayed.

This also creates a `novell` group and a `novell` user, if they do not already exist.

6 Accept the command list.

The displayed commands are executed.

7 Specify the following command to change to the newly created non-root (novell) user:

```
su novell
```

8 Specify the following command:

```
./install-slm
```

9 To proceed with a language of your choice, select the number specified next to the language.

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

10 Read the end user license and enter `yes` or `y` to accept the license and continue with the installation.

The installation starts installing all RPM packages. This installation might take a few seconds to complete.

11 You are prompted to specify the mode of installation.

- ◆ If you select to proceed with the standard installation, continue with [Step 8 in Section 3.2, “Standard Installation,” on page 30](#).
- ◆ If you select to proceed with the custom installation, continue with [Step 8 in Section 3.3, “Custom Installation,” on page 32](#).

The Sentinel Log Manager installation finishes and the server starts.

12 Specify the following command to change to the `root` user:

```
su root
```

13 Specify the following command to finish installation:

```
./bin/root_install_finish
```

14 To log in to the Sentinel Log Manager server, use the URL specified in the installation output. The URL is similar to `https://10.0.0.1:8443/novelllogmanager`.

For more information on logging in to the server, see [Chapter 6, “Logging In to the Web Interface,” on page 55](#).

NOTE: When you start the system for the first time after installation, it might take approximately five minutes for the system to initialize before you can start using it. This delay only occurs when you start the system for the first time after the installation or an update.

4 Installing the Appliance

Sentinel Log Manager Appliance is a ready to run software appliance built on SUSE Studio that combines a hardened SUSE Linux Enterprise Server (SLES) 11 SP1 operating system and Novell Sentinel Log Manager software integrated update service to provide an easy and seamless user experience as well as allow customers to leverage existing investments. The software appliance can be installed either on hardware or in a virtual environment.

- ♦ [Section 4.1, “Before You Begin,” on page 37](#)
- ♦ [Section 4.2, “Ports Used,” on page 37](#)
- ♦ [Section 4.3, “Installing the VMware Appliance,” on page 39](#)
- ♦ [Section 4.4, “Installing the Xen Appliance,” on page 40](#)
- ♦ [Section 4.5, “Installing the Appliance on Hardware,” on page 42](#)
- ♦ [Section 4.6, “Post-Installation Setup for the Appliance,” on page 43](#)
- ♦ [Section 4.7, “Configuring WebYaST,” on page 43](#)
- ♦ [Section 4.8, “Configuring the Appliance with SMT,” on page 44](#)
- ♦ [Section 4.9, “Stopping and Starting the Appliance by Using Web UI,” on page 46](#)
- ♦ [Section 4.10, “Registering for Updates,” on page 47](#)

4.1 Before You Begin

- ♦ Make sure that the hardware requirements are met. For more information, see [Section 2.1, “Hardware Requirements,” on page 17](#).
- ♦ Obtain your license key from the [Novell Customer Care Center \(http://www.novell.com/center\)](http://www.novell.com/center), to install the licensed version.
- ♦ Obtain your registration code from the [Novell Customer Care Center \(http://www.novell.com/center\)](http://www.novell.com/center) to register for software updates.
- ♦ Synchronize time by using the Network Time Protocol (NTP).
- ♦ (Conditional) If you are planning to use VMware, make sure that you have the VMware Converter to simultaneously upload the image to the VMware ESX server and convert it to a format that can run on the ESX server.

4.2 Ports Used

Note that Novell Sentinel Log Manager appliance uses the following ports for communication, and some of them are opened on the firewall:

- ♦ [Section 4.2.1, “Ports Opened in the Firewall,” on page 38](#)
- ♦ [Section 4.2.2, “Ports Used Locally,” on page 38](#)

4.2.1 Ports Opened in the Firewall

Table 4-1 Network Ports Used by Sentinel Log Manager

Ports	Description
TCP 1289	Used for Novell Audit connections.
TCP 289	Forwarded to 1289 for Novell Audit connections.
TCP 22	Used for secure shell access to the Sentinel Log Manager appliance.
UDP 1514	Used for syslog messages.
UDP 514	Forwarded to 1514 for syslog messages.
TCP 8080	Used for HTTP communication.
TCP 80	Forwarded to 8080 for the Sentinel Log Manager Web Server for HTTP communication.
TCP 8443	Used for HTTPS communication.
TCP 1443	Used for SSL encrypted syslog messages.
TCP 443	Forwarded to 8443 for the Sentinel Log Manager Web server for HTTPS communication. Also used by the Sentinel Log Manager Appliance for the update service.
TCP 61616	Used for communication between Collector Managers and the server.
TCP 10013	Used by the Event Source Management user interface SSL Proxy.
TCP 54984	Used by the Sentinel Log Manager appliance Management Console (WebYaST).
TCP 1468	Used for syslog messages.

4.2.2 Ports Used Locally

Table 4-2 Ports Used for Communication Locally

Ports	Description
TCP 61617	Used for internal communication between the Web server and the server.
TCP 5556	Used on the loop back interface for internal communication, with the internal_gateway_server and internal_gateway. It is used for communication between the agent engine and the Collector Manager.

Ports	Description
TCP 5432	Used for the PostgreSQL database. You do not need to open this port by default. However, if you are developing reports by using the Sentinel SDK, then you must open this port. For more information, see Sentinel Plug-in SDK Web site (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) .
Two additional randomly selected TCP ports	Used for internal communication between the agent engine and the Collector Manager.
TCP 8005	Used for internal communication with Tomcat processes.
TCP 32000	Used for internal communication between the agent engine and the Collector Manager.

4.3 Installing the VMware Appliance

To run the appliance image from the VMware ESX server, import and install the appliance image on the server.

- 1 Download the VMware appliance installation file.

The correct file for the VMware appliance has `vmx` in the filename. For example, `<sentinel_log_manager_vmx.tar.gz>`

- 2 Specify the following command to extract the compressed appliance image from the machine where VM Converter is installed:

```
tar zxvf <install_file>
```

Replace `<install_file>` with the actual file name.

- 3 To import the VMware image to the ESX server, use the VMware Converter and follow the on-screen instructions in the installation wizard.
- 4 Log in to the ESX server machine.
- 5 Select the imported VMware image of the appliance and click the *Power On* icon.
- 6 Select the language of your choice, then click *Next*.
- 7 Select the keyboard layout, then click *Next*.
- 8 Read and accept the Novell SUSE Enterprise Server Software License Agreement.
- 9 Read and accept the Novell Sentinel Log Manager End User License Agreement.
- 10 In the Hostname and Domain Name screen, specify the hostname and domain name. Ensure that the *Assign Hostname to Loopback IP* option is selected.
- 11 Select *Next*. The hostname configurations are saved.
- 12 Do one of the following:
 - ♦ To use the current network connection settings, select *Use the following configuration* in the *Network Configuration* screen.
 - ♦ To change the network connection settings, select *Change*.

- 13 Set the Time and Date, click *Next*, then click *Finish*.

NOTE: To change the NTP configuration after installation, use YaST from the appliance command line. You can use WebYaST to change the time and date, but not the NTP configuration.

If the time appears out of sync immediately after the install, run the following command to restart NTP:

```
rcntp restart
```

- 14 Set the Novell SUSE Enterprise Server `root` password, then click *Next*.
- 15 Set the `root` password, then click *Next*.
- 16 Set the Sentinel Log Manager admin password and the `dbauser` password, then click *Next*.
- 17 Select *Next*.

The installation proceeds and completes. Make a note of the appliance IP address that is shown in the console.

- 18 Proceed with [Section 4.6, "Post-Installation Setup for the Appliance,"](#) on page 43.

NOTE: When you start the system for the first time after installation, it might take approximately five minutes for the system to initialize before you can start using it. This delay only occurs when you start the system for the first time after the installation or an update.

4.4 Installing the Xen Appliance

- 1 Download and copy the Xen virtual appliance installation file to `/var/lib/xen/images`.
The correct filename for the Xen virtual appliance contains `xen`. For example,
`<sentinel_log_manager_xen.tar.gz>`

- 2 Specify the following command to unpack the file:

```
tar -xvzf <install_file>
```

Replace `<install_file>` with the actual name of the installation file.

- 3 Change to the new installation directory. This directory has the following files:

- ♦ `<file_name>.raw` image file
- ♦ `<file_name>.xenconfig` file

- 4 Open the `<file_name>.xenconfig` file by using a text editor.

- 5 Modify the file as follows:

Specify the full path to `.raw` file in the `disk` setting.

Specify the bridge setting for your network configuration. For example, `"bridge=br0"` or `"bridge=xenbr0"`.

Specify values for name and memory settings.

For example:

```
# -*- mode: python; -*-
name="Sentinel_Log_Manager_1.2.0.0_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/Sentinel_Log_Manager_1.2.0.0_64_Xen-
0.777.0/Sentinel_Log_Manager_1.2.0.0_64_Xen.x86_64-0.777.0.raw,xvda,w" ]
vif=[ "bridge=br0" ]
```


- 6 After you have modified the `<filename>.xenconfig` file, specify the following command to create the VM:

```
xm create <file_name>.xenconfig
```

- 7 (Optional) To verify if the VM is created, specify the following command:

```
xm list
```

The VM appears in the list.

For example, if you have configured `name="Sentinel_Log_Manager_1.2.0.0_64"` in the `.xenconfig` file, then the VM appears with that name.

- 8 To start the installation, specify the following command:

```
xm console <vm_name>
```

Replace `<vm_name>` with the name specified in the name setting of the `.xenconfig` file, which is also the value returned in [Step 7](#). For example:

```
xm console Sentinel_Log_Manager_1.2.0.0_64
```

- 9 Select the language of your choice, then click *Next*.
- 10 Select the keyboard layout, then click *Next*.
- 11 Read and accept the Novell SUSE Enterprise Server Software License Agreement.
- 12 Read and accept the Novell Sentinel Log Manager End User License Agreement.
- 13 In the Hostname and Domain Name screen, specify the hostname and domain name.
Ensure that the *Assign Hostname to Loopback IP* option is selected.
- 14 Select *Next*. The hostname configurations are saved.
- 15 Do one of the following:
- ◆ To use the current network connection settings, select *Use the following configuration* in the *Network Configuration* screen.
 - ◆ To change the network connection settings, select *Change*.
- 16 Set the Time and Date, click *Next*, then click *Finish*

NOTE: To change the NTP configuration after installation, use YaST from the appliance command line. You can use WebYast to change the time and date, but not the NTP configuration. If the time appears out of sync immediately after the install, run the following command to restart NTP:

```
rcntp restart
```

- 17 Set the Novell SUSE Enterprise Server root password, then click *Next*.
- 18 Set the Sentinel Log Manager admin password and dbauser password, then click *Next*.
The installation proceeds and completes. Make a note of the appliance IP address that is shown in the console.
- 19 Proceed with [Section 4.6, "Post-Installation Setup for the Appliance,"](#) on page 43.

NOTE: When you start the system for the first time after installation, it might take approximately five minutes for the system to initialize before you can start using it. This delay only occurs when you start the system for the first time after the installation or an update.

4.5 Installing the Appliance on Hardware

Before installing the appliance on the hardware, ensure that the appliance ISO disk image is downloaded from the support site, unpacked, and is available on a DVD.

- 1 Boot the physical machine from the DVD drive with the DVD.
- 2 Use the on-screen instructions of the installation wizard.
- 3 Run the Live DVD appliance image by selecting the top entry in the boot menu.
- 4 Read and accept the Novell SUSE Enterprise Server Software License Agreement.
- 5 Read and accept the Novell Sentinel Log Manager End User License Agreement.
- 6 Select *Next*.
- 7 In the Hostname and Domain Name screen, specify the hostname and domain name.
Ensure that the *Assign Hostname to Loopback IP* option is selected.
- 8 Select *Next*. The hostname configurations are saved.
- 9 Do one of the following:
 - ♦ To use the current network connection settings, select *Use the following configuration* in the Network Configuration screen.
 - ♦ To change the network connection settings, select *Change*.
- 10 Select *Next*. The network connection settings are saved.
- 11 Set the Time and Date, then click *Next*.

NOTE: To change the NTP configuration after installation, use YaST from the appliance command line. You can use WebYast to change the time and date, but not the NTP configuration. If the time appears out of sync immediately after the install, run the following command to restart NTP:

```
rcntp restart
```

- 12 Set the `root` password, then click *Next*.
- 13 Set the Sentinel Log Manager admin password and `dbauser` password, then click *Next*.
- 14 Enter the username and password at the console to log in to the appliance.
The default value for the username is `root` and the password is `password`.
- 15 Reset the terminal configurations:

```
reset
```
- 16 To install the appliance on the physical server, run the following command:

```
/sbin/yast2 live-installer
```

The installation proceeds and completes. Make a note of the appliance IP address that is shown in the console.
- 17 Proceed with [Section 4.6, “Post-Installation Setup for the Appliance,”](#) on page 43.

NOTE: When you start the system for the first time after installation, it might take approximately five minutes for the system to initialize before you can start using it. This delay only occurs when you start the system for the first time after the installation or an update.

4.6 Post-Installation Setup for the Appliance

- [Section 4.6.1, “Installing VMware Tools,”](#) on page 43
- [Section 4.6.2, “Logging in to the Appliance Web Interface,”](#) on page 43

4.6.1 Installing VMware Tools

For Sentinel Log Manager to work effectively on the VMware server, you need to install VMware Tools. VMware Tools is a suite of utilities that enhances the performance of the virtual machine’s operating system. It also improves management of the virtual machine. For more information on installing VMware Tools, see [VMware Tools for Linux Guests \(https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177\)](https://www.vmware.com/support/ws55/doc/ws_newguest_tools_linux.html#wp1127177).

For more information on the VMware documentation, see [Workstation User’s Manual \(http://www.vmware.com/pdf/ws71_manual.pdf\)](http://www.vmware.com/pdf/ws71_manual.pdf).

4.6.2 Logging in to the Appliance Web Interface

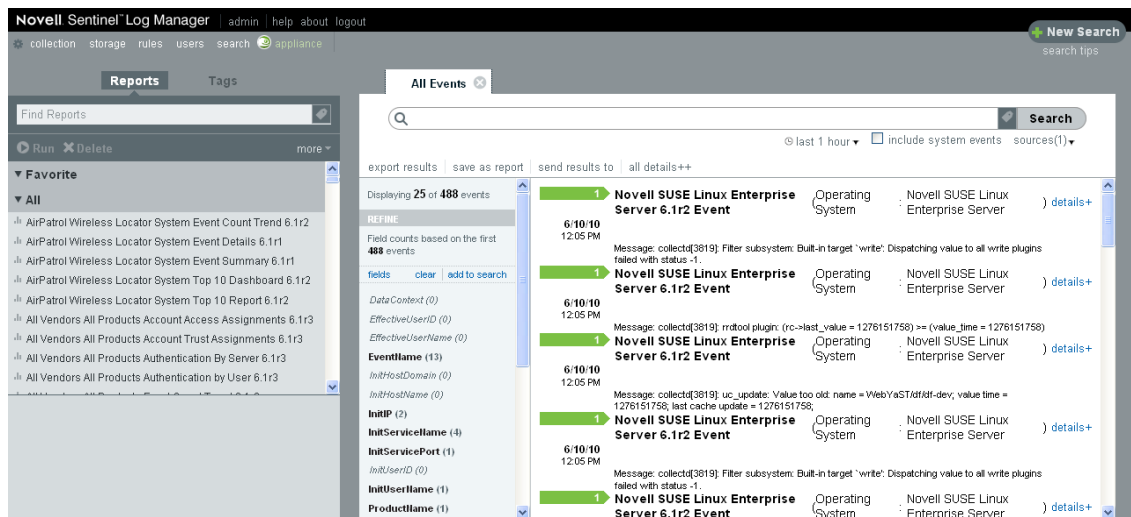
To log in to the appliance Web console and initialize the software:

- 1 Open a Web browser and log in to <https://<IP address>:8443>. The Sentinel Log Manager Web page is displayed.
The IP address of the appliance is displayed on the appliance console after the installation completes and the server restarts.
- 2 You can configure the Sentinel Log Manager appliance for data storage and data collection. For more information, see the [Sentinel Log Manager 1.2.2 Administration Guide](#).
- 3 To register for updates, see [Section 4.10, “Registering for Updates,”](#) on page 47.

4.7 Configuring WebYaST

The Novell Sentinel Log Manager appliance user interface is equipped with WebYaST. WebYaST is a Web-based remote console for controlling appliances based on SUSE Linux Enterprise. You can access, configure, and monitor the Sentinel Log Manager appliances with WebYaST. The following procedure briefly describes the steps to configure WebYaST. For more information on detailed configuration, see the [WebYaST User Guide \(http://www.novell.com/documentation/webyast/\)](http://www.novell.com/documentation/webyast/).

- 1 Log in to the Sentinel Log Manager appliance.



2 Click *Appliance*.

Login

Enter login credentials for host localhost.

Username:

root

Password:

●●●●●●●●

3 Configure the Sentinel Log Manager Server to receive updates as described in [Section 4.10, “Registering for Updates,”](#) on page 47.

4 Click *Next* to finish the initial setup.

4.8 Configuring the Appliance with SMT

In secured environments where the appliance must run without direct internet access, you must configure the appliance with Subscription Management Tool (SMT), which enables you to upgrade the appliance to the latest available versions. SMT is a package proxy system that is integrated with Novell Customer Center and provides key Novell Customer Center capabilities.

- ◆ [Section 4.8.1, “Prerequisites,”](#) on page 45
- ◆ [Section 4.8.2, “Configuring the Appliance,”](#) on page 46
- ◆ [Section 4.8.3, “Upgrading the Appliance,”](#) on page 46

4.8.1 Prerequisites

- ◆ Get the Novell Customer Center credentials for Sentinel Log Manager to get updates from Novell. For information on getting the credentials, contact [Novell Support \(http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup\)](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup).
- ◆ Ensure that SLES 11 SP1 is installed with the following packages on the machine where you want to install SMT:
 - ◆ `htmldoc`
 - ◆ `smt`
 - ◆ `perl-DBIx-Transaction`
 - ◆ `perl-File-Basename-Object`
 - ◆ `pertl-DBIx-Migration-Director`
 - ◆ `perl-MIME-Lite`
 - ◆ `perl-Text-ASCIITable`
 - ◆ `smt-support`
 - ◆ `yast2-smt`
 - ◆ `yum-metadata-parser`
 - ◆ `createrepo`
 - ◆ `sle-smt-release-cd`
 - ◆ `sle-smt_en`
 - ◆ `perl-DBI`
 - ◆ `apache2-prefork`
 - ◆ `libapr1`
 - ◆ `perl-Data-ShowTable`
 - ◆ `perl-Net-Daemon`
 - ◆ `perl-Tie-IxHash`
 - ◆ `fltk`
 - ◆ `libapr-util1`
 - ◆ `perl-PIRPC`
 - ◆ `apache2-mod_perl`
 - ◆ `apache2-utils`
 - ◆ `apache2`
 - ◆ `perl-DBD-mysql`
- ◆ Install SMT and configure the SMT server. For more information, refer to the following sections in the [SMT Documentation \(http://www.novell.com/documentation/smt11/\)](http://www.novell.com/documentation/smt11/):
 - ◆ SMT Installation
 - ◆ SMT Server Configuration
 - ◆ Mirroring Installation and Update Repositories with SMT
- ◆ Install the `wget` utility on the appliance machine.

4.8.2 Configuring the Appliance

For information on configuring the appliance with SMT, see “Configuring Clients to Use SMT” (http://www.novell.com/documentation/smt11/smt_sle_11_guide/?page=/documentation/smt11/smt_sle_11_guide/data/smt_client.html) in the *Subscription Management Tool* documentation.

To enable the appliance repositories, execute the following command:

- ◆ **VMWare Appliance Image:**

```
smt-repos -p sentinel_log_manager_1100_64_vmx_x86_64
```

- ◆ **Xen Appliance Image:**

```
smt-repos -p sentinel_log_manager_1100_64_xen_x86_64
```

- ◆ **ISO:**

```
smt-repos -p sentinel_log_manager_1100_64_xen_x86_64
```

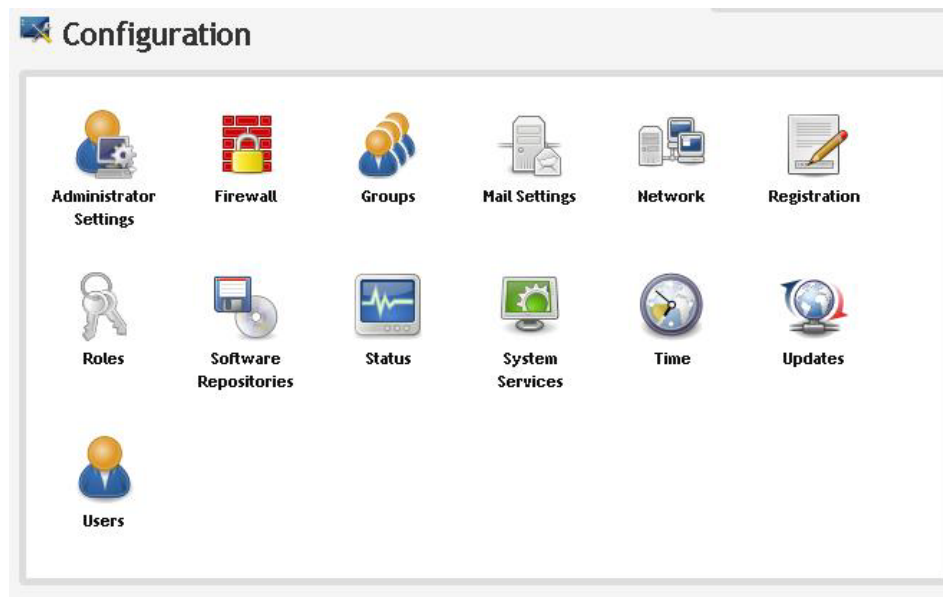
4.8.3 Upgrading the Appliance

For information on upgrading the appliance, see [Section 5.4.3, “Upgrading the Appliance by Using SMT,”](#) on page 53.

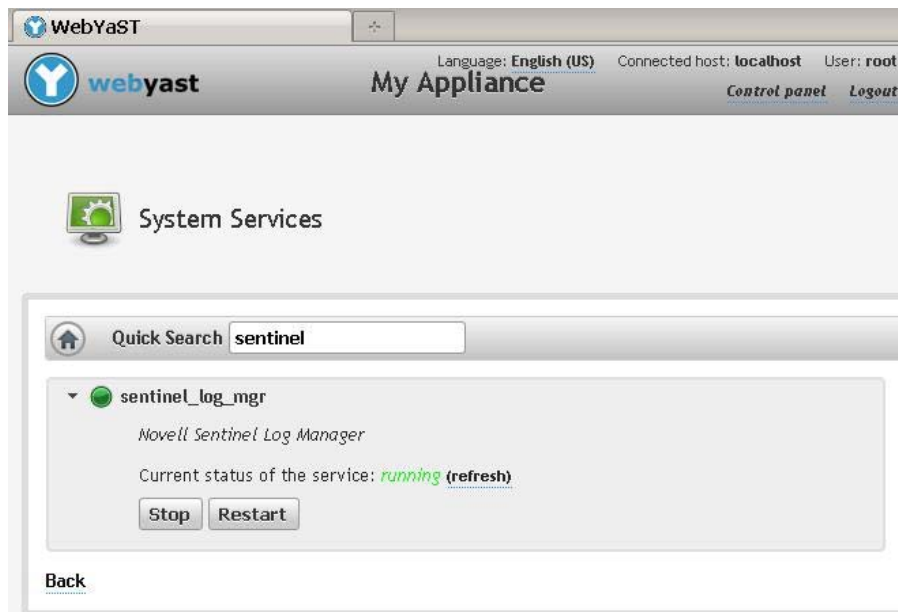
4.9 Stopping and Starting the Appliance by Using Web UI

You can start and stop the Sentinel Log Manager server by using the Web UI as follows:

- 1 Log in to the Sentinel Log Manager appliance.
The Sentinel Log Manager Web User Interface is displayed.
- 2 Click *Appliance* to launch WebYaST.



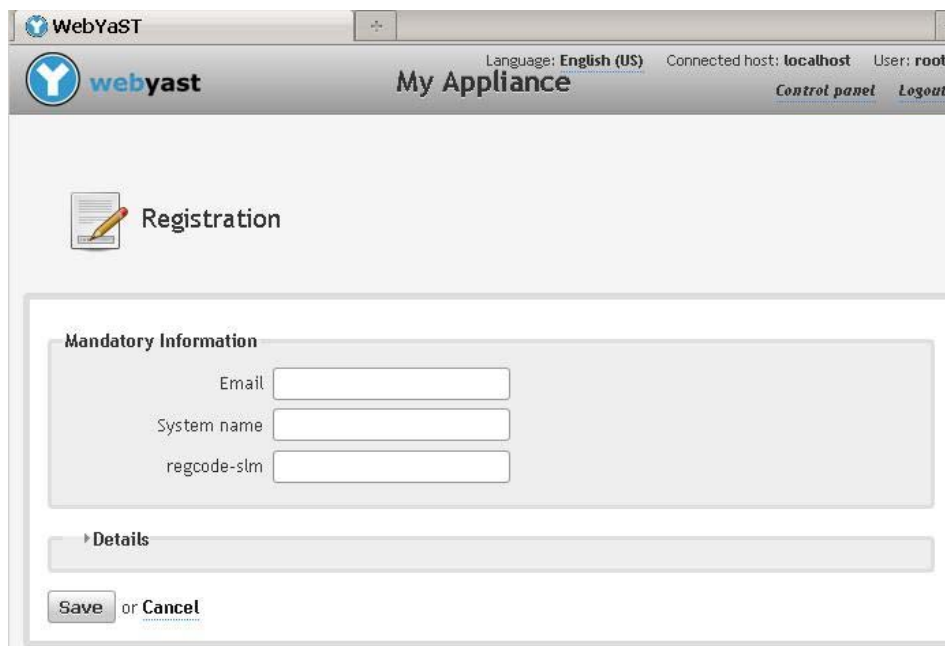
- 3 Click *System Services*.



- 4 To stop the Sentinel Log Manager server, click *stop*.
- 5 To start the Sentinel Log Manager server, click *start*.

4.10 Registering for Updates

- 1 Log in to the Sentinel Log Manager appliance.
The Sentinel Log Manager Web UI is displayed.
- 2 Click *Appliance* to launch WebYaST.
- 3 Click *Registration*.



- 4 Specify the email ID to which you want to receive updates, system name, and the appliance registration code.
- 5 Click *Save*.

For information on upgrading appliance, see [Section 5.4, "Upgrading the Appliance,"](#) on page 52.

5 Upgrading Sentinel Log Manager

You can install Sentinel Log Manager 1.2.0.2 on Sentinel Log Manager versions 1.2 and later. If you want to upgrade Sentinel Log Manager versions 1.1.x, you must first upgrade to Sentinel Log Manager 1.2.0.1 and then install Sentinel Log Manager 1.2.0.2.

NOTE: After the upgrade, any Collector customizations performed by using the Custom Execution Mode and the auxiliary file method recommended in the SDK documentation are preserved.

- ◆ [Section 5.1, “Prerequisites,” on page 49](#)
- ◆ [Section 5.2, “Upgrading the Sentinel Log Manager Server,” on page 50](#)
- ◆ [Section 5.3, “Upgrading the Collector Manager,” on page 51](#)
- ◆ [Section 5.4, “Upgrading the Appliance,” on page 52](#)
- ◆ [Section 5.5, “Upgrading Sentinel Plug-Ins,” on page 54](#)

5.1 Prerequisites

- ◆ Sentinel Log Manager 1.2 and later require the SUSE Linux Enterprise Server (SLES) 11 SP1 platform. If you are upgrading to Sentinel Log Manager 1.2 or a later version, ensure that the operating system is upgraded to SLES 11 SP1.
- ◆ For Sentinel Log Manager 1.2 and later to work successfully on SLES 11 SP1, the following RPMs or a later version must be installed:
 - ◆ **Kernel patches:**
 - ◆ `kernel-default-2.6.32.29-0.3.1.x86_64.rpm`
 - ◆ `kernel-default-base-2.6.32.29-0.3.1.x86_64.rpm`
 - ◆ **Linux util RPMs:**
 - ◆ `libblkid1-2.16-6.11.1.x86_64.rpm`
 - ◆ `libuuid1-2.16-6.11.1.x86_64.rpm`
 - ◆ `util-linux-2.16-6.11.1.x86_64.rpm`
 - ◆ `util-linux-lang-2.16-6.11.1.x86_64.rpm`
 - ◆ `uuid-runtime-2.16-6.11.1.x86_64.rpm`

Sentinel Log Manager 1.1.0.x uses squashfs version 3.4-35.1; however SLES 11 SP1 supports squashfs 4.0 and later, which is not backward compatible and cannot open a squashed file system created with previous squashfs versions. Installing these RPMs fixes the incompatibility issue between the squashfs versions of Sentinel Log Manager 1.1.0.x and SLES 11 SP1.

These RPMs are available through the SLES 11 online update channel. For more information on updating the SLES system, see “[YaST Online Update](http://www.novell.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html)” ([http://www.novell.com/documentation/sles11/book_sle_admin/?page=/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html](http://www.novell.com/documentation/sles11/book_sle_admin/data/cha_onlineupdate_you.html)) in the *SLES 11 SP1 Administration Guide* (http://www.novell.com/documentation/sles11/book_sle_admin/data/book_sle_admin_pre.html).

NOTE: The installation does not proceed unless the above mentioned kernel patches and Linux util rpms are installed.

- ♦ If you want to upgrade Sentinel Log Manager versions 1.1.x, you must first upgrade to Sentinel Log Manager 1.2.0.1 and then install Sentinel Log Manager 1.2.0.2.
- ♦ Ensure that symbolic links have not been used for the following folders and subfolders:
 - ♦ `opt/novell` (Base folder)
 - ♦ `etc/opt/novell` (Configuration folder)
 - ♦ `var/opt/novell` (Data folder)

If symbolic links have been used, remove them; that is, move these directories back to the standard installation directories.

5.2 Upgrading the Sentinel Log Manager Server

- 1 Make a backup of your configuration, then create an ESM export.

For more information on backing up data, see “[Backing Up and Restoring Data.](#)”

- 2 Download the latest patch from the [Novell download site \(http://download.novell.com\)](http://download.novell.com).

- 3 (Conditional) If you want to upgrade to Sentinel Log Manager Hotfix 1, download the patch from the [Novell Patch Finder site \(http://download.novell.com/patch/finder/\)](http://download.novell.com/patch/finder/).

- 4 Log in as `root` to the server where you want to install Sentinel Log Manager.

- 5 Specify the following command to stop the Sentinel Log Manager server:

```
<install_directory>/bin/server.sh stop
```

For example, `/opt/novell/sentinel_log_mgr/bin # ./server.sh stop.`

- 6 Specify the following command to extract the install files from the tar file:

```
tar xfz <install_filename>
```

Replace `<install_filename>` with the actual name of the install file.

- 7 Change to the directory where the install file was extracted.

- 8 Specify the following command to run the `install-slm` script to upgrade Sentinel Log Manager:

```
./install-slm
```

- 9 To proceed with a language of your choice, select the number next to the language.

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

- 10 Read the end user license, enter `yes` or `y` to accept the license, then continue with the installation.

- 11 The installation script detects that an older version of the product already exists and prompts you to specify if you want to upgrade the product. If you press `n`, the installation terminates. To continue with the upgrade, press `y`.

The installation starts installing all RPM packages. This installation might take a few seconds to complete.

If you are upgrading a Sentinel Log Manager 1.1 system that was upgraded from Sentinel Log Manager 1.0, the existing Sentinel Log Manager 1.0 installation is left intact, with the following exceptions:

- ◆ If the 1.0 data directory (For example, `/opt/novell/sentinel_log_manager_1.0_x86-64/data`) and the 1.1 data directory (For example, `/var/opt/novell/sentinel_log_mgr/data`) are in the same file system, then the `<1.0>/data/eventdata` and `<1.0>/data/rawdata` subdirectories are moved to the 1.1 location because the `eventdata` and `rawdata` directories are typically large. If the 1.0 data and 1.1 data directories are in different file systems, then the `eventdata` and `rawdata` subdirectories are copied to the 1.1 location and the 1.0 files are left intact.
- ◆ If the existing 1.0 data directory, such as `/opt/novell/sentinel_log_mgr_1.0_x86-64`, is on a separately mounted file system and there is insufficient space on the file system containing the 1.1 data directory (`/var/opt/novell/sentinel_log_mgr/data`), then you can allow the installer to remount the file system from the 1.0 location to the 1.1 location. Any entry in `/etc/fstab` is also updated. If you decide not to allow the installer to remount the existing file system, the upgrade exits. You can then create sufficient space on the file system for the 1.1 data directory.

After the Sentinel Log Manager 1.2.0.2 installation is successful and the server is functional, specify the following command to manually remove the Sentinel Log Manager 1.0 directory:

```
rm -rf /opt/novell/slm_1.0_install_directory
```

For example:

```
rm -rf /opt/novell/sentinel_log_mgr_x86-64
```

Removing the installation directory permanently deletes the Sentinel Log Manager 1.0 installation.

- 12** Specify the following command to start the Sentinel Log Manager server:

```
<install_directory>/bin/server.sh start
```

- 13** Make sure that all the Collector Managers are upgraded to a version compatible with the upgraded Sentinel Log Manager server.

For more information on upgrading Collector Managers, see [Section 5.3, “Upgrading the Collector Manager,” on page 51](#).

NOTE: When you start the system for the first time after the upgrade, it might take approximately five minutes for the system to initialize before you can start using it. This delay occurs only when you start the system for the first time after the installation or an upgrade.

5.3 Upgrading the Collector Manager

- 1** Make a backup of your configuration and create an ESM export.

For more information, see “[Backing Up and Restoring Data](#)” in the *Sentinel Log Manager 1.2.2 Administration Guide*.

- 2** Log in to Sentinel Log Manager as an administrator.

- 3** Select *collection > Advanced*.

You can download the latest upgrade installer for Collector Manager that is compatible with the Sentinel Log Manager from this page.

- 4** Click the *Download Installer* link in the Collector Manager Upgrade Installer section.

A window is displayed with options to either open or to save the `scm_upgrade_installer.zip` file on the local machine.

- 5 Save the file.
- 6 Copy the file to a temporary location.
- 7 Extract the contents of the `.zip` file.
- 8 Run one of the following scripts:
 - ♦ To upgrade the Windows Collector Manager, run `service_pack.bat`.
 - ♦ To upgrade the Linux Collector Manager, run `service_pack.sh`.
- 9 Follow the on-screen instructions to complete the installation.

5.4 Upgrading the Appliance

You can upgrade the Sentinel Log Manager appliance either by using the WebYaST or by using SMT.

- ♦ [Section 5.4.1, “Upgrading the Appliance through WebYast,” on page 52](#)
- ♦ [Section 5.4.2, “Upgrading the Appliance by Using Zypper,” on page 53](#)
- ♦ [Section 5.4.3, “Upgrading the Appliance by Using SMT,” on page 53](#)

5.4.1 Upgrading the Appliance through WebYast

NOTE: If you are upgrading Sentinel Log Manager appliance that is on a operating system prior to SLES 11 SP3, you must upgrade the appliance by using the `zypper` command line utility because user interaction is required to complete the upgrade. WebYaST is not capable of facilitating the required user interaction. For information about using `zypper` to upgrade the appliance, see [Section 5.4.2, “Upgrading the Appliance by Using Zypper,” on page 53](#)

- 1 Specify the URL of the Sentinel Log Manager using the port 4984 to launch WebYaST.
- 2 Log in to WebYast using the appliance credentials.
- 3 Make a backup of your configuration, then create an ESM export.
For more information on backing up data, see [“Backing Up and Restoring Data.”](#)
- 4 (Conditional) If you have not already registered the appliance for automatic updates, register it.
For more information, see [Section 4.10, “Registering for Updates,” on page 47](#).
If the appliance is not registered, a yellow warning is displayed in WebYast, indicating that the appliance is not registered.
- 5 To check if there are any updates, click *Updates*.
The available updates are displayed.
- 6 Select and apply the updates.
The updates might take a few minutes to complete. After the update is successful, the WebYaST login page is displayed.
Before upgrading the appliance, WebYaST automatically stops the Sentinel Log Manager service. You must manually restart this service after the upgrade is complete.
- 7 Restart the Sentinel Log Manager server by using the Web UI.
For more information, see [Section 4.9, “Stopping and Starting the Appliance by Using Web UI,” on page 46](#).

5.4.2 Upgrading the Appliance by Using Zypper

To upgrade the appliance by using the zypper patch:

- 1 Make a backup of your configuration, then create an ESM export.
For more information on backing up data, see [“Backing Up and Restoring Data.”](#)
- 2 (Conditional) If you have not already registered the appliance for automatic updates, register it.
For more information, see [Section 4.10, “Registering for Updates,”](#) on page 47.
If the appliance is not registered, a yellow warning is displayed in WebYast, indicating that the appliance is not registered.
- 3 Log in to the appliance console as the `root` user.
- 4 Run the following command:

```
usr/bin/zypper patch
```
- 5 (Conditional) If you are upgrading Sentinel Log Manager prior to version 1.2, a message is displayed indicating a squashfs version conflict. Enter `1` to upgrade squashfs version 4.0-1.2.10 and to accept the vendor change.

Sentinel Log Manager 1.1. versions use squashfs version 3.4, but Sentinel Log Manager 1.2 and later use squashfs version 4.0. Also, the vendor for squashfs yast2-live-installer has changed from OpenSUSE to SLES. To proceed with the upgrade, you must first upgrade squashfs and accept the vendor change.
- 6 Enter `y` to proceed.
- 7 (Conditional) If you are upgrading Sentinel Log Manager prior to version 1.2, the end user license agreement for Sentinel Log Manager is displayed. Enter `yes` to accept the license.

The license agreement for Sentinel Log Manager 1.2 and later is different from the license agreement for Sentinel Log Manager 1.1. You must accept the new license agreement to upgrade Sentinel Log Manager 1.1 and later to 1.2 and later.
- 8 (Conditional) If you are upgrading Sentinel Log Manager appliance that is on a operating system prior to SLES 11 SP3, the end user license agreement is displayed. Enter `yes` to accept the license.

The Sentinel Log Manager appliance upgrades successfully.
- 9 (Conditional) If you are upgrading Sentinel Log Manager prior to version 1.2, after the upgrade is complete, a deprecation warning is displayed.

This is because Sentinel Log Manager 1.2.0.1 uses WebYaST 1.1, but Sentinel Log Manager 1.1 versions use WebYaST 1.0. During the upgrade, the WebYaST 1.0 language module is deprecated in WebYaST 1.1. However, this warning does not affect the upgrade.
- 10 Restart the Sentinel Log Manager appliance.

5.4.3 Upgrading the Appliance by Using SMT

In secured environments where the appliance must run without direct internet access, you must configure the appliance with Subscription Management Tool (SMT), which enables you to upgrade the appliance to the latest available versions.

- 1 Ensure that the appliance is configured with SMT.
For more information, see [Section 4.8, “Configuring the Appliance with SMT,”](#) on page 44.
- 2 Log in to the appliance console as the `root` user.
- 3 Refresh the repository for upgrade:

```
zypper ref -s
```

- 4 Check whether the appliance is enabled for upgrade:

```
zypper lr
```

- 5 (Optional) Check the available updates for the appliance:

```
zypper lu
```

- 6 (Optional) Check the packages that include the available updates for the appliance:

```
zypper lp -r SMT-http_<smt_server_ipaddress>:SLM-1.1.0.0-ISO
```

- 7 Update the appliance:

```
zypper up -t patch -r SMT-http_<smt_server_ipaddress>:SLM-1.1.0.0-ISO
```

- 8 Restart the appliance.

```
rcsentinel_log_mgr restart
```

5.5 Upgrading Sentinel Plug-Ins

The new and updated Sentinel plug-ins are frequently uploaded to the [Sentinel Plug-ins Web site \(http://support.novell.com/products/sentinel/secure/sentinelplugins.html\)](http://support.novell.com/products/sentinel/secure/sentinelplugins.html). To get the latest bug fixes, documentation updates, and enhancements for a plug-in, download the most recent version of the plug-in. For information on installing or upgrading a plug-in, see the specific plug-in documentation.

6 Logging In to the Web Interface

The administrator user created during the installation can log in to the Web interface to configure and use Sentinel Log Manager:

- 1 Open a supported Web browser. For more information, see [Section 2.3, “Supported Browsers,”](#) on page 22.
- 2 Specify the URL for the Novell Sentinel Log Manager page (for example, `https://10.0.0.1:8443/novelllogmanager`), then press Enter.
- 3 (Conditional) The first time you log in to the Sentinel Log Manager, you are prompted to accept a certificate. The Sentinel Log Manager login page is displayed when you accept the certificate.

Novell

Novell
Sentinel Log Manager

Version 1.1

© Novell, Inc. All rights reserved.

Username:
admin

Password:
••••••

Language:
English

Sign in

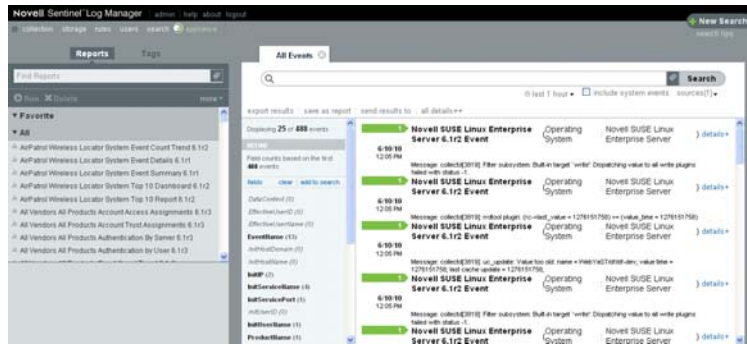
Novell Sentinel Log Manager supports Firefox 3 (works best on 3.6) and Internet Explorer 8 (works best on 8.0)

- 4 Specify the username and password for the Sentinel Log Manager administrator.
- 5 Select the language for the Sentinel Log Manager interface.

The Sentinel Log Manager user interface is available in English, Portuguese, French, Italian, German, Spanish, Japanese, Traditional Chinese, or Simplified Chinese.

6 Click *Sign in*.

The Novell Sentinel Log Manager Web User Interface is displayed.



7 Installing Additional Collector Managers

The Collector Managers manage all data collection and data parsing for Novell Sentinel Log Manager. The Sentinel Log Manager installation process installs a Collector Manager by default on the Sentinel Log Manager server. However, you can install multiple Collector Managers in a distributed setup.

- ♦ [Section 7.1, “Before You Begin,” on page 57](#)
- ♦ [Section 7.2, “Advantages of Additional Collector Managers,” on page 58](#)
- ♦ [Section 7.3, “Installing Additional Collector Managers,” on page 58](#)

7.1 Before You Begin

- ♦ Make sure that your hardware and software meet the minimum requirements mentioned in [Chapter 2, “System Requirements,” on page 17](#).
- ♦ Synchronize time by using the Network Time Protocol (NTP).
- ♦ A Collector Manager requires network connectivity to the message bus port (61616) on the Sentinel Log Manager server. Before you start installing the Collector Manager, make sure that all firewall and other network settings are allowed to communicate over this port.
- ♦ To install the Collector Manager on RHEL 6, the following script and packages must be installed:
 - ♦ Install the ksh script:

```
install ksh-20100621-2.el6.x86_64
```
 - ♦ To run the installer in the console mode, the following packages must be installed:
 - ♦ `glibc-2.12-1.7.el6.i686`
 - ♦ `nss-softokn-freebl-3.12.7-1.1.el6.i686`
 - ♦ To run the installed in the GUI mode, the following packages must be installed:
 - ♦ `glibc-2.12-1.7.el6.i686`
 - ♦ `libX11-1.3-2.el6.i686`
 - ♦ `libXau-1.0.5-1.el6.i686`
 - ♦ `libxcb-1.5-1.el6.i686`
 - ♦ `libXext-1.1-3.el6.i686`
 - ♦ `libXi-1.3-3.el6.i686`
 - ♦ `libXtst-1.0.99.2-3.el6.i686`
 - ♦ `nss-softokn-freebl-3.12.7-1.1.el6.i686`

7.2 Advantages of Additional Collector Managers

Installing more than one Collector Manager in a distributed network provides several advantages:

- ♦ **Improved system performance:** The additional Collector Managers can parse and process event data in a distributed environment, thus increasing the system performance.
- ♦ **Additional data security and decreased network bandwidth requirements:** If the Collector Managers are co-located with event sources, then filtering, encryption, and data compression can be performed at the source.
- ♦ **Ability to collect data from additional operating systems:** For example, you can install a Collector Manager on Microsoft Windows to enable data collection through the WMI protocol.
- ♦ **File caching:** The remote Collector Manager can cache large amounts of data while the server is temporarily busy 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.

7.3 Installing Additional Collector Managers

- 1 Log in to the Sentinel Log Manager as an administrator.
- 2 Select *collection > Advanced*.
- 3 Click the *Download Installer* link. in the Collector Manager installer section.

A window is displayed with options to either open or to save the `scm_installer.zip` file on the local machine. Save the file.
- 4 Copy and extract the file to the location where you want to install the Collector Manager.
- 5 Run one of the following install files depending on your operating software:
 - ♦ To install the Collector Manager on a Windows system, run `setup.bat`.
 - ♦ To install the Collector Manager on a Linux system, run `setup.sh`.
- 6 Select a language, then click *OK*.

The install shield is displayed.
- 7 Click *OK*.
- 8 Read and accept the license agreement, then click *Next*.
- 9 You can either proceed with the default installation directory or browse and select the directory, then click *Next*.
- 10 Leave the default Message bus port (61616) unchanged and specify the host name/IP address of the Sentinel Log Manager server.
- 11 Click *Next* to proceed with the default Automatic Memory Configuration (256 Megabytes).

A Summary of the installation is displayed.
- 12 Click *Install*.
- 13 Specify the username and password for the Collector Manager.

The username and password is stored in the `/etc/opt/novell/sentinel_log_mgr/config/activemqusers.properties` file located in the Sentinel Log Manager server.

See the following line in the `activemqusers.properties` file:

```
collectormanager=<password>
```

where `collectormanager` is the username and the corresponding value is the password.
- 14 Accept the certificate permanently when prompted.

15 Click *Finish* to complete the installation.

16 Restart the machine.

If your Collector Manager is running on Windows 2008, and if any exceptions are logged in the `collector_manager0.0.log` file after restarting, see [Section A.4, “Collector Manager Throws Exception on Windows 2008 When UAC is Enabled,”](#) on page 67 to troubleshoot the issue.

8 Uninstallation

This section discusses the procedures to uninstall Novell Sentinel Log Manager server and the Collector Manager.

- ◆ [Section 8.1, “Uninstalling the Appliance,” on page 61](#)
- ◆ [Section 8.2, “Uninstalling Sentinel Log Manager,” on page 61](#)
- ◆ [Section 8.3, “Uninstalling the Collector Manager,” on page 62](#)

8.1 Uninstalling the Appliance

If you want to retain any Log Manager data, then you must back up the data before uninstalling the appliance, so that you can restore the data later. For more information, see [“Backing Up and Restoring Data”](#) in the *Sentinel Log Manager 1.2.2 Administration Guide*.

If you do not need to retain any data, use the following procedures to uninstall the appliance:

- ◆ **VMware ESX Appliance:** If the virtual machine is dedicated to Novell Sentinel Log Manager and you do not need to retain any data, delete the virtual machine to uninstall the Log Manager virtual appliance.
- ◆ **Xen Appliance:** If the Xen virtual machine is dedicated to Novell Sentinel Log Manager and you do not need to retain any data, delete it to uninstall the Log Manager virtual appliance.
- ◆ **Hardware Appliance:** If the system is dedicated to Novell Sentinel Log Manager and if you do not need to retain any data, reformat the hard drive to uninstall the Log Manager on a physical machine.

8.2 Uninstalling Sentinel Log Manager

- 1 Log in to the Sentinel Log Manager server as `root`.
- 2 To run the uninstall script, execute the following command:

```
/opt/novell/sentinel_log_mgr/setup/uninstall-slm
```
- 3 When you are prompted to reconfirm that you want to proceed with the uninstall, press `y`.
The Sentinel Log Manager server is first stopped and then uninstalled.

8.3 Uninstalling the Collector Manager

This section discusses the procedures to uninstall the Sentinel Collector Manager installed either on Windows or on Linux machines.

- ♦ [Section 8.3.1, “Uninstalling the Linux Collector Manager,” on page 62](#)
- ♦ [Section 8.3.2, “Uninstalling the Windows Collector Manager,” on page 62](#)
- ♦ [Section 8.3.3, “Manual Cleanup of Directories,” on page 63](#)

8.3.1 Uninstalling the Linux Collector Manager

- 1 Log in as `root`.
- 2 In the machine where the Collector Manager is installed, navigate to the following location:
`$ESEC_HOME/_uninst`
- 3 Run the following command:
`./uninstall.bin`
- 4 Select a language, then click *OK*.
- 5 Click *Next* in the install shield wizard.
- 6 Select the features that you want to uninstall, then click *Next*.
- 7 Stop all the Sentinel Log Manager applications that are running, then click *Next*.
- 8 Click *Uninstall*.
- 9 Click *Finish*.
- 10 Select *Reboot the system* and click *Finish*.

8.3.2 Uninstalling the Windows Collector Manager

- 1 Log in as administrator.
- 2 Stop the Sentinel Log Manager server.
- 3 Select Start > Run.
- 4 Specify the following:
`%Esec_home%_uninst`
- 5 Double `uninstall.exe` to run it.
- 6 Select a language, then click *OK*.
The Install Shield Wizard is displayed.
- 7 Click *Next*.
- 8 Select the features that you want to uninstall, then click *Next*.
- 9 Stop all the Sentinel Log Manager applications that are running, then click *Next*.
- 10 Click *Uninstall*.
- 11 Click *Finish*.
- 12 Select *Reboot the system* and click *Finish*.

8.3.3 Manual Cleanup of Directories

- ♦ [“Linux” on page 63](#)
- ♦ [“Windows” on page 63](#)

Linux

- 1 Log in to the machine from where uninstalled the Collector Manager as root.
- 2 Stop all the Sentinel Log Manager processes.
- 3 Remove the contents of `/opt/novell/sentinel6`

Windows

- 1 Log in to the machine from where uninstalled the Collector Manager as administrator.
- 2 Delete the `%CommonProgramFiles%\InstallShield\Universal` folder and all of its contents.
- 3 Delete the `%ESEC_HOME%` folder. This is by default `C:\Program Files\Novell\Sentinel6`.

A Troubleshooting Installation

This section contains some of the issues that might occur during installation and the procedure to work around the issues.

- [Section A.1, “Sentinel Log Manager Upgrade Fails if the dbauser Password does not Match the dbauser Password Stored in the .pgpass File,” on page 65](#)
- [Section A.2, “Failed Installation Because of an Incorrect Network Configuration,” on page 66](#)
- [Section A.3, “Trouble Configuring the Network with VMware Player 3 on SLES 11,” on page 66](#)
- [Section A.4, “Collector Manager Throws Exception on Windows 2008 When UAC is Enabled,” on page 67](#)
- [Section A.5, “Upgrading Log Manager installed as a Non-Root User Other Than Novell User,” on page 68](#)
- [Section A.6, “UUID Does Not get Created for Imaged Collector Managers,” on page 68](#)

A.1 Sentinel Log Manager Upgrade Fails if the dbauser Password does not Match the dbauser Password Stored in the .pgpass File

Issue:

When you upgrade Sentinel Log Manager, the database upgrade fails if the dbauser password does not match the password stored in the `.pgpass` file.

The behavior is different for different ways of installation:

Standard installer: The upgrade does not proceed and an appropriate message is displayed indicating the cause of the error and the workaround.

Appliance Console: The following error message is displayed:

```
Installing: novell-SLMdb-1.2.0.2-954 [error]
Installation of novell-SLMdb-1.2.0.2-954 failed:
(with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Unable to
login to the database, cannot continue with the upgrade. Check if the dbauser
password specified in /home/novell/.pgpass is correct and try again.
error: %pre(novell-SLMdb-1.2.0.2-954.x86_64) scriptlet failed, exit status 2
error:   install: %pre scriptlet failed (2), skipping novell-SLMdb-1.2.0.2-954
```

```
Abort, retry, ignore? [a/r/i] (a):
```

WebYaST: WebYaST continues to indicate that an update is still available. You can check the `/var/opt/novell/sentinel_log_mgr/log/install.log` file to know the actual cause for this error.

Workaround:

Update the password in the `.pgpass` file with the current dbauser password and proceed with the upgrade. For information on the `.pgpass` file, see [PostgreSQL documentation](#).

If you are upgrading using appliance console, perform either of the following:

- ♦ Enter `a` to abort the installation, update the password in the `/home/novell/.pgpass` file, then run the `zypper patch` to proceed with the upgrade.
- ♦ Open another console, update the password in the `/home/novell/.pgpass` file. In the upgrade console, enter `r` to proceed with the upgrade.
- ♦ Enter `i` to ignore the error message and proceed with the installation. After the upgrade is complete, update the password in the `/home/novell/.pgpass` file and then run the `zypper patch` in the console to successfully complete the upgrade procedure.

If you are upgrading using WebYaST:

- 1 Log in to the appliance console.
- 2 Update the dbauser password in the `/home/novell/.pgpass` file.
- 3 In the WebYaST, click *Update All* to continue the upgrade process.

After the upgrade is complete, the `System is up to date` message is displayed in the WebYaST.

A.2 Failed Installation Because of an Incorrect Network Configuration

During the first boot, if the installer finds that the network settings are incorrect, an error message is displayed. If the network is unavailable, installing Sentinel Log Manager on the appliance fails.

To resolve this issue, properly configure the network settings so that the system has a valid IP address and hostname.

A.3 Trouble Configuring the Network with VMware Player 3 on SLES 11

You might see the following error when you try to configure the network with VMware Player 3 on SLES 11:

```
Jan 12 14:57:34.761: vmx| VNET: MACVNetPortOpenDevice: Ethernet0: can't open vmnet
device (No such device or address)
Jan 12 14:57:34.761: vmx| VNET: MACVNetPort_Connect: Ethernet0: can't open data fd
Jan 12 14:57:34.761: vmx| Msg_Post: Error
Jan 12 14:57:34.761: vmx| [msg.vnet.connectvnet] Could not connect Ethernet0 to
virtual network "/dev/vmnet0". More information can be found in the vmware.log
file.
Jan 12 14:57:34.761: vmx| [msg.device.badconnect] Failed to connect virtual device
Ethernet0.
Jan 12 14:57:34.761: vmx| --
```

This error indicates that the VMX file might have been opened by another VM. To work around this issue, you must update the MAC address in the VMX file as follows:

- 1 Open the VMX file in a text editor.
- 2 Copy the MAC address from the `ethernet0.generatedAddress` field.
- 3 Open the `/etc/udev/rules.d/70-persistent-net.rules` file from the guest operating system.

- 4 Comment out the original line, then type a `SUBSYSTEM` line as follows:

```
SUBSYSTEM=="net", DRIVERS=="?*", ATTRS{address}=="<MAC address>", NAME="eth0"
```

- 5 Replace `<MAC address>` with the MAC address you copied in [Step 2](#).
- 6 Save and close the file.
- 7 Open the VM in VMware Player.

A.4 Collector Manager Throws Exception on Windows 2008 When UAC is Enabled

Issue: Log in as any user who belongs to the Administrator group. Execute the `setup.bat` command in a terminal prompt to install the Collector Manager. Restart the system or start the Collector Manager services manually, then log in with the same user credentials. Exceptions are logged in the `collector_manager0.0.log` that impacts the following Collector Manager functionalities:

- ♦ Maps are not being initialized.
- ♦ You can not choose any event source file on the Collector Manager (Win2008) machine's file system by using the File Connector.

Possible Cause: You have installed the Collector Manager on a Windows 2008 SP1 standard edition 64-bit. By default, the machine has the User Access Control (UAC) set to Enabled.

Workaround: Change the Log On owner for the Sentinel 6.1 Rapid Deployment services to the current user. By default, the Log On owner is set to Local System Account. To change the default option:

- 1 Run `services.msc` to open the Services window.
- 2 Right-click *Sentinel*, then select *Properties*.
- 3 In the Sentinel Properties window, select the *Log On* tab.
- 4 Select *This Account*, then provide the credentials for the current user that you have used to install the Collector Manager.

NOTE: The user must be in the administrators group.

A.5 Upgrading Log Manager installed as a Non-Root User Other Than Novell User

The upgrade procedure fails if you try to upgrade the Novell Sentinel Log Manager 1.0 server installed as a non-root user other than the `novell` user. This issue occurs because of the nature of file permissions set during the Sentinel Log Manager 1.0 installation.

To upgrade the Sentinel Log Manager 1.0 server installed as a non-root user other than `novell`, do the following:

- 1 Create `novell` user.
- 2 Change the ownership of the Sentinel Log Manager 1.0 installation to `novell:novell`.

```
chown -R novell:novell /opt/novell/<install_directory>
```

Change `<install_directory>` to the name of the installation directory. For example,

```
chown -R novell:novell /opt/novell/sentinel_log_mgr_1.0_x86-64
```

- 3 Change the `ESEC_USER` entry in `/etc/opt/novell/sentinel_log_mgr/config/eseuser.properties` to `novell`.

A.6 UUID Does Not get Created for Imaged Collector Managers

If you image a Collector Manager server (for example, by using ZenWorks Imaging) and restore the images on different machines, Sentinel Log Manager does not uniquely identify the new instances of Collector Manager. This happens due to duplicate UUIDs.

You must generate the UUID on the newly installed Collector Manager systems by performing the following steps:

- 1 Delete the `host.id` or `sentinel.id` file that is located in the `/var/opt/novell/sentinel_log_mgr/data` folder.
- 2 Restart the Collector Manager.

The Collector Manager automatically generates the UUID.

Sentinel Terminology

This section describes the terminology used in this document.

Collectors. A utility that parses the data and delivers 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. A utility that uses industry standard methods to connect to the data source to get raw data.

Data Retention. A policy that defines the duration for which the events remain before they are deleted from the Sentinel Log Manager server.

Event Source. The applicator or system that logs the event.

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

Events Per Second. EPS. A value that measures 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. Plug-ins that allow Sentinel systems to connect to other external systems. JavaScript actions can use Integrators to interact with other systems.

Raw Data . The unprocessed events that are received by the connector and sent directly to the Sentinel Log Manager message bus and then written to the disk on the Sentinel Log Manager server. Raw data varies from Connector to Connector because of the format of the data stored on the device.

