Installation and Configuration Guide

NetIQ Sentinel 7.0.1

April 2012

NetIQ®

Legal Notices

NetIQ Corporation (“NetIQ”) makes no representations or warranties with respect to the contents or use of the online help or other documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. NetIQ reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. NetIQ assumes no responsibility for your failure to obtain any necessary export approvals.

For more information, please contact NetIQ at:

1233 West Loop South, Houston, Texas 77027

U.S.A

www.netiq.com

Contents

About This Guide

This guide provides an introduction to NetIQ Sentinel and explains how to install, migrate, and configure Sentinel.

Audience

This guide is intended for Sentinel administrators and consultants.

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.

Documentation Updates

For the most recent version of the *NetIQ Sentinel 7.0.1 Installation and Configuration Guide*, visit the Sentinel documentation Web site (http://www.novell.com/documentation/sentinel70).

Additional Documentation

Sentinel technical documentation is broken down into several different volumes. They are:

- Sentinel Overview Guide (http://www.novell.com/documentation/sentinel70/s701_overview/data/bookinfo.html)
- Sentinel Quick Start Guide (http://www.novell.com/documentation/sentinel70/s701_quickstart/data/s701_quickstart.html)
- Sentinel Administration Guide (http://www.novell.com/documentation/sentinel70/s701_admin/data/bookinfo.html)
- Sentinel User Guide (http://www.novell.com/documentation/sentinel70/s701_user/data/bookinfo.html)
- Sentinel Link Overview Guide (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Sentinel Internal Audit Events (http://www.novell.com/documentation/sentinel70/s701_auditevents/data/bookinfo.html)
- Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)

  The Sentinel SDK site provides information about building your own plug-ins.

Contacting Novell and NetIQ

Sentinel is now a NetIQ product, but Novell still handles many support functions.

- Novell Web site (http://www.novell.com)
- NetIQ Web site (http://www.netiq.com)

- Technical Support (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Self Support (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Patch download site (http://download.novell.com/index.jsp)
- Sentinel Community Support Forums (http://forums.novell.com/netiq/netiq-product-discussion-forums/sentinel/)
- Sentinel TIDs (http://support.novell.com/products/sentinel)
- Sentinel Plug-in Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **Notification Email List:** Sign up through the Sentinel Plug-in Web site

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team.

Worldwide: NetIQ Office Locations (http://www.netiq.com/about_netiq/officelocations.asp)

United States and Canada: 888-323-6768

Email: info@netiq.com

Web site: www.netiq.com

I Installing

Use the following information to install Sentinel:

- Chapter 1, “Meeting System Requirements,” on page 11
- Chapter 2, “Installing Sentinel,” on page 21
- Chapter 3, “Installing Additional Collector Managers,” on page 31
- Chapter 4, “Installing Additional Correlation Engines,” on page 35
- Chapter 5, “Installing the Appliance,” on page 39
- Chapter 6, “Troubleshooting the Installation,” on page 53
- Chapter 7, “What’s Next,” on page 55

1 Meeting System Requirements

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

- Section 1.1, “System Requirements and Supported Platforms,” on page 11
- Section 1.2, “Connector and Collector System Requirements,” on page 17
- Section 1.3, “Ports Used,” on page 17

1.1 System Requirements and Supported Platforms

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

- Section 1.1.1, “Supported Operating Systems and Platforms,” on page 11
- Section 1.1.2, “Hardware Requirements,” on page 12
- Section 1.1.3, “Supported Database Platforms,” on page 14
- Section 1.1.4, “Supported Browsers,” on page 14
- Section 1.1.5, “Data Storage Requirement Estimation,” on page 15
- Section 1.1.6, “Disk I/O Utilization Estimation,” on page 16
- Section 1.1.7, “Network Bandwidth Utilization Estimation,” on page 17
- Section 1.1.8, “Virtual Environment,” on page 17

1.1.1 Supported Operating Systems and Platforms

The Sentinel server, Collector Manager, and Correlation Engine are supported on the following operating systems and platforms:

Category	Requirement
Operating System	Sentinel is supported on the following operating systems: ◆ SUSE Linux Enterprise Server (SLES) 11 SP1 64-bit * ◆ Red Hat Enterprise Linux for Servers (RHEL) 6 64-bit * Sentinel 7 is not supported on the Open Enterprise Server installs of SLES.

Category	Requirement
Virtual Platform	NetIQ provides appliances that install a SLES 11 SP1 64-bit server and Sentinel on the following virtual platforms: ◆ VMWare ESX 4.0 ◆ Xen 4.0
DVD ISO	NetIQ provides a DVD ISO file that installs SLES 11 SP1 64-bit and Sentinel on: ◆ Hyper-V Server 2008 R2 ◆ Hardware without an operating system installed

1.1.2 Hardware Requirements

The hardware recommendations for a Sentinel implementation can vary based on the individual implementation, so you should consult NetIQ Consulting Services or any of the NetIQ Sentinel partners prior to finalizing the Sentinel architecture.

- "Sentinel Server" on page 12
- "Collector Manager" on page 13
- "Correlation Engine" on page 13

Sentinel Server

This section lists the hardware recommendations for a production system that holds 90 days of online data. The recommendations assume an average event size of 600 bytes. The local and network storage recommendations include a 20% buffer above the actual storage estimates. NetIQ recommends building in a buffer in case estimates are inaccurate or some of the servers become busier over time.

Use the following hardware recommendations for running the Sentinel server with all of the Sentinel components installed on a single server:

Category	100 EPS	2500 EPS	5000 EPS
CPU	One Intel Xeon X5570 2.93-GHz (4 CPU cores)	Two Intel Xeon X5470 3.33-GHz (4 core) CPUs (8 cores total)	Two Intel Xeon X5470 3.33-GHz (4core) CPUs (8 cores total)
Local Storage (30 days)	2x256 GB, 7.2k RPM drives (Hardware RAID 1 with 256 MB cache)	8x1.2 TB, 7.2k RPM drives (Hardware RAID 10 with 256 MB cache)	16x1.2 TB, 15k RPM drives, (Hardware RAID 10 with 512 MB cache) or an equivalent storage area network (SAN)
Networked Storage (90 days)	2x128 GB	4x1 TB	8x1 TB
Memory	**Other Installations:** 4 GB **DVD ISO Installation:** 4.5 GB	16 GB	24 GB

NOTE: Sentinel is supported on x86-64-bit Intel Xeon and AMD Opteron processors, but is not supported on pure 64-bit processors like Itanium.

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 1.1.5, "Data Storage Requirement Estimation," on page 15.
- 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 cost 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).
- The recommended steady state volume is 80% of the maximum licensed EPS. NetIQ recommends that you add additional Sentinel instances if this limit is reached.

Collector Manager

Use the following hardware requirements for running the Collector Manager on a separate system from the Sentinel Server in a production environment:

Category	Minimum	Recommendation
CPU	Intel Xeon L5240 3-Ghz (2 core)	One Intel Xeon X5570 2.93-GHz (4 CPU cores)
Disk Space	10 GB (RAID 1)	20 GB (RAID 1)
Memory	1.5 GB	4 GB
Estimated Rate (EPS)	500	2000

Correlation Engine

Use the following system requirements for running the Correlation Engine on a separate system from the Sentinel Server in a production environment:

Category	Minimum	Recommendation
CPU	Intel Xeon L5240 3-Ghz (2 core)	One Intel Xeon X5570 2.93-GHz (4 CPU cores)
Disk Space	10 GB (no RAID required)	10 GB (no RAID required)
Memory	1.5 GB	4 GB
Estimated Rate (EPS)	500	2500

1.1.3 Supported Database Platforms

Sentinel includes an embedded file-based storage system and a database, which is all is necessary to run Sentinel. However, if you use the optional data synchronization feature to copy data to a data warehouse, Sentinel supports using Oracle version 11g R2 or Microsoft SQL Server 2008 R2 as the data warehouse.

1.1.4 Supported Browsers

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

NOTE: To load the Sentinel client applications properly, you must have Sun Java plug-in installed on your system.

Platform	Browser
Windows 7	◆ Firefox 5, 6, 7, 8, 9, and 10 ◆ Internet Explorer 8 and 9 * For information about Internet Explorer 8, see “Prerequisites for Internet Explorer” on page 14.
SLES 11 SP1 and RHEL 6	◆ Firefox 5, 6, 7, 8, 9, and 10 For more information, see “Manually Updating Firefox Version” on page 14.

Prerequisites for Internet Explorer

If the Internet Security Level is set to High, a blank page appears after logging in to Sentinel and the file download pop-up might be blocked by the browser. To work around this issue, you need to first set the security level to Medium-high and then change to Custom level as follows:

1. Navigate to *Tools* > *Internet Options* > *Security tab* and set the security level to *Medium-high*.
2. Make sure that the *Tools* > *Compatibility View* option is not selected.
3. Navigate to *Tools* > *Internet Options* > *Security tab*> *Custom Level*, then scroll down to the *Downloads* section and select *Enable* under the *Automatic prompting for file downloads* option.

Manually Updating Firefox Version

Sentinel supports Firefox versions 5 through 10; however, the SLES 11 SP1 system is packaged with Firefox version 3.6*x*. Perform the following steps to manually update a SLES 11 SP1 installation to include a supported version of Firefox:

1. Open YaST.
2. Select *Software* > *Software Repositories* to display the Configured Software Repositories window.
3. Click *Add* to open the Media Type window.
4. Select the *Specify URL* option, then click *Next*.

   This displays the Repository URL window.

5 Type the Software Repository (http://download.opensuse.org/repositories/mozilla/SLE_11/) link in the URL text box, then click *Next*.

The software repository is downloaded.

6 Click *OK* to refresh the software repository.

7 Click *Software Management* to open the YaST2 window.

8 Enter `Firefox` in the *Search* text box.

The list of Firefox packages is displayed.

9 Select the required packages for the supported version of Firefox you want to install.

If you select a package that conflicts with the existing version, a Warning dialog box displays. Select the appropriate option, then click the *OK Try Again* button.

10 Click *Accept.*

1.1.5 Data Storage Requirement Estimation

Sentinel is used to retain raw data for a long period of time to comply with legal and other requirements. Sentinel 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 *NetIQ Sentinel 7.0.1 Administration Guide*.

To determine the amount of random-access storage space required for Sentinel, 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 machine, or remotely on the Server Message Block (SMB) protocol or CIFS protocol, the network file system (NFS), or a SAN for Sentinel 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 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 0.00008 = 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 0.00001 = 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 0.000003 = 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 copied to networked storage typically after 2 days. For more information, see "Configuring Data Storage" in the *NetIQ Sentinel 7.0.1 Administration Guide*.
- **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.

1.1.6 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 .002 compression coefficient = data written per second to disk

  For example, at 500 EPS, for an average event size of 758 bytes and an average raw data size of 490 bytes in the log file, data written to disk is determined as follows:

  (758 bytes + 490 bytes) x 500 EPS x .002 = ~1100 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 .00002 compression coefficient = I/O requests per second to disk

  For example, at 500 EPS, for an average event size of 758 bytes and an average raw data size of 490 bytes in the log file, number of I/O requests per second to the disk is determined as follows:

  (758 bytes + 490 bytes) x 500 EPS x .00002 = ~10 transfers per second
- **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 .003 compression coefficient = Blocks written per second to disk

  For example, at 500 EPS, for an average event size of 758 bytes and an average raw data size of 490 bytes in the log file, number of blocks written per second to the disk is determined as follows:

  (758 bytes + 490 bytes) x 500 EPS x .003 = ~1800 blocks per second

- **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 .40 compression coefficient = kilobytes read per second from disk

  For example, at 5 millions of events matching the search query, for an average event size of 758 bytes and an average raw data size of 490 bytes in the log file, data read per second from the disk is determined as follows:

  (758 bytes + 490 bytes) x 5 x .40 = ~500 KB

1.1.7 Network Bandwidth Utilization Estimation

Use the following formulas to estimate the network bandwidth utilization between the Sentinel server and remote Collector Manager 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 758 bytes and an average raw data size of 490 bytes in the log file, the network bandwidth utilization is determined as follows:

(758 bytes + 490 bytes} x 500 EPS x .0003 = ~175 Kbps

1.1.8 Virtual Environment

Sentinel is extensively tested and fully supported on a VMware ESX server. When you set up a virtual environment, the virtual machines must have 2 or more CPUs. 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, disk space, and I/O as the physical machine recommendations.

For information on physical machine recommendations, see Section 1.1, “System Requirements and Supported Platforms,” on page 11.

1.2 Connector and Collector System Requirements

Each Connector and Collector has its own set of system requirements and supported platforms. See the Connector and Collector documentation on the Sentinel Plug-ins Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

1.3 Ports Used

- Section 1.3.1, “Sentinel Server,” on page 17
- Section 1.3.2, “Collector Manager,” on page 19
- Section 1.3.3, “Correlation Engine,” on page 20

1.3.1 Sentinel Server

Local Ports

Sentinel uses the following ports for internal communication with database and other internal processes:

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 the Sentinel Plug-in SDK Web site (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).
TCP 27017	Used for the Security Intelligence configuration database.
TCP 28017	Used for the Web interface for Security Intelligence database.
TCP 32000	Used for internal communication between the wrapper process and the server process.

Network Ports

Sentinel uses different ports for external communication with other components. For the appliance installation, the ports are opened on the firewall by default. However, for the standard installation, you need to configure the operating system on which you are installing Sentinel in order to open the ports on the firewall.

For Sentinel to work properly, ensure that the following ports are open on the firewall:

Ports	Description
TCP 1099 and 2000	Used together by monitoring tools to connect to Sentinel server process using Java Management Extensions (JMX).
TCP 1289	Used for Audit connections.
UDP 1514	Used for syslog messages.
TCP 8443	Used for HTTPS communication.
TCP 1443	Used for SSL encrypted syslog messages.
TCP 61616	Used for communication between Collector Managers and the server.
TCP 10013	Used by the Sentinel Control Center and Solution Designer.
TCP 1468	Used for syslog messages.
TCP 10014	Used by the remote Collector Managers to connect to the server through the SSL proxy. However, this is uncommon. By default, remote Collector Managers use the SSL port 61616 to connect to the server.

Sentinel Server Appliance Specific Ports

In addition to the above ports, the following ports are open on Sentinel server appliance.

Ports	Description
TCP 22	Used for secure shell access to the Sentinel appliance.
TCP 54984	Used by the Sentinel Appliance Management Console (WebYaST). Also used by the Sentinel appliance for the update service.
TCP 289	Forwarded to 1289 for Audit connections.
UDP 443	Forwarded to 8443 for HTTPS communication.
UDP 514	Forwarded to 1514 for syslog messages.
TCP 1290	This is the Sentinel Link port that is allowed to connect through the SuSE Firewall.
UDP and TCP 40000 - 41000	Ports that can be used when configuring data collection servers, such as syslog. Sentinel does not listen on these ports by default.

1.3.2 Collector Manager

Network Ports

For Sentinel Collector Manager to work properly, ensure that the following ports are open on the firewall:

Ports	Description
TCP 1289	Used for Audit connections.
UDP 1514	Used for syslog messages.
TCP 1443	Used for SSL encrypted syslog messages.
TCP 1468	Used for syslog messages.
TCP 1099 and 2000	Used together by monitoring tools to connect to Sentinel server process using Java Management Extensions (JMX).

Collector Manager Appliance Specific Ports

In addition to the above ports, the following ports are open on Sentinel Collector Manager appliance.

Ports	Description
TCP 22	Used for secure shell access to the Sentinel appliance.
TCP 54984	Used by the Sentinel Appliance Management Console (WebYaST). Also used by the Sentinel appliance for the update service.
TCP 289	Forwarded to 1289 for Audit connections.
UDP 514	Forwarded to 1514 for syslog messages.
TCP 1290	This is the Sentinel Link port that is allowed to connect through the SuSE Firewall.
UDP and TCP 40000 - 41000	Ports that can be used when configuring data collection servers, such as syslog. Sentinel does not listen on these ports by default.

1.3.3 Correlation Engine

Network Ports

For Sentinel Correlation Engine to work properly, ensure that the following ports are open on the firewall:

Ports	Description
TCP 1099 and 2000	Used together by monitoring tools to connect to Sentinel server process using Java Management Extensions (JMX).

Correlation Engine Appliance Specific Ports

In addition to the above ports, the following ports are open on Sentinel Correlation Engine appliance.

Ports	Description
TCP 22	Used for secure shell access to the Sentinel appliance.
TCP 54984	Used by the Sentinel Appliance Management Console (WebYaST). Also used by the Sentinel appliance for the update service.

2 Installing Sentinel

Sentinel can be installed either as a stand-alone install or as an appliance install. The stand-alone installer installs Sentinel on an existing SUSE Linux Enterprise Server (SLES) 11 SP1 or Red Hat Enterprise Linux (RHEL) 6 operating system. The appliance installer installs both the SLES 11 SP1 64-bit operating system and Sentinel.

This section describes the procedure for a stand-alone installation of the Sentinel server on an existing SLES 11 SP1 system or RHEL 6. For appliance install, see Chapter 5, "Installing the Appliance," on page 39.

- Section 2.1, "Installation Methods," on page 21
- Section 2.2, "Before You Begin," on page 22
- Section 2.3, "Installation Options," on page 23
- Section 2.4, "Interactive Installation," on page 24
- Section 2.5, "Silent Installation," on page 26
- Section 2.6, "Installing Sentinel as a Non-root User," on page 27
- Section 2.7, "Modifying the Configuration after Installation," on page 28

2.1 Installation Methods

The following methods are available for stand-alone installation:

- **Interactive:** The installation proceeds with user inputs. During installation, you can record the installation options (user inputs or default values) to a file, which later can be used for silent installation.
- **Silent:** You can use this option if the installation options are pre-recorded. The Silent installation refers to the file that has the recorded installation input and performs the installation with the values captured in the file. The silent install is effective when you want to install many replicas of the same configuration in your environment. For more information, see Section 2.5, "Silent Installation," on page 26.

Both the interactive and silent installation of Sentinel can be done either as a `root` user or a non-root user.

- Section 2.1.1, "Standard and Custom Installation," on page 22
- Section 2.1.2, "Components Installed," on page 22

2.1.1 Standard and Custom Installation

When you install Sentinel, the following configurations are available:

- **Standard:** In this configuration, the installation uses default values for the configuration setup. User input is required only for the password. For more information on installing Sentinel with the standard configuration, see Section 2.4.1, "Standard Configuration," on page 24.
- **Custom:** In this configuration, the installation prompts you to specify the values for the configuration setup. You can either select the default values or specify the necessary values. For more information on installing Sentinel with a custom configuration, see Section 2.4.2, "Custom Configuration," on page 25.

Standard Configuration	Custom Configuration
Installs with default 90-day evaluation key.	Allows you to install with the 90-day license key or with a valid license key.
Allows you to specify the admin password and uses the admin password as the default password for both dbauser and appuser.	Allows you to specify the admin password. For dbauser and appuser, you can either specify new password or use admin password.
Installs the default ports for all the components.	Allows you to specify ports for different components.
Authenticates users with the internal database.	Gives the option to authenticate users either with the internal database or LDAP authentication.

2.1.2 Components Installed

There are multiple components in Sentinel. All of the following components are installed by default:

- Sentinel server
- Correlation Engine
- Collector Manager

Additional Correlation Engines or Collector Managers can be installed on different systems.

2.2 Before You Begin

Verify that you have completed the following tasks before you start the installation:

- Verify that your hardware and software meet the system requirements listed in Section 1.1, "System Requirements and Supported Platforms," on page 11.
- If there was a previous installation of Sentinel, ensure that there are no files or system settings remaining from a previous installation. For more information, see Part V, "Uninstalling," on page 93.
- For optimal performance, stability, and reliability of Sentinel server, use the ext3 file system on SLES and ext4 file system on RHEL. For more information on file systems, see Overview of File Systems in Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) in the *Storage Administration Guide*.
- Configure the network settings such that the system has a valid IP address and a valid hostname.
- Obtain your license key from the Novell Customer Care Center if you plan to install the licensed version.

- Synchronize time by using the Network Time Protocol (NTP).
- Ensure that the ports listed in Section 1.3, “Ports Used,” on page 17 are opened in the firewall.
- For optimal performance, the memory settings must be appropriate for the PostgreSQL database:

  The SHMMAX parameter must be greater than or equal to 1073741824. To set the appropriate value, append the following information in the `/etc/sysctl.conf` file:

  ```
  # for Sentinel Postgresql
  kernel.shmmax=1073741824
  ```
- For a minimal or headless installation, the operating system for the Sentinel server must include at least the Base Server components of the SLES server or the RHEL 6 server. Sentinel requires the 64-bit versions of the following RPMs:
  - bash
  - bc
  - coreutils
  - glibc
  - grep
  - libgcc
  - libstdc
  - lsof
  - net-tools
  - openssl
  - python-libs
  - sed
  - zlib

2.3 Installation Options

`./install-sentinel --help` displays the following options:

Options	Value	Description
--location	Directory	Specifies a directory other than the root (/) to install Sentinel.
-m, --manifest	File name	Specifies a product manifest file to use instead of the default manifest file.
--no-configure		Specifies to not configure the product after installation.
-n, --no-start		Specifies to not start or restart Sentinel after installation or configuration.
-r, --recordunattended	Filename	Specifies a file to record the parameters that can be used for unattended installation.
-u, --unattended	Filename	Uses the parameters from the specified file in order to install Sentinel on unattended systems.

Options	Value	Description
-h, --help		Displays the options that can be used while installing Sentinel.
-l, --log-file	Filename	Records log messages to a file.
--no-banner		Suppresses the display of banner message.
-q, --quiet		Displays fewer messages.
-v, --verbose		Displays all messages during installation.

2.4 Interactive Installation

- Section 2.4.1, "Standard Configuration," on page 24
- Section 2.4.2, "Custom Configuration," on page 25

2.4.1 Standard Configuration

1 Download the Sentinel installation file from the Novell Downloads Web page (http://download.novell.com/index.jsp):

1a In the *Product or Technology* field, browse to and select *SIEM-Sentinel*.

1b Click *Search*.

1c Click the button in the *Download* column for *Sentinel 7.0 Evaluation*.

1d Click *proceed to download*, then specify your customer name and password.

1e Click *download* for the installation version for your platform.

2 Specify at the command line the following command to extract the installation file.

```
tar zxvf <install_filename>
```

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

3 Change to the directory where you extracted the installer:

```
cd sentinel_server-7.0.0.0.x86_64
```

4 Specify the following command to install Sentinel:

```
./install-sentinel
```

or

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

```
./install-sentinel -r <response_filename>
```

5 Specify the number for the language you want to use for the installation, then press Enter.

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

6 Press the Spacebar to read through the license agreement.

7 Enter `yes` or `y` to accept the license and continue with the installation.

The installation might take a few seconds to load the installation packages and prompt for the configuration type.

8 When prompted, specify `1` to proceed with the standard configuration.

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

9 Specify the password for the administrator user `admin`.

10 Confirm the password again.

This password is used by `admin`, `dbauser`, and `appuser`.

The Sentinel installation finishes and the server starts. It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

To access the Sentinel Web interface, specify the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443.
```

The <*IP_Address_Sentinel_server*> is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

2.4.2 Custom Configuration

If you are installing Sentinel with a custom configuration, you can specify the license key, change the password for different users, and specify values for different ports that are used to interact with the internal components.

1 Download the Sentinel installation file from the Novell Downloads Web page (http://download.novell.com/index.jsp):

1a In the *Product or Technology* field, browse to and select *SIEM-Sentinel*.

1b Click *Search*.

1c Click the button in the *Download* column for *Sentinel 7.0 Evaluation*.

1d Click *proceed to download*, then specify your customer name and password.

1e Click *download* for the installation version for your platform.

2 Specify at the command line the following command to extract the installation file.

```
tar zxvf <install_filename>
```

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

3 Specify the following command in the root of the extracted directory to install Sentinel:

```
./install-sentinel
```

or

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

```
./install-sentinel -r <response_filename>
```

4 Specify the number for the language you want to use for the installation, then press Enter.

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

5 Press the Spacebar to read through the license agreement.

6. Enter yes or y to accept the license agreement and continue with the installation.

   The installation might take a few seconds to load the installation packages and prompt for the configuration type.

7. Specify 2 to perform a custom configuration of Sentinel.

8. Enter 1 to use the default 90-day evaluation license key

   or

   Enter 2 to enter a purchased license key for Sentinel.

9. Specify the password for the administrator user admin and confirm the password again.

10. Specify the password for the database user dbauser and confirm the password again.

    The dbauser account is the identity used by Sentinel to interact with the database. The password you enter here can be used to perform database maintenance tasks, including resetting the admin password if the admin password is forgotten or lost.

11. Specify the password for the application user appuser and confirm the password again.

12. Change the port assignments for the Sentinel services by entering the desired number, then specifying the new port number.

13. After you have changed the ports, specify 7 for done.

14. Enter 1 to authenticate users using only the internal database.

    or

    If you have configured an LDAP directory in your domain, enter 2 to authenticate users by using LDAP directory authentication.

    The default value is 1.

    The Sentinel installation finishes and the server starts. It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

To access the Sentinel Web interface, specify the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443.
```

The <*IP_Address_Sentinel_server*> is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

2.5 Silent Installation

The silent or unattended installation of Sentinel is useful if you need to install more than one Sentinel server in your deployment. In such a scenario, you can record the installation parameters during the interactive installation and then run the recorded file on all the other servers. You can record the installation parameters while installing Sentinel with the standard configuration or a custom configuration.

To perform silent installation, ensure that you have recorded the installation parameters to a file. For information on creating the response file, see Section 2.4.1, “Standard Configuration,” on page 24 or Section 2.4.2, “Custom Configuration,” on page 25.

1. Download the installation files from the Novell Downloads Web page (http://download.novell.com/index.jsp).

2. Log in as root to the server where you want to install Sentinel.

3. Specify the following command to extract the install files from the tar file:

```
tar -zxvf <install_filename>
```

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

4 Specify the following command to install Sentinel in silent mode:

```
./install-sentinel -u <response_file>
```

The installation proceeds with the values stored in the response file.

The Sentinel installation finishes and the server starts. It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

To access the Sentinel Web interface, specify the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443.
```

The <*IP_Address_Sentinel_server*> is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

2.6 Installing Sentinel as a Non-root User

If your organizational policy does not allow you to run the full installation of Sentinel as `root`, you can install Sentinel as another user. In this installation, few steps are performed as a `root` user, then you proceed to install Sentinel as another user created by the `root` user. Finally, the `root` user completes the installation.

1 Download the installation files from the Novell Downloads Web page (http://download.novell.com/index.jsp)

2 Specify the following command at the command line to extract the install files from the tar file:

```
tar -zxvf <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 as `root`.

4 Specify the following command:

```
./bin/root_install_prepare
```

A list of commands to be executed with root privileges is displayed. If you want the non-root user to install Sentinel in non-default location, specify the --location option along with the command. For example:

```
./bin/root_install_prepare --location=/foo
```

The value that you pass to the `--location` option `foo` is prepended to the directory paths.

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

5 Accept the command list.

The displayed commands are executed.

6 Specify the following command to change to the newly created non-root `novell` user: `novell`:

```
su novell
```

7 (Conditional) To do an interactive installation:

7a Specify the following command:

```
./install-sentinel
```

To install Sentinel in non-default location, specify the --location option along with the command. For example:.

```
./install-sentinel --location=/foo
```

7b Continue with Step 9.

8 (Conditional) To do a silent installation:

8a Specify the following command:

```
./install-sentinel -u <response_file>
```

The installation proceeds with the values stored in the response file.

8b Continue with Step 12.

9 Specify the number for the language you want to use for the installation.

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 configuration, continue with Step 8 through Step 10 in Section 2.4.1, "Standard Configuration," on page 24.
- If you select to proceed with the custom configuration, continue with Step 7 through Step 14 in Section 2.4.2, "Custom Configuration," on page 25.

12 Log in as a `root` user and specify the following command to finish installation:

```
./bin/root_install_finish
```

The Sentinel installation finishes and the server starts. It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

To access the Sentinel Web interface, specify the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443.
```

The <*IP_Address_Sentinel_server*> is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

2.7 Modifying the Configuration after Installation

After installing Sentinel, if you want to enter the valid license key, change the password or modify any of the assigned ports, you can run the `configure.sh` script to modify them. The script is found in the `/opt/novell/sentinel/setup` folder.

1 Specify the following command at the command line to run the `configure.sh` script:

```
./configure.sh
```

2 Specify `1` to perform a standard configuration or specify `2` to perform a custom configuration of Sentinel.

3 Press the Spacebar to read through the license agreement.

4 Enter `yes` or `y` to accept the license agreement and continue with the installation.

The installation might take a few seconds to load the installation packages.

5. Enter `1` to use the default 90-day evaluation license key

   or

   Enter `2` to enter a purchased license key for Sentinel.

6. Decide whether you want to keep the existing password for the `admin` administrator user.

   - If you want to keep the existing password, enter `1`, then continue with Step 7.
   - If you want to change the existing password, enter `2`, specify the new password, confirm the password, then continue with Step 7.

7. Decide whether you want to keep the existing password for the `dbauser` database user.

   - If you want to keep the existing password, enter `1`, then continue with Step 8.
   - If you want to change the existing password, enter `2`, specify the new password, confirm the password, then continue with Step 8.

   The `dbauser` account is the identity used by Sentinel to interact with the database. The password you enter here can be used to perform database maintenance tasks, including resetting the admin password if the admin password is forgotten or lost.

8. Decide whether you want to keep the existing password for the `appuser` application user.

   - If you want to keep the existing password, enter `1`, then continue with Step 9.
   - If you want to change the existing password, enter `2`, specify the new password, confirm the password, then continue with Step 9.

   The `dbauser` account is the identity used by Sentinel to interact with the database. The password you enter here can be used to perform database maintenance tasks, including resetting the admin password if the admin password is forgotten or lost.

9. Change the port assignments for the Sentinel services by entering the desired number, then specifying the new port number.

10. After you have changed the ports, specify 7 for done.

11. Enter `1` to authenticate users using only the internal database.

    or

    If you have configured an LDAP directory in your domain, enter `2` to authenticate users by using LDAP directory authentication.

    The default value is `1`.

3 Installing Additional Collector Managers

By default, Sentinel installs one Collector Manager. Depending on your environment, you might need more than one Collector Manager. Use the following information to install remote Collector Managers.

IMPORTANT: You cannot install another Collector Manager or Correlation Engine on the same server where Sentinel is running.

3.1 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, which increases 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.
- **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, which do not natively support event caching.

3.2 Before You Begin

Verify that you have completed the following tasks before starting the installation.

- ❐ Make sure that your hardware and software meet the minimum requirements. For more information, see Section 1.1, "System Requirements and Supported Platforms," on page 11.
- ❐ Synchronize time by using the Network Time Protocol (NTP).
- ❐ A Collector Manager requires network connectivity to the message bus port (61616) on the Sentinel server. Before you start installing the Collector Manager, make sure that all firewall and network settings are allowed to communicate over this port.

3.3 Installing an Additional Collector Manager

You must install the remote Collector Manager on a different system than where Sentinel or the remote Correlation Engine is installed.

1 Launch the Sentinel Web interface by specifying the following URL in your Web browser:

```
https://<IP_Address_Sentinel_server>:8443.
```

The <*IP_Address_Sentinel_server*> is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

Log in with the username and password specified during the installation of the Sentinel server.

2 In the toolbar, click *Downloads*.

3 Under the Collector Manager heading, click *Download Installer*.

4 Click *Save File* to save the installer to the desired location.

5 Specify the following command to extract the installation file.

```
tar zxvf <install_filename>
```

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

6 Change to the directory where you extracted the installer. For example:

```
cd sentinel_collector_mgr-7.0.0.0.x86_64
```

7 Specify the following command to install Sentinel Collector Manager:

```
./install-cm
```

The install script first checks for the available memory and disk space. If the available memory is less than 1.5 GB, the script automatically terminates the installation.

8 Specify the number for the language you want to use for the installation.

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

9 Press the Spacebar to read through the license agreement.

10 Enter `yes` or `y` to accept the license agreement and continue with the installation.

The installation might take a few seconds before prompting for the configuration type.

11 When prompted, specify 1 to proceed with the standard configuration.

12 Enter default Communication Server Hostname or IP Address of the machine on which Sentinel is installed.

13 Specify the username and password for the Collector Manager.

The username and password are stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located in the Sentinel server.

For example:

```
collectormanager=1c51ae55
```

In this example, `collectormanager` is the username and the corresponding value is the password.

14 Accept the certificate permanently when prompted.

The remote Sentinel Collector Manager installation is complete.

3.4 Adding a Custom User for a Collector Manager

Sentinel recommends that you use the default Collector Manager username of collectormanager. However, if you have installed multiple remote Collector Managers and you want to identify them separately, you can create new users:

1 Log in to the server as the user who has access to the installation files for Sentinel.

2 Open the activemqgroups.properties file.

This file is located in the /<*install_dir*>/etc/opt/novell/sentinel/config/ directory.

3 Add the new Collector Manager user under the cm section, separated by comma. For example:

```
cm=collectormanager,cmuser1,cmuser2,...
```

4 Save and close the file.

5 Open the activemqusers.properties file.

This file is located in the /<*install_dir*>/etc/opt/novell/sentinel/config/ directory.

6 Add the password for the user you created in Step 3.

The password can be any random string. For example:

```
system=c7f34372ecd20d831cceb29e754e5ac9
collectormanager=1c51ae56
cmuser1=1b51de55
cmuser2=1a51ce57
```

7 Save and close the file.

8 Restart the Sentinel server.

4 Installing Additional Correlation Engines

By default, Sentinel installs one Correlation Engine. For environments with large numbers of correlation rules or extremely high event rates, it might be advantageous to install more than one Correlation Engine. For information on recommended event rates per Correlation Engine, see Correlation Engine in Chapter 1, "Meeting System Requirements," on page 11.

IMPORTANT: You cannot install another Collector Manager or Correlation Engine on the server where Sentinel is running.

- Section 4.1, "Before You Begin," on page 35
- Section 4.2, "Installing an Additional Correlation Engine," on page 35
- Section 4.3, "Adding a Custom User for the Correlation Engine," on page 36

4.1 Before You Begin

Verify that you have completed the following tasks before starting the installation.

- □ Make sure that your hardware and software meet the minimum requirements. For more information, see Section 1.1, "System Requirements and Supported Platforms," on page 11.
- □ Synchronize time by using the Network Time Protocol (NTP).
- □ A Correlation Engine requires network connectivity to the message bus port (61616) on the Sentinel server. Before you start installing the Correlation Engine, make sure that all firewall and network settings are allowed to communicate over this port.

4.2 Installing an Additional Correlation Engine

You must install the remote Correlation Engine on a different system than the one where Sentinel or an remote Collector Manager is installed.

1. Launch the Sentinel Web interface by specifying the following URL in your Web browser:

   ```
   https://<IP_Address_Sentinel_server>:8443.
   ```

   The <*IP_Address_Sentinel_server*> is the IP address or DNS name of the Sentinel server and 8443 is the default port for the Sentinel server.

   Log in with the username and password specified during the installation of the Sentinel server.
2. In the toolbar, click *Downloads*.
3. Under the Correlation Engine heading, click *Download Installer*.
4. Click *Save File* to save the installer to the desired location.
5. Specify the following command to extract the installation file.

```
tar zxvf <install_filename>
```

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

6 Change to the directory where you extracted the installer. For example:

```
cd sentinel_correlation_engine-7.0.0.0.x86_64
```

7 Specify the following command to install Sentinel Correlation Engine:

```
./install-ce
```

The install script first checks for the available memory and disk space. If the available memory is less than 1.5 GB, the script automatically terminates the installation.

8 Specify the number for the language you want to use for the installation.

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

9 Press the Spacebar to read through the license agreement.

10 Enter `yes` or `y` to accept the license agreement and continue with the installation.

The installation might take a few seconds to load the installation packages and prompt for the configuration type.

11 When prompted, specify 1 to proceed with the standard configuration.

12 Enter default Communication Server Hostname or IP Address of the machine on which Sentinel is installed.

13 Specify the username and password for the Correlation Engine.

The username and password are stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located in the Sentinel server.

For example:

```
correlationengine=68790d7a
```

In this example, `correlationengine` is the username and the corresponding value is the password.

14 Accept the certificate permanently when prompted.

The remote Sentinel Correlation Engine installation is complete.

4.3 Adding a Custom User for the Correlation Engine

Sentinel recommends that you use the default Correlation Engine username of `correlationengine`. However, if you have installed multiple remote Correlation Engines and you want to identify them separately, you can create new users:

1 Log in to the server as the user who has access to the installation files for Sentinel.

2 Open the `activemqgroups.properties` file.

This file is located in the `/<install_dir>/etc/opt/novell/sentinel/config/` directory.

3 Add the new Correlation Engine user in the `admin` section, separated by a comma. For example:

```
admins=system,correlationengine,ceuser1,ceuser2,...
```

4 Save and close the file.

5 Open the `activemqusers.properties` file.

This file is located in the `/<install_dir>/etc/opt/novell/sentinel/config/` directory.

6 Add the password for the user you created in Step 3.

The password can be any random string. For example:

```
system=c7f34372ecd20d831cceb29e754e5ac9
correlationengine=68790d7a
ceuser1=69700c6d
ceuser2=70701b5c
```

7 Save and close the file.

8 Restart the Sentinel server.

5 Installing the Appliance

The Sentinel appliance is a ready-to-run software appliance built on SUSE Studio. The appliance combines a hardened SUSE Linux Enterprise Server (SLES) 11 SP 1 operating system and the Sentinel software integrated update service to provide an easy and seamless user experience that allows customers to leverage existing investments. The software appliance can be installed on hardware or in a virtual environment.

- Section 5.1, “Before You Begin,” on page 39
- Section 5.2, “Installing the VMware Appliance,” on page 39
- Section 5.3, “Installing the Xen Appliance,” on page 42
- Section 5.4, “Installing the Appliance on Hardware,” on page 46
- Section 5.5, “Post-Installation Configuration for the Appliance,” on page 48
- Section 5.6, “Configuring WebYaST,” on page 49
- Section 5.7, “Configuring the Appliance with SMT,” on page 49
- Section 5.8, “Stopping and Starting the Server by Using the Web Interface,” on page 51
- Section 5.9, “Registering for Updates,” on page 51

5.1 Before You Begin

Make sure that you have completed the following tasks before you start installing the installation of the appliance.

- ❒ Verify that the hardware requirements are met. For more information, see Section 1.1, “System Requirements and Supported Platforms,” on page 11.
- ❒ Obtain your license key from the Novell Customer Care Center if you plan to install the licensed version.
- ❒ Obtain your registration code from the Novell Customer Care Center to register for software updates.

5.2 Installing the VMware Appliance

- Section 5.2.1, “Installing Sentinel,” on page 40
- Section 5.2.2, “Installing the Collector Manager,” on page 41
- Section 5.2.3, “Installing the Correlation Engine,” on page 42

5.2.1 Installing Sentinel

To import and install the Sentinel appliance image on a VMware ESX server:

1 Download the VMware appliance installation file from the Novell Download Web site (http://download.novell.com/index.jsp).

The correct file for the VMware appliance has `vmx` in the filename. For example, `sentinel_server_7.0.0.0.x86_64.vmx.tar.gz`

2 Establish an ESX datastore to which the appliance image can be installed.

3 Log in as Administrator to the server where you want to install the appliance.

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

```
tar zxvf <install_file>
```

Replace <*install_file*> with the actual filename.

5 To import the VMware image to the ESX server, use the VMware Converter and follow the on-screen instructions in the installation wizard.

6 Log in to the ESX server machine.

7 Select the imported VMware image of the appliance and click the *Power On* icon.

8 Select the language of your choice, then click *Next*.

9 Select the keyboard layout, then click *Next*.

10 Read and accept the SUSE Linux Enterprise Server (SLES) 11 SP1 Software License Agreement.

11 Read and accept the NetIQ Sentinel End User License Agreement.

12 On the Hostname and Domain Name page, specify the hostname and domain name, then ensure that the *Assign Hostname to Loopback IP* option is selected.

13 Click *Next*. The hostname configurations are saved.

14 Do one of the following:

- To use the current network connection settings, select *Use Following Configuration* on the Network Configuration II page, then click *Next*.
- To change the network connection settings, select *Change*, make the desired changes, then click *Next*.

The network connection settings are saved.

15 Set the time and date, then click *Next*.

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
```

16 Set the `root` password, then click *Next*.

The installation checks for the available memory and disk space. If the available memory is less than 2.5 GB, the installation will not let you proceed and the *Next* button is greyed out.

If the available memory is more than 2.5 GB but less than 6.7 GB, the installation displays a message that you have less memory than is recommended. When this message is displayed, click *Next* to continue with the installation.

17 Set Sentinel admin password, then click *Next*.

It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

18 Make a note of the appliance IP address that is shown in the console.

19 Proceed with Section 5.5, "Post-Installation Configuration for the Appliance," on page 48.

5.2.2 Installing the Collector Manager

To import and install the appliance image on the VMWare ESX server:

1 Download the VMware appliance installation file from the Novell Download Web site (http://download.novell.com/index.jsp).

The correct file for the VMware appliance has `vmx` in the filename. For example, `sentinel_colletor_manager_7.0.0.0.x86_64.vmx.tar.gz`

2 Establish an ESX datastore to which the appliance image can be installed.

3 Log in as Administrator to the server where you want to install the appliance.

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

```
tar zxvf <install_file>
```

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

5 To import the VMware image to the ESX server, use the VMware Converter and follow the on-screen instructions in the installation wizard.

6 Log in to the ESX server machine.

7 Select the imported VMware image of the appliance and click the *Power On* icon.

8 Specify the host name/IP address of the Sentinel server that the Collector Manager should connect to.

9 Specify the Communication Server port number. The default message bus port is `61616`.

10 Specify the JMS User Name, which is the Collector Manager username. The default username is `collectormanager`.

11 Specify the password for the JMS User.

The username and password are stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located on the Sentinel server.

12 (Optional) To verify the password, see the following line in the `activemqusers.properties`

```
collectormanager=<password>
```

In this example, `collectormanager` is the username and the corresponding value is the password.

13 Click *Next*.

14 Accept the certificate when prompted.

15 Click *Next* to complete the installation.

When the installation is complete, it displays a message indicating that this appliance is the Sentinel Collector Manager, along with the IP address. It also displays the Sentinel server user interface IP address.

5.2.3 Installing the Correlation Engine

Installing the Correlation Engine appliance is similar to installing Collector Manager appliance.

1 Download the VMware appliance installation file from the Novell Download Web site (http://download.novell.com/index.jsp).

   The correct file for the VMware Correlation Engine appliance has `vmx` in the filename. For example, `sentinel_correlation_engine_7.0.0.0.x86_64.vmx.tar.gz`

2 Establish an ESX datastore to which the appliance image can be installed.

3 Log in as Administrator to the server where you want to install the appliance.

4 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 filename.

5 To import the VMware image to the ESX server, use the VMware Converter and follow the on-screen instructions in the installation wizard.

6 Log in to the ESX server machine.

7 Select the imported VMware image of the appliance and click the *Power On* icon.

8 Specify the hostname/IP address of the Sentinel server that the Correlation Engine should connect to.

9 Specify the Communication Server port number. The default message bus port is `61616`.

10 Specify the JMS User Name, which is the Correlation Engine username. The default username is `correlationengine`.

11 Specify the password for the JMS User.

   The username and password are stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located on the Sentinel server.

12 (Optional) To verify the password, see the following line in the `activemqusers.properties` file:

   ```
   correlationengine=<password>
   ```

   In this example, `correlationengine` is the username and the corresponding value is the password.

13 Click *Next*.

14 Accept the certificate when prompted.

15 Click *Next* to complete the installation.

   When the installation is finished, it displays a message indicating that this appliance is the Sentinel Correlation Engine, along with the IP address. It also displays the Sentinel server user interface IP address.

5.3 Installing the Xen Appliance

- Section 5.3.1, “Installing Sentinel,” on page 43
- Section 5.3.2, “Installing the Collector Manager,” on page 44
- Section 5.3.3, “Installing the Correlation Engine,” on page 45

5.3.1 Installing Sentinel

1 Download the Xen virtual appliance installation file from the Novell Download Web site (http://download.novell.com/index.jsp) to `/var/lib/xen/images`.

The correct filename for the Xen virtual appliance contains `xen`. For example, `Sentinel_7.0.0.0.x86_64.xen.tar.gz`

2 Specify the following command to unpack the file:

```
tar -zxvf <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`
- `<file_name>.xenconfig`

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 the `name` and `memory` settings.

For example:

```
# -*- mode: python; -*-
name="Sentinel_7.0.0.0.x86_64"
memory=4096
disk=[ "tap:aio:/var/lib/xen/images/sentinel_7.0.0.0.x86_64/
sentinel_7.0.0.0.x86_64.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 that is generated.

For example, if you have configured `name="Sentinel_7.0.0.0.x86_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_7.0.0.0.x86_64
```

The installation first checks for the available memory and disk space. If the available memory is less than 2.5 GB, the installation is automatically terminated. If the available memory is more than 2.5 GB but less than 6.7 GB, the installation displays a message that you have less memory than is recommended. Enter `y` if you want to continue with the installation, or enter `n` if you do not want to proceed.

9 Select the language of your choice, then click *Next*.

10 Select the keyboard layout, then click *Next*.

11 Read and accept the SUSE Linux Enterprise Server (SLES) 11 SP1 Software License Agreement.

12 Read and accept the NetIQ Sentinel End User License Agreement.

13 On the Hostname and Domain Name page, specify the hostname and domain name, then 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* on the *Network Configuration II* page.
- To change the network connection settings, select *Change*, then make the desired changes.

16 Select *Next*. The network connection settings are saved.

17 Set the time and date, click *Next*, then click *Finish*

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
```

18 Set the SUSE Enterprise Server `root` password, then click *Next*.

19 Set Sentinel admin password, then click *Next*.

The Sentinel installation proceeds and completes. It might take few minutes for all services to start up after installation as the system performs a one time initialization. Wait until the installation finishes before you log in to the server.

Make a note of the appliance IP address that is shown in the console.

20 Proceed with Section 5.5, "Post-Installation Configuration for the Appliance," on page 48.

5.3.2 Installing the Collector Manager

You can install the Collector Manager as an appliance on a Xen-enabled Linux system that meets the minimum hardware requirements for Collector Manager. For more information, see Section 1.1.2, "Hardware Requirements," on page 12.

1 Complete Step 1 through Step 14 in Section 5.3.1, "Installing Sentinel," on page 43.

The correct filename for the Xen Collector Manager virtual appliance installation file is `sentinel_collector_manager_7.0.0.0.x86_64.xen.tar.gz`

2 On the Network Configuration II screen, select *Change* and specify the IP address of the virtual machine where you want to install the additional Collector Manager appliance.

3 Specify the subnet mask of the specified IP.

4 Select *Next*. The network connection settings are saved.

5 Set the time and date, then select *Next*.

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
```

6. Set the SUSE Enterprise Server `root` password, then select *Next*.
7. Specify the hostname/IP address of the Sentinel server that the Correlation Engine should connect to.
8. Specify the Communication Server port number. The default message bus port is `61616`.
9. Specify the JMS User Name, which is the Collector Manager username. The default username is `collectormanager`.
10. Specify the password for the JMS User.

    The username and password are stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located on the Sentinel server.
11. (Optional) To verify the password, see the following line in the `activemqusers.properties` file:

    ```
    collectormanager=<password>
    ```

    In this example, `collectormanager` is the username and the corresponding value is the password.
12. Select *Next* to complete the installation.

    When the installation is complete, it displays a message that this appliance is the Sentinel Collector Manager, along with the IP address.

5.3.3 Installing the Correlation Engine

You can install the Correlation Engine as an appliance on a on a Xen-enabled Linux system that meets the minimum hardware requirements for Correlation Engine. For more information, see Section 1.1.2, "Hardware Requirements," on page 12.

1. Complete Step 1 through Step 14 in Section 5.3.1, "Installing Sentinel," on page 43.

   The correct filename for the Xen Correlation Engine virtual appliance installation file is `sentinel_correlation_engine_7.0.0.0.x86_64.xen.tar.gz`
2. On the Network Configuration II screen, select *Change* and specify the IP address of the virtual machine where you want to install the Correlation Engine appliance.
3. Specify the subnet mask of the specified IP.
4. Select *Next*. The network connection settings are saved.
5. Set the time and date, then select *Next*.

   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
   ```
6. Set the SUSE Enterprise Server `root` password, then select *Next*.
7. Specify the hostname/IP address of the Sentinel server that the Correlation Engine should connect to.
8. Specify the Communication Server port number. The default message bus port is `61616`.
9. Specify the JMS User Name, which is the Correlation Engine username. The default user name is `correlationengine`.
10. Specify the password for the JMS User.
11. Click *Next*.

The username and password are stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located on the Sentinel server.

12 To verify the password, see the following line in the `activemqusers.properties` file:

```
correlationengine=<password>
```

In this example, `correlationengine` is the username and the corresponding value is the password.

13 Accept the certificate when prompted.

14 Click *Next* to complete the installation.

When the installation is complete, it displays a the message that this appliance is the Sentinel Correlation Engine, along with the IP address. It also displays the Sentinel server user interface IP address.

5.4 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.

IMPORTANT: Installation on hardware using the ISO disk image (bare metal & Hyper-V) requires minimum memory of 4.5 GB for the installation to complete. For more information on Hardware requirements, see Section 1.1.2, “Hardware Requirements,” on page 12.

- Section 5.4.1, “Installing Sentinel,” on page 46
- Section 5.4.2, “Installing the Collector Manager,” on page 47
- Section 5.4.3, “Installing the Correlation Engine,” on page 48

5.4.1 Installing Sentinel

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.

The installation first checks for the available memory and disk space. If the available memory is less than 2.5 GB, the installation is automatically terminated. If the available memory is more than 2.5 GB but less than 6.7 GB, the installation displays a message that you have less memory than is recommended. Enter `y` if you want to continue with the installation, or enter `n` if you do not want to proceed.

4 Select the language of your choice, then click *Next*.

5 Select the keyboard layout, then click *Next*.

6 Read and accept the SUSE Enterprise Server Software License Agreement.

7 Read and accept the NetIQ Sentinel End User License Agreement.

8 Select *Next*.

9 On the Hostname and Domain Name page, specify the hostname and domain name, then ensure that the *Assign Hostname to Loopback IP* option is selected.

10 Select *Next*.The hostname configurations are saved.

11 Do one of the following:

- To use the current network connection settings, select *Use the following configuration* on the Network Configuration II page.
- To change the network connection settings, select *Change*, then make the desired changes.

12 Select *Next*. The network connection settings are saved.

13 Set the time and date, then click *Next*.

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 `root` password, then click *Next*.

15 Set the Sentinel admin password, then click *Next*.

16 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 the password set in Step 14.

17 Stop Sentinel server:

```
service sentinel stop
```

18 Enter the following command to reset the UI for a clear display in YaST:

```
reset
```

19 To install the appliance on the physical server, run the following command:

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

It might take few minutes for all services to start up after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

20 Make a note of the appliance IP address that is shown in the console.

21 Proceed with Section 5.5, "Post-Installation Configuration for the Appliance," on page 48.

5.4.2 Installing the Collector Manager

You can install Collector Manager as appliance on a system that meets the minimum hardware requirements for Collector Manager. For more information, see Section 1.1.2, "Hardware Requirements," on page 12.

1 Complete Step 1 through Step 14 in Section 5.4.1, "Installing Sentinel," on page 46.

2 Specify the host name/IP address of the Sentinel server that the Collector Manager should connect to.

3 Specify the Communication Server Port number. The default Message bus port is `61616`.

The installation tries to connect to the server with the specified credentials. If you have entered any of these values wrongly, the installation displays an error.

4 Specify the JMS User Name, which is the Collector Manager user name. The default user name is `collectormanager`.

5 Specify the password for the JMS User.

6 Click *Next*.

The username and password is stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located on the Sentinel server.

7 To verify the password, see the following line in the `activemqusers.properties` file:

```
collectormanager=<password>
```

In this example, `collectormanager` is the username and the corresponding value is the password.

8 Accept the certificate when prompted.

9 Click *Next* to complete the installation.

When the installation is complete, it displays a message that this appliance is the Sentinel Collector Manager, along with the IP address. It also displays the Sentinel server user interface IP address.

5.4.3 Installing the Correlation Engine

You can install the Correlation Engine as an appliance on a system that meets the minimum hardware requirements for the Correlation Engine. For more information, see Section 1.1.2, “Hardware Requirements,” on page 12.

1 Complete Step 1 through Step 14 in Section 5.4.1, “Installing Sentinel,” on page 46.

2 Specify the host name/IP address of the Sentinel server that the Correlation Engine should connect to.

3 Specify the Communication Server port number. The default message bus port is `61616`.

4 Specify the JMS User Name, which is the Correlation Engine username. The default username is `correlationengine`.

5 Specify the password for the JMS User.

6 Click *Next*.

The username and password is stored in the `/<install_dir>/etc/opt/novell/sentinel/config/activemqusers.properties` file located on the Sentinel server.

7 To verify the password, see the following line in the `activemqusers.properties` file:

```
correlationengine=<password>
```

In this example, `correlationengine` is the username and the corresponding value is the password.

8 Accept the certificate when prompted.

9 Click *Next* to complete the installation.

When the installation is complete, it displays a message that this appliance is the Sentinel Correlation Engine, along with the IP address. It also displays the Sentinel server user interface IP address.

10 Proceed with Section 5.5, “Post-Installation Configuration for the Appliance,” on page 48.

5.5 Post-Installation Configuration for the Appliance

- Section 5.5.1, “Installing VMware Tools,” on page 49
- Section 5.5.2, “Logging in to the Appliance Web Interface,” on page 49

5.5.1 Installing VMware Tools

For Sentinel 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).

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

5.5.2 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, where 8443 is the default port for the Sentinel server. The Sentinel 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 Configure the Sentinel appliance for data storage and data collection.

  For more information about configuring the appliance, see the *NetIQ Sentinel 7.0.1 Administration Guide*.

3 Register for updates.

  For more information, see Section 5.9, "Registering for Updates," on page 51.

5.6 Configuring WebYaST

The Sentinel appliance user interface is equipped with WebYaST, which is a Web-based remote console for controlling appliances based on SUSE Linux Enterprise. You can access, configure, and monitor the Sentinel 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/).

1 Log in to the Sentinel appliance.

2 Click *Appliance*.

3 Configure the Sentinel Server to receive updates as described in Section 5.9, "Registering for Updates," on page 51.

4 Click *Next* to finish the initial setup.

5.7 Configuring the Appliance with SMT

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

- Section 5.7.1, "Prerequisites," on page 50
- Section 5.7.2, "Configuring the Appliance," on page 51

5.7.1 Prerequisites

- Get the Novell Customer Center credentials for Sentinel to get updates from Novell. For information on getting the credentials, contact Novell Support (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/):
    - SMT Installation
    - SMT Server Configuration
    - Mirroring Installation and Update Repositories with SMT
- Install the `wget` utility on the appliance machine.

5.7.2 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.

5.8 Stopping and Starting the Server by Using the Web Interface

You can start and stop the Sentinel server by using the Web interface as follows:

1. Log in to the Sentinel appliance.
2. Click *Appliance* to launch WebYaST.
3. Click *System Services*.
4. To stop the Sentinel server, click *stop*.
5. To start the Sentinel server, click *start*.

5.9 Registering for Updates

1. Log in to the Sentinel appliance.
2. Click *Appliance* to launch WebYaST.
3. Click *Registration*.
4. Specify the e-mail ID that you want to receive updates, then specify the system name and the appliance registration code.
5. Click *Save*.

6 Troubleshooting the Installation

This section contains some of the issues that might occur during installation, along with the actions to work around the issues.

- Section 6.1, "Failed Installation Because of an Incorrect Network Configuration," on page 53
- Section 6.2, "The UUID Is Not Created for Imaged Collector Managers or Correlation Engine," on page 53

6.1 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 on the appliance fails.

To resolve this issue, properly configure the network settings. To verify the configuration, use the `ifconfig` command to return the valid IP address, and use the `hostname -f` command to return the valid hostname.

6.2 The UUID Is Not Created for Imaged Collector Managers or Correlation Engine

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

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

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

   The Collector Manager automatically generates the UUID.

7 What's Next

After Sentinel is installed, there are two guides to help you configure Sentinel: the *NetIQ Sentinel 7.0.1 Administration Guide* and the *NetIQ Sentinel 7.0.1 User Guide*.

The Administration Guide contains configuration information for tasks only a user with administration rights can perform. For example:

- "Configuring Users and Roles"
- "Configuring Data Storage"
- "Configuring Data Collection"
- "Searching and Reporting Events in a Distributed Environment"

For more information on these and other administration tasks, see the *NetIQ Sentinel 7.0.1 Administration Guide*.

The User Guide contains instructions to help users perform tasks in Sentinel. For example:

- "Searching Events"
- "Analyzing Trends in Data"
- "Reporting"
- "Configuring Incidents"

For more information on these and other user tasks, see the *NetIQ Sentinel 7.0.1 User Guide*.

You can also configure Sentinel to analyze your events, add data using correlation rules, set up baselines, configure workflows to act on the information, and more. Use the information in the *NetIQ Sentinel 7.0.1 Administration Guide* to help you configure these Sentinel features.

II Configuring

After Sentinel is installed, you can configure it to run in your environment.

- Chapter 8, “Accessing the Sentinel Web Interface,” on page 59
- Chapter 9, “Adding Additional Sentinel Components,” on page 61
- Chapter 10, “Managing Data,” on page 63
- Chapter 11, “Configuring Out-of-the-box Content,” on page 65
- Chapter 12, “Configuring Time,” on page 67
- Chapter 13, “License Information,” on page 71
- Chapter 14, “Configuring Sentinel for High Availability,” on page 73

8 Accessing the Sentinel Web Interface

After Sentinel is installed, you can log into the Sentinel Web interface to perform administration tasks and configure Sentinel to collect data.

1. Open a Web browser and log in to https://<*IP address*>:8443, where 8443 is the default port for the Sentinel server.
2. (Conditional) The first time you log in to the Sentinel, accept the certificate when you are prompted.

   The Sentinel login page is displayed when you accept the certificate.
3. Specify the username and password for the Sentinel administrator.
4. Click *Log in*.

   The NetIQ Sentinel Web interface is displayed.

9 Adding Additional Sentinel Components

By default, Sentinel has a Syslog Connector and Collector installed and configured, as well as different Audit Connectors and different Novell product Collectors. The following sections explain how to install and configure additional Connectors and Collectors.

- Section 9.1, "Installing Collectors and Connectors," on page 61
- Section 9.2, "Adding Additional Collectors and Connectors," on page 62

9.1 Installing Collectors and Connectors

By default, all released Collectors and Connectors are installed when you install Sentinel 7. If a new Collector or Connector is released after Sentinel 7, you must install the Collector or Connector files before you can configure the Collector or Connector.

- Section 9.1.1, "Installing a Collector," on page 61
- Section 9.1.2, "Installing a Connector," on page 61

9.1.1 Installing a Collector

1. Download the correct Collector from the Sentinel Plug-ins Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
2. Log in to the Sentinel Web interface at https://<*IP address*>:8443, where 8443 is the default port for the Sentinel server.
3. Click *applications* in the toolbar, then click *Applications*.
4. Click *Launch Control Center* to launch the Sentinel Control Center.
5. In the toolbar, click *Event Source Management* > *Live View*, then click *Tools* > *Import plugin*.
6. Browse to and select the Collector file you downloaded in Step 1, then click *Next*.
7. Follow the remaining prompts, then click *Finish*.

To configure the Collector, see the documentation for the specific Collector on the Sentinel Plug-ins Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.1.2 Installing a Connector

1. Download the correct Connector from the Sentinel Plug-ins Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
2. Log in to the Sentinel Web interface at https://<*IP address*>:8443, where 8443 is the default port for the Sentinel server.
3. Click *application* in the toolbar, then click *Applications*.
4. Click *Launch Control Center* to launch the Sentinel Control Center.

5. In the toolbar, select *Event Source Management* > *Live View*, then click *Tools* > *Import plugin*.
6. Browse to and select the Connector file you downloaded in Step 1, then click *Next*.
7. Follow the remaining prompts, then click *Finish*.

To configure the Connector, see the documentation for the specific Connector on the Sentinel Plug-ins Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2 Adding Additional Collectors and Connectors

9.2.1 Adding Additional Collectors

You can add additional Collectors to normalize data from other sources.

1. Log in to the Sentinel Web interface at https://<*IP address*>:8443, where 8443 is the default port for the Sentinel server.
2. Click *application* in the toolbar, then click *Applications*.
3. Click *Launch Connector Center* to launch the Sentinel Control Center.
4. In the toolbar, select *Event Source Management* > *Live View*.
5. Right-click the Collector Manager, then click *Add Collector*.
6. Select your Collector from the *Vendor* column, then click *Next*.
7. The fields are different for each Collector, so you need to follow the specific Collector documentation to configure the Collector at this point.

   The Collector documentation is located on the Sentinel Plug-in Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

9.2.2 Adding Additional Connectors

You can add additional Connectors to gather information from other sources.

1. Log in to the Sentinel Web interface at https://<*IP address*>:8443, where 8443 is the default port for the Sentinel server.
2. Click *application* in the toolbar, then click *Applications*.
3. Click *Launch Control Center* to launch the Sentinel Control Center.
4. In the toolbar, select *Event Source Management* > *Live View*.
5. Right-click the Collector you want to add the additional Connector to, then click *Add Connector*.
6. Select the desired Connector from the *Name* column, then click *Next*.
7. The fields are different for each Connector, so you need to follow the specific Connector documentation to configure the Connector at this point.

   The Connector documentation is located on the Sentinel Plug-in Web page (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

10 Managing Data

10.1 Directory Structure

By default, the Sentinel directories are in the following locations:

- The data files are in `/var/opt/novell/sentinel/data` and `/var/opt/novell/sentinel/3rdparty` directories.
- Executables and libraries are stored in the following directories:
    - `/opt/novell/sentinel/bin`
    - `/opt/novell/sentinel/setup`
    - `/opt/novell/sentinel/3rdparty`
- Log files are in the directory `/var/opt/novell/sentinel/log`
- Configuration files are in the following directory `/etc/opt/novell/sentinel`
- The process ID (PID) file is in the directory `/var/run/sentinel/server.pid`.

  Using the PID, administrators can identify the parent process of Sentinel server and monitor or terminate the process.

10.2 Storage Consideration

While storing the Sentinel data files, ensure that the data files are stored on a separate partition than the executables, configuration, and operating system files. The benefits of storing the data separately allows easier imaging of one set of files and recovery in case of corruption. It also improves the overall performance of systems where smaller file systems are more efficient. For more information, see “Disk partitioning” (http://en.wikipedia.org/wiki/Disk_partitioning#Benefits_of_multiple_partitions).

You can decide to install Sentinel on multiple partitions or on a single partition depending on the following installation types:

- Stand-alone installation
- Appliance installation.

10.2.1 Using Partition in a Stand-alone Installation

If you are installing Sentinel as a stand-alone install, then you can modify the partition layout of the operating system prior to installing Sentinel. The administrator should create and mount the desired partitions to the appropriate directories, based on the directory structure detailed in Section 10.1, "Directory Structure," on page 63. When you run the installer, Sentinel is installed into the pre-created directories resulting in an install that spans multiple partitions.

NOTE:

- You can use the `--location` option while running the installer to specify a different location than the default directories to store the file. The value that you pass to the `--location` option is prepended to the directory paths. For example, if you specify `--location=/foo`, the data directory will be `/foo/var/opt/novell/sentinel/data` and the config directory will be `/foo/etc/opt/novell/sentinel/config`.
- You must not use file-system links (for example, soft links) for the `--location` option.

10.2.2 Using Partition in an Appliance Installation

If you are installing Sentinel by using appliance install, it is not possible to reconfigure the operating system prior to Sentinel installation because the operating system is installed along with Sentinel. However, you can add partition in the appliance and move a directory to the new partition by using the YaST tool.

The following procedure creates a new partition and moves the data files from its directory to the newly created partition:

1. Log in to Sentinel as `root`.
2. Run the following command to stop the Sentinel on the appliance:

   ```
   /etc/init.d/sentinel stop
   ```

3. Specify the following command to change to `novell` user:

   ```
   su -novell
   ```

4. Move the contents of the directory at `/var/opt/novell/sentinel` to a temporary location.
5. Change to `root` user.
6. Enter the following command to access the YaST2 Control Center:

   ```
   yast
   ```

7. Select *System* > *Partitioner*.
8. Read the warning and select *Yes* to add the new unused partition.
9. Mount the new partition at `/var/opt/novell/sentinel`.
10. Specify the following command to change to `novell` user:

    ```
    su -novell
    ```

11. Move the contents of the data directory from the temporary location (where it was saved in Step 4) back to `/var/opt/novell/sentinel` in the new partition.
12. Change to `root` user.
13. Run the following command to restart the Sentinel appliance:

    ```
    /etc/init.d/sentinel start
    ```

11 Configuring Out-of-the-box Content

Sentinel ships with a wide variety of useful out-of-the-box content that you can use immediately to meet many of your analysis needs. Much of this content comes from a pre-installed Sentinel Core Solution Pack. For more information, see “Using Solution Packs” in the *NetIQ Sentinel 7.0.1 Administration Guide*.

Solution Pack allows categorization and grouping of content into controls or policy sets that are treated as a unit. The controls in the Sentinel Core Solution Pack are pre-installed to provide you with this out-of-the-box content, but those controls have to be formally implemented or tested by using the Sentinel Web UI.

If a certain amount of rigor is desired to help show that your Sentinel implementation is working as designed, you may use the formal attestation process built into the Solution Packs. This attestation process implements and tests the Sentinel Core controls just as you would implement and test controls from any other Solution Pack. As part of this process, the implementer and tester will attest that they have completed their work; these attestations will then become part of an audit trail that can be examined to demonstrate that any particular control was properly deployed.

You can do the attestation process by using the Solution Manager. For more information on implementing and testing the controls, see “Installing and Managing Solution Packs” in the *NetIQ Sentinel 7.0.1 Administration Guide*.

12 Configuring Time

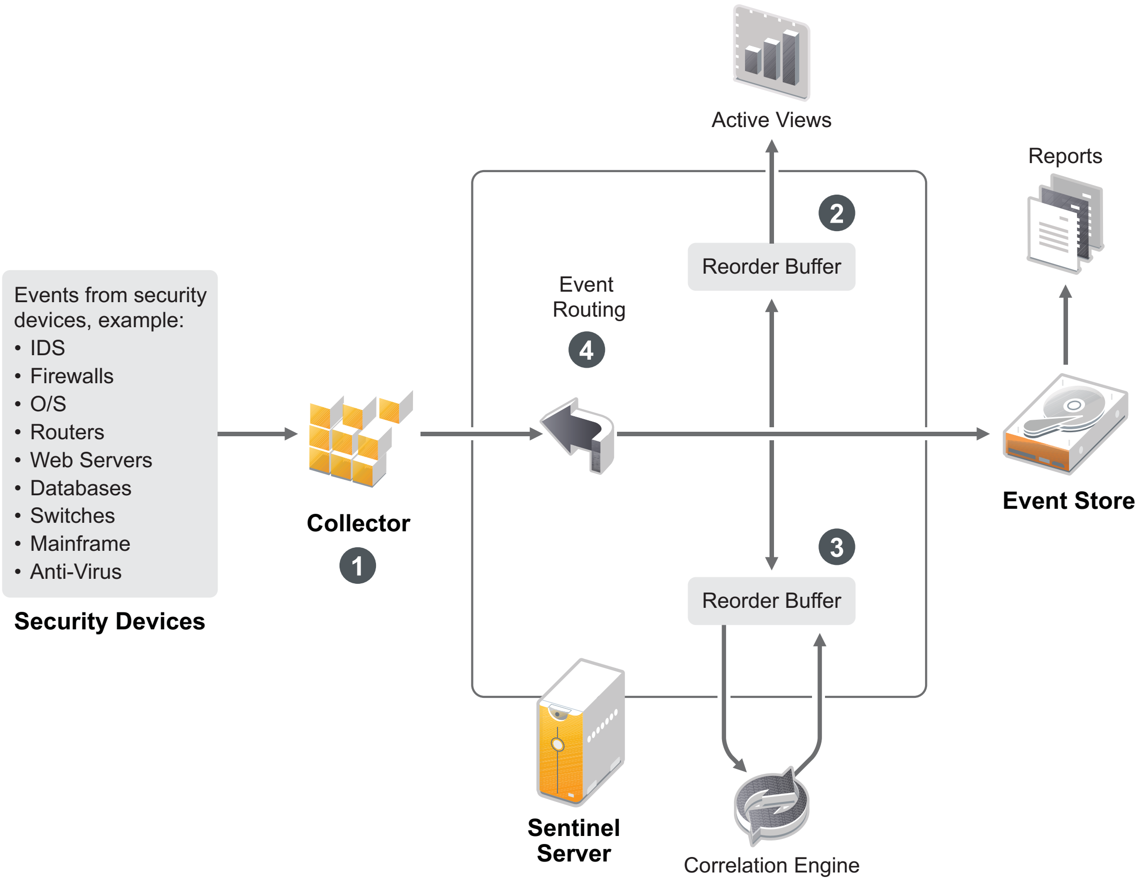
The time of an event is very critical to its processing in Sentinel. It is important for reporting and auditing purposes as well as for real-time processing.

12.1 Understanding Time in Sentinel

Sentinel is a distributed system that is made up of several processes that can be in different parts of the network. In addition, there can be some delay introduced by the device. In order to accommodate this, the Sentinel processes reorder the events into a time-ordered stream before processing.

The following illustration explains how Sentinel does this:

Figure 12-1 Sentinel Time



1. By default, the event time is set to the Collector Manager time. The ideal time is the device time. Therefore, it is best to set the event time to the device time if the device time is available, accurate, and properly parsed by the Collector.
2. Events are sorted into 30-second intervals so that they can be viewed in Active Views. By default, the events that have a time stamp within a 5-minute range from the server time (in the past or future) are processed normally. Events that have time stamps more than 5 minutes in the future do not show in the Active Views, but are inserted into the event store. Events that have time stamps more than 5 minutes and less than 24 hours in the past are still shown in the charts, but are not shown in the event data for that chart. A drill-down operation is necessary to retrieve those events from the event store.
3. If the event time is more than 30 seconds older than the server time, the Correlation Engine does not process the events.
4. If the event time is older than 5 minutes than the Collector Manager time (correct time), events are directly routed to the event store.

12.2 Configuring Time in Sentinel

The Correlation Engine processes time-ordered streams of events and detects patterns within events as well as temporal patterns in the stream. However, sometimes the device generating the event might not include the time in its log messages. To configure time to work correctly with Sentinel, you have two options:

- Configure NTP on the Collector Manager and deselect *Trust Event Source Time* on the event source in the Event Source Manager. Sentinel uses the Collector Manager as the time source for the events.
- Select *Trust Event Source Time* on the event source in Event Source Manager. Sentinel uses the time from the log message as the correct time.

To change this setting on the event source:

1. Log in to Event Source Management.

   For more information, see "Accessing Event Source Management" in the *NetIQ Sentinel 7.0.1 Administration Guide*.
2. Right-click the event source you want to change the time setting for, then select *Edit*.
3. Select or deselect the *Trust Event Source* option on the bottom of the *General* tab.
4. Click *OK* to save the change.

12.3 Handling Time Zones

Handling time zones can become very complex in a distributed environment. For example, you might have an event source in one time zone, the Collector Manager in another, the back-end Sentinel server in another, and the client viewing the data in yet another. When you add concerns such as daylight saving time and the many event sources that don't report what time zone they are set to (such as all syslog sources), there are many possible problems that need to be handled. Sentinel is flexible so that you can properly represent the time when events actually occur, and compare those events to other events from other sources in the same or different time zones.

In general, there are three different scenarios for how event sources report time stamps:

- The event source reports the time in UTC. For example, all standard Windows Event Log events are always reported in UTC.
- The event source reports in local time, but always includes the time zone in the time stamp. For example, any event source that follows RFC3339 in structuring time stamps include the time zone as an offset; other sources report long time zone IDs such as Americas/New York, or short time zone IDs such as EST, which can present problems because of conflicts and inadequate resolutions.
- The event source reports local time, but does not indicate the time zone. Unfortunately, the extremely common syslog format follows this model.

For the first scenario, you can always calculate the absolute UTC time that an event occurred (assuming that a time sync protocol is in use), so you can easily compare the timing of that event to any other event source in the world. However, you cannot automatically determine what the local time was when the event occurred. For this reason, Sentinel allows customers to manually set the time zone of an event source by editing the Event Source node in the Event Source Manager and specifying the appropriate time zone. This information does not affect the calculation of DeviceEventTime or EventTime, but is placed into the ObserverTZ field, and is used to calculate the various ObserverTZ fields, such as ObserverTZHour. These fields are always expressed in local time.

The second scenario is in many ways the simplest. If the long-form time zone IDs or offsets are used, you can easily convert to UTC to get the absolute canonical UTC time (stored in DeviceEventTime), but you can also easily calculate the local time ObserverTZ fields. If a short-form time zone ID is used, there is some potential for conflicts.

The third scenario can be the trickiest, because it requires the administrator to manually set the event source time zone for all affected sources so that Sentinel can properly calculate the UTC time. If the time zone is not properly specified by editing the Event Source node in the Event Source Manager, then the DeviceEventTime (and probably the EventTime) can be incorrect; also, the ObserverTZ and associated fields might be incorrect.

In general, the Collector for a given type of event source (such as Microsoft Windows) knows how an event source presents time stamps, and adjusts accordingly. It is always good policy to manually set the time zone for all Event Source nodes in the Event Source Manager, unless you know that the event source reports in local time and always includes the time zone in the time stamp

Processing the event source presentation of the time stamp happens in the Collector and on the Collector Manager. The DeviceEventTime and the EventTime are stored as UTC, and the ObserverTZ fields are stored as strings set to local time for the event source. This information is sent from the Collector Manager to the Sentinel server and stored in the event store. The time zone that the Collector Manager and the Sentinel server are in should not affect this process or the stored data. However, when a client views the event in a Web browser, the UTC EventTime is converted to the local time according to the Web browser, so all events are presented to clients in the local time zone. If the users want to see the local time of the source, they can examine the ObserverTZ fields for details.

13 License Information

This section describes the various Sentinel licenses and provides information on how you can manage the licenses.

- Section 13.1, "Understanding Sentinel Licenses," on page 71
- Section 13.2, "Adding a License Key," on page 72

13.1 Understanding Sentinel Licenses

Sentinel has several licenses that you can use. By default, Sentinel comes with the trial license.

- Section 13.1.1, "Trial License," on page 71
- Section 13.1.2, "Enterprise Licenses," on page 71

13.1.1 Trial License

The Sentinel default licensing allows you to use all the enterprise features of Sentinel for the evaluation period of 90 days. A system running with the trial license displays an indicator on the Web Interface indicating that the temporary license key is being used. It also displays the number of days left before the functionality expires and indicates how to upgrade to a full license.

NOTE: The expiration date of the system is based on the oldest data in the system. If you restore old events into your system, the expiration date will be adjusted accordingly.

After the 90-day trial period, most functionality is disabled, but you are still able to log in and update the system to use an enterprise license key.

After you upgrade to an enterprise license, all functionality is restored. To prevent any interruption in functionality, you must upgrade the system with an enterprise license before the expiration date.

13.1.2 Enterprise Licenses

When you purchase Sentinel, you receive a license key through the customer portal. Depending on what you purchase, your license key enables certain features, data collection rates, and event sources. There may be additional license terms that are not enforced by the license key, so please read your license agreement carefully.

To make changes to your licensing, please contact your account manager. To add the license key to the system, see Section 13.2.1, "Adding a License Key By Using the Web Interface," on page 72.

13.2 Adding a License Key

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

You can add a license key either by using the Web interface or through the command line.

- Section 13.2.1, "Adding a License Key By Using the Web Interface," on page 72
- Section 13.2.2, "Adding a License Key through the Command Line," on page 72

13.2.1 Adding a License Key By Using the Web Interface

1. Log in to the Sentinel Web interface as an administrator.
2. Click the *About* link in the upper left corner of the page.
3. Click the *License*s tab.
4. In the Licenses section, click *Add License*.
5. Specify the license key in the *Key* field. After you specify the license, the following information is displayed in the Preview section:

   Features: The features that are available with the license.

   Hostname: This field is for internal NetIQ use only.

   Serial: This field is for internal NetIQ use only.

   EPS: Event rate built into the license key. Beyond this rate, Sentinel will generate warnings but will continue to collect data.

   Expires: Expiry date of the license. You must specify a valid license key before the expiry date to prevent an interruption in functionality.
6. Click *Save*.

13.2.2 Adding a License Key through the Command Line

You can add the license through the command line by using the `softwarekey.sh` script.

1. Log in to the Sentinel server as `root`.
2. Change to the `/opt/novell/sentinel/bin` directory.
3. Enter the following command to change to the novell user:

   ```
   su novell
   ```
4. Specify the following command to run the `softwarekey.sh` script.

   ```
   ./softwarekey.sh
   ```
5. Enter 1 to insert the license key.
6. Specify the license key, then press Enter.

14 Configuring Sentinel for High Availability

Sentinel has been tested and certified to work in a high availability environment, and it supports disaster recovery architectures. NetIQ Consulting and NetIQ partners can help you implement Sentinel high availability and disaster recovery.

To enable the Sentinel servers for high availability, you need the following:

- Redundant, clustered Sentinel nodes.
- Access to shared data storage.
- Virtual IP addresses that can be used to transparently shift from a failed node to another node.
- Scripts to start, stop, and monitor the application based on policies defined in your cluster solutions. You can use cluster solutions such as Cluster Resource Agents or LSB init scripts on Linux Enterprise High Availability systems.

There are many packages in the market that enable high availability. Testing for Sentinel was performed with the *SUSE Linux Enterprise High Availability (HA) Extension* (http://www.novell.com/products/highavailability/), shared storage RAID drives, and custom scripts. This architecture can be replicated across data centers to ensure availability of everything from the Sentinel server to the Collector Managers and Collectors.

High availability for event sources should be considered on a case-by-case basis because of the wide variety of devices that can be used.

III Upgrading Sentinel

15 Upgrading the Sentinel 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” in the *NetIQ Sentinel 7.0.1 Administration Guide*.

2. Download the latest installer from the Novell download site (http://download.novell.com).
3. Log in as `root` to the server where you want to upgrade Sentinel.
4. 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.

5. Change to the directory where the install file was extracted.
6. Specify the following command to upgrade Sentinel:

   ```
   ./install-sentinel
   ```

7. 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.

8. Read the end user license, enter `yes` or `y` to accept the license, then continue with the installation.
9. 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.

10. (Conditional) To upgrade Collector Manager systems, see Chapter 17, “Upgrading the Collector Manager,” on page 81.
11. (Conditional) To upgrade the Correlation Engine system, see Chapter 18, “Upgrading the Correlation Engine,” on page 83.

16 Upgrading the Sentinel Appliance

This procedure guides you through upgrading the Sentinel Appliance as well as Collector Manager and Correlation Engine Appliances.

1. Log in to the Sentinel appliance as a user in the administrator role.
2. ***If you want to upgrade the Sentinel Appliance***, click *Appliance* to launch WebYaST.
3. ***If you want to upgrade a Collector Manager or Correlation Engine Appliance***, specify the URL of the Collector Manager or Correlation Engine computer using port 54984 to launch WebYaST.
4. Make a backup of your configuration, then create an ESM export.

   For more information on backing up data, see "Backing Up and Restoring Data" in the *NetIQ Sentinel 7.0.1 Administration Guide*.
5. (Conditional) If you have not already registered the appliance for automatic updates, register for updates.

   For more information, see Section 5.9, "Registering for Updates," on page 51.

   If the appliance is not registered, an yellow warning is displayed, indicating that the appliance is not registered.
6. To check if there are any updates, click *Updates*.

   The available updates are displayed.
7. 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 service. You must manually restart this service after the upgrade is complete.
8. Restart the Sentinel service by using the Web interface.

   For more information, see Section 5.8, "Stopping and Starting the Server by Using the Web Interface," on page 51.

17 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 *NetIQ Sentinel 7.0.1 Administration Guide*.
2. Log in to the Sentinel web interface as a user in the administrator role.
3. Select *Downloads*.
4. Click *Download Installer* in the Collector Manager Installer section.

   A window is displayed with options to either open or to save the installer file on the local machine.
5. Save the file.
6. Copy the file to a temporary location.
7. Extract the contents of the file.
8. Run the following script:

   ```
   ./install-cm
   ```
9. Follow the on-screen instructions to complete the installation.

18 Upgrading the Correlation Engine

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

   For more information, see “Backing Up and Restoring Data” in the *NetIQ Sentinel 7.0.1 Administration Guide*.

2. Log in to the Sentinel web interface as a user in the administrator role.
3. Select *Downloads*.
4. Click *Download Installer* in the Correlation Engine Installer section.

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

5. Save the file.
6. Copy the file to a temporary location.
7. Extract the contents of the file.
8. Run the following script:

   ./install-ce

9. Follow the on-screen instructions to complete the installation.

19 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). 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.

IV Migrating

20 Supported Migration Scenarios

You can migrate Sentinel configuration data, such as user account, plug-in, collector manager, action, and correlation rule configuration data using the Sentinel 6 to 7 Migration Utility. You can download this utility from the Novell Patch Finder Web site. For more information, see the *Migration Utility Technical Reference* in the Sentinel 7.0 Documentation Web site.

IMPORTANT: For this release of Sentinel, migrating event data is not possible. You could leave Sentinel 6 in production until you no longer need the event data stored in the older systems.

21 What's Next

After Sentinel is installed, there are two guides to help you configure Sentinel: the *NetIQ Sentinel 7.0.1 Administration Guide* and the *NetIQ Sentinel 7.0.1 User Guide*.

The Administration Guide contains configuration information for tasks only a user with administration rights can perform. For example:

- "Configuring Users and Roles"
- "Configuring Data Storage"
- "Configuring Data Collection"
- "Searching and Reporting Events in a Distributed Environment"

For more information on these and other administration tasks, see the *NetIQ Sentinel 7.0.1 Administration Guide*.

The User Guide contains instructions to help users perform tasks in Sentinel. For example:

- "Searching Events"
- "Analyzing Trends in Data"
- "Reporting"
- "Configuring Incidents"

For more information on these and other user tasks, see the *NetIQ Sentinel 7.0.1 User Guide*.

You can also configure Sentinel to analyze your events, add data using correlation rules, set up baselines, configure workflows to act on the information, and more. Use the information in the *NetIQ Sentinel 7.0.1 Administration Guide* to help you configure these Sentinel features.

V Uninstalling

You uninstall Sentinel by performing the following tasks:

- Chapter 22, “Uninstalling Sentinel,” on page 95
- Chapter 23, “Post-Uninstallation Tasks,” on page 97

22 Uninstalling Sentinel

An uninstall script is available to help you remove a Sentinel installation. Several files, including log files, are preserved and can be manually removed if desired. Before performing a new installation, you should perform all of the following steps to ensure there are no files or system settings remaining from a previous installation.

WARNING: These instructions involve modifying operating system settings and files. If you are not familiar with modifying these system settings and files, please contact your system administrator.

- Section 22.1, “Uninstalling the Sentinel Server,” on page 95
- Section 22.2, “Uninstalling the Remote Collector Manager or Correlation Engine,” on page 95

22.1 Uninstalling the Sentinel Server

1 Log in to the Sentinel server as `root`.

NOTE: You can not uninstall Sentinel server as non-root user, if the installation is performed as a `root` user. However, non-root user can uninstall Sentinel server if the installation is done by non-root user.

2 Access the following directory:

```
/opt/novell/sentinel/setup/
```

3 Run the following command:

```
./uninstall-sentinel
```

4 When prompted to reconfirm that you want to proceed with the uninstall, press y.

The script first stops the service and then removes it completely.

22.2 Uninstalling the Remote Collector Manager or Correlation Engine

1 Log in as `root`.

NOTE: You can not uninstall Remote Collector Manager or Remote correlation engine as non-root user, if installation is performed as a `root` user. However, non-root user can uninstall, if the installation is done by a non-root user.

2 Go to the following location:

```
/opt/novell/sentinel/setup
```

3 Run the following command:

```
./uninstall-sentinel
```

The script displays a warning that Collector Manager or Correlation Engine and all associated data will be completely removed.

4 Enter y to remove the Collector Manager or Correlation Engine.

The script first stops the service and then removes it completely.

23 Post-Uninstallation Tasks

NOTE: Uninstalling Sentinel Server does not remove the Sentinel Administrator User from the operating system. You must manually remove that user, if desired.

- Section 23.1, “Removing the Sentinel System Settings,” on page 97

23.1 Removing the Sentinel System Settings

After you uninstall Sentinel, certain systems settings remain.These settings should be removed before performing a “clean” installation of Sentinel, particularly if the Sentinel uninstallation encountered errors.

To manually clean up the Sentinel system settings:

1. Log in as `root`.
2. Ensure that all Sentinel processes are stopped.
3. Remove the contents of `/opt/novell/sentinel` or wherever the Sentinel software was installed.
4. Make sure no one is logged in as the Sentinel Administrator operating system user (novell by default), then remove the user, the home directory, and the group.

   ```
   userdel -r novell
   ```

   ```
   groupdel novell
   ```
5. Restart the operating system.

23.1.1 Completing the Uninstallation of the Correlation Engine

After you run the uninstall script for uninstalling the Correlation Engine, the Correlation Engine icon is still displayed in inactive state in the Web interface. You need to perform the following additional steps to manually delete the Correlation Engine in the Web interface:

1. Log in to the Sentinel Web interface as an administrator.
2. Expand *Correlation*, then select the Correlation Engine that you want to delete.
3. Click the *Delete* button (garbage can icon).

23.1.2 Completing the Uninstallation of the Collector Manager

After you run the uninstall script for uninstalling the Collector Manager, the Collector Manager icon is still displayed in inactive state in the Web interface. You need to perform the following additional steps to manually delete the Collector Manager in the Web interface:

1. Access *Event Source Management* > *Live View*.
2. Right-click the Collector Manager you want to delete, then click *Delete*.