AUTHORIZED DOCUMENTATION

Installation Guide

Novell® Sentinel™ Rapid Deployment

6.1

November 2009

www.novell.com

Legal Notices

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

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

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

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

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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

Sentinel™ is a security information and event management solution that receives information from many sources throughout an enterprise, standardizes it, prioritizes it, and presents it to you so you can make threat, risk, and policy related decisions.

Sentinel Rapid Deployment is a simplified version of Novell® Sentinel that leverages open source PostgreSQL*, activeMQ*, and JasperReports* components. The following sections help you understand and install the major components of the Sentinel Rapid Deployment system.

Audience

This documentation is intended for Information Security Professionals.

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 and enter your comments there.

Additional Documentation

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

- *Novell Sentinel 6.1 RD Installation Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html)
- *Novell Sentinel 6.1 RD User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/index.html)
- *Novell Sentinel 6.1 RD Reference Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/index.html)
- *Sentinel 6.1 Install Guide* (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_installation_guide.pdf)
- *Sentinel 6.1 User Guide* (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_user_guide.pdf)

- *Sentinel 6.1 Reference Guide* (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_reference_guide.pdf)
- *Sentinel SDK* (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel)

  The Sentinel SDK site provides the details about developing collectors (proprietary or JavaScript) and JavaScript correlation actions.

Documentation Conventions

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

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

When a single path name can be written with a backslash for some platforms or a forward slash for other platforms, the path name is presented with forward slashes to reflect the Linux* convention. Users of platforms that require a backslash, such as NetWare®, should use backlashes as required by your software.

Contacting Novell

- *Novell Website* (http://www.novell.com)
- *Novell Technical Support* (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- *Novell Self Support* (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- *Patch Download Site* (http://download.novell.com/index.jsp)
- *Novell 24x7 Support* (http://www.novell.com/company/contact.html)
- *Sentinel TIDS* (http://support.novell.com/products/sentinel)

Introduction

1

Sentinel™ is a security information and event management solution that receives information from many sources throughout an enterprise, standardizes it, prioritizes it, and presents it to you so you can make threat, risk, and policy-related decisions.

The following sections describe the installation and configuration of Novell® Sentinel™ 6.1 Rapid Deployment. The Sentinel 6.1 Rapid Deployment User Guide (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) has more detailed architecture, operation, and administrative procedures.

1.1 Sentinel Rapid Deployment Overview

Sentinel automates log collection, analysis, and reporting processes to ensure that IT controls are effective in supporting threat detection and audit requirements. Sentinel replaces labor-intensive manual processes with automated, continuous monitoring of security and compliance events and IT controls.

Sentinel gathers and correlates security and non-security information from across the networked infrastructure of an organization, as well as the third-party systems, devices, and applications. Sentinel presents the collected data in a GUI, identifies security or compliance issues, and tracks remedial activities to streamline the error-prone processes and build a more rigorous and secure management program.

Automated incident response management enables you to document and formalize the process of tracking, escalating, and responding to incidents and policy violations, and provides two-way integration with trouble-ticketing systems. Sentinel enables you to react promptly and resolve incidents efficiently.

Solution Packs are a simple way to distribute and import Sentinel correlation rules, dynamic lists, maps, reports, and iTRAC™ workflows into controls. These controls can be designed to meet specific regulatory requirements, such as the Payment Card Industry Data Security Standard, or they can be related to a specific data source, such as user authentication events for a database.

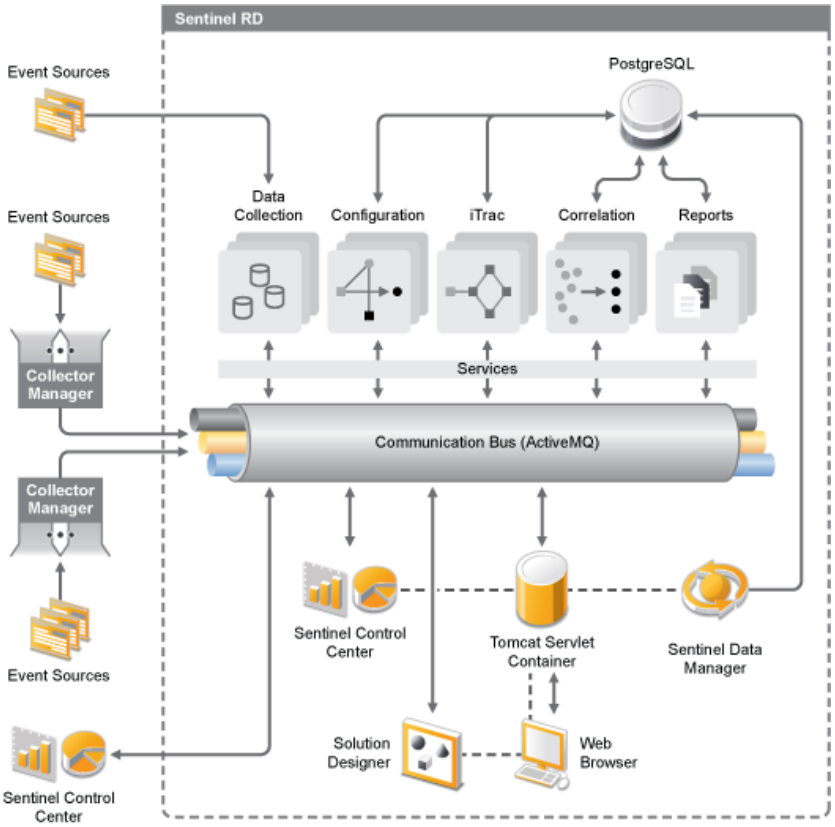
With Sentinel Rapid Deployment, you get:

- Integrated, automated real-time security management and compliance monitoring across all systems and networks
- A framework that enables business policies to drive IT policy and action
- Automatic documenting and reporting of security, systems, and access events across the enterprise

- Built-in incident management and remediation
- The ability to demonstrate and monitor compliance with internal policies and government regulations such as Sarbanes-Oxley, HIPAA, GLBA, FISMA, and others. The content required to implement these controls is distributed and implemented through Solution Packs

The following is an illustration of the conceptual architecture of Sentinel 6.1 Rapid Deployment, which shows the components involved in performing security and compliance management.

Figure 1-1 *Conceptual Architecture of Sentinel*



1.2 Sentinel Rapid Deployment User Interfaces

Sentinel includes the following easy-to-use user interfaces:

- Sentinel Rapid Deployment Web Interface
- Sentinel Control Center
- Sentinel Data Manager
- Sentinel Solution Designer
- Sentinel Plug-in SDK
- Sentinel Collector Builder

1.2.1 Sentinel Rapid Deployment Web Interface

With the Novell Sentinel Rapid Deployment Web interface, you can manage and search Reports and launch the Sentinel Control Center, the Sentinel Data Manager, and the Solution Designer. You can also download the Collector Manager installer and the Client installer from the *Application* tab of the Sentinel 6.1 Rapid Deployment Web interface.

For more information, see Managing Sentinel 6.1 Rapid Deployment Through the Web Interface in the Sentinel 6.1 Rapid Deployment User Guide (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html).

1.2.2 Sentinel Control Center

The Sentinel Control Center (SCC) provides an integrated security management dashboard that enables analysts to quickly identify new trends or attacks, manipulate and interact with real-time graphical information, and respond to incidents.

You can launch the SCC either as a client application or by using Java* Webstart.

Key features of the Sentinel Control Center include:

- **Active Views:** Real-time analytics and visualization
- **Analysis:** Runs and saves offline queries
- **Incidents:** Incident creation and management
- **Correlation:** Correlation rules definition and management
- **iTRAC:** Process management for documenting, enforcing, and tracking incident resolution processes
- **Event Source Management:** Collector deployment and monitoring
- **Solution Manager:** Install, implement, and test the Solution pack contents

For more information, see "Sentinel Control Center" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.2.3 Sentinel Data Manager

The Sentinel Data Manager allows you to manage the Sentinel database. You can perform the following operations in the Sentinel Data Manager:

- Monitor database space utilization
- View and manage database partitions
- Manage database archives
- Import archived data back into the database

For more information, see "Sentinel Data Manager"in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.2.4 Sentinel Solution Designer

The Sentinel Solution Designer is used to create and modify Solution Packs, which are packaged sets of Sentinel content, such as correlation rules, actions, iTRAC worflows, and reports.

Sentinel content is the extended functionality of the Sentinel system. It includes Sentinel plug-ins, Sentinel Actions, Integrators, and Sentinel plug-ins such as Collectors, Connectors, and Solution Packs that might include multiple other types of plug-ins.These modular components are used to integrate with third-party systems, install a complete control-based security solution, and provide automated remediation for detected incidents.

For more information, see Solution Designer in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.2.5 Sentinel Plug-in SDK

The Sentinel Plug-in SDK includes libraries and code developed by the Novell Engineering, as well as the template and sample code which you can use to begin developing your own projects. For more information, see Sentinel SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel#Sentinel_Plug-in_SDK).

1.2.6 Sentinel Collector Builder

The Sentinel Collector Builder enables you to build Collectors in the Sentinel proprietary, legacy language to process events. You can create and customize the templates so that the Collector can parse the data. For more information on developing your own Collectors, see Developing Sentinel Collector Plug-ins (http://developer.novell.com/wiki/index.php/Collectors).

1.3 Sentinel Server Components

Sentinel is made up of the following components:

1.3.1 Data Access Service

The Sentinel Data Access Service is the primary component used to communicate with the Sentinel database. The Data Access Server and other server components work together to store events received from the Collector Managers into the database, filter data, process Active Views™ displays, perform database queries and process results, and manage administrative tasks such as user authentication and authorization. For more information, see Sentinel 6.1 Rapid Deployment Data Access Service in the Sentinel 6.1 Rapid Deployment Reference Guide.

1.3.2 Message Bus

Sentinel 6.1 Rapid Deployment uses the open source message broker named Apache*Active MQ. The message bus is capable of moving thousands of message packets in a second between the components of Sentinel. Its architecture is built around the Java Message Oriented Middleware (JMOM) that supports asynchronous calls between the client and server applications. Message queues provide temporary storage when the destination program is busy or not connected. For more information, see "Communication Server" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.3.3 Sentinel Database

The Sentinel product is built around a back-end database that stores security events and all of the Sentinel metadata. Sentinel 6.1 Rapid Deployment supports PostgreSQL. The events are stored in normalized form, along with asset and vulnerability data, identity information, incident and workflow status, and many other types of data. For more information, see "Sentinel Data Manager" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.3.4 Sentinel Collector Manager

The Sentinel Collector Manager manages data collection, monitors system status messages, and performs event filtering as needed. The main functions of the Collector Manager include transforming events, adding business relevance to events through taxonomy, performing global filtering on events, routing events, and sending health messages to the Sentinel server. The Sentinel Collector Manager directly connects to the message bus. For more information, see "Collectors" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.3.5 Correlation Engine

Correlation adds intelligence to security event management by automating analysis of the incoming event stream to find patterns of interest. Correlation allows you to define rules that identify critical threats and complex attack patterns so that you can prioritize events and initiate effective incident management and response. For more information, see "Correlation Tab" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.3.6 iTRAC

Sentinel provides an iTRAC™ workflow management system to define and automate processes for incident response. Incidents that are identified in Sentinel, either by a correlation rule or manually, can be associated with an iTRAC workflow. For more information, see "iTRAC Workflows" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.3.7 Sentinel Advisor and Exploit Detection

Sentinel Advisor is an optional data subscription service that includes known attacks, vulnerabilities, and remediation information. This data, combined with known vulnerabilities and real-time intrusion detection or prevention information from your environment, provide proactive exploit detection and the ability to immediately act when an attack takes place against a vulnerable system.

An Advisor data snapshot is installed by default with Sentinel 6.1 Rapid Deployment installation. You need an Advisor license to subscribe to the ongoing Advisor data updates. For more information, see "Advisor Usage and Maintenance" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.3.8 Web Server

Sentinel 6.1 Rapid Deployment uses Apache* Tomcat as its Web server to allow secure connection to the Sentinel Rapid Deployment Web interface.

1.4 Sentinel Plug-Ins

Sentinel supports a variety of plug-ins to expand and enhance system functionality. Some of these plugins are pre-installed. Additional plugins (and updates) are available for download at Sentinel Content Page (http://support.novell.com/products/sentinel/sentinel61rd.html).

Some plugins, such as the Remedy* Integrator, the IBM* Mainframe Connector, and the Connector for SAP* XAL, require an additional license for download.

1.4.1 Collectors

Sentinel collects data from source devices and delivers a richer event stream by injecting taxonomy, exploit detection, and business relevance into the data stream before events are correlated and analyzed and sent to the database. A richer event stream means that data is correlated with the required business context to identify and remediate internal or external threats and policy violations.

Sentinel Collectors can parse data from the types of devices listed below and more:

- Intrusion Detection Systems (host)
- Intrusion Detection Systems (network)
- Firewalls
- Operating Systems
- Policy Monitoring
- Authentication
- Routers and Switches
- VPNs
- Anti-Virus Detection Systems
- Web Servers
- Databases
- Mainframe
- Vulnerability Assessment Systems
- Directory Services
- Network Management Systems
- Proprietary Systems

JavaScript Collectors can be written by using the standard JavaScript development tools and the Collector SDK. Proprietary (or Legacy) Collectors can be built or modified by using the Sentinel Collector Builder, which is, a standalone application included with the Sentinel system. For more information, see Section 1.2.6, "Sentinel Collector Builder," on page 14.

1.4.2 Connectors and Integrators

Connectors provide connectivity from the Collector Manager to event sources through standard protocols such as JDBC* and syslog. Events are passed from the Connector to the Collector for parsing.

Integrators enable remediation actions on systems outside of Sentinel. For example, a correlation action can use the SOAP Integrator to initiate a Novell Identity Manager™ workflow.

The optional Remedy AR Integrator provides the ability to create a Remedy ticket from Sentinel events or incidents. For more information, see "Action Manager and Integrator" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.4.3 Correlation Rules and Actions

Correlation rules identify important patterns in the event stream. When a correlation rule triggers, it initiates correlation actions, such as sending e-mail notifications, initiating an iTRAC workflow, or executing an action using an Integrator. For more information, see "Correlation Tab" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.4.4 Reports

You can run a wide variety of dashboard and operational reports from the Sentinel 6.1 Rapid Deployment Web interface by using JasperReports. The reports are typically distributed via Solution Packs.

1.4.5 iTRAC Workflows

iTRAC workflows provide consistent, repeatable processes for managing incidents. The workflow templates are typically distributed via Solution Packs. iTRAC is shipped with a set of default templates that you can modify to suit your requirement. For more information, see "iTRAC Workflows" in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.4.6 Solution Packs

Solution Packs are packaged sets of related Sentinel content, such as correlation rules, actions, iTRAC workflows, and reports. Novell also creates Collector packs, which include content focused on a specific event source, such as Windows* Active Directory*. For more information, see "Solution Packs " in the *Sentinel 6.1 Rapid Deployment User Guide*.

1.5 Language Support

Sentinel components are available in the following languages:

- Czech
- English
- French
- German
- Italian

- Japanese
- Dutch
- Polish
- Portuguese
- Simplified Chinese
- Spanish
- Traditional Chinese

What's New in Sentinel 6.1 Rapid Deployment

2

Novell® Sentinel™ 6.1 Rapid Deployment is a simplified alternate platform for the Sentinel 6.1 application that you can install on a single machine. Sentinel 6.1 Rapid Deployment features an easy-to-install SIEM solution that leverages open source components, including a PostgreSQL database and JasperReports. It has many new capabilities, such as reporting and searching functionalities through the Web interface.

2.1 New and Updated Features

Sentinel 6.1 Rapid Deployment gives you the ability to:

- Use Sentinel with an embedded PostgreSQL database.
- Use a simplified single-machine server installer.
- Use the Web interface for the following:
  - Accessing the reporting and free-form search functionalities.
  - Running the Sentinel Control Center (SCC), the Solution Designer, and the Sentinel Data Manager (SDM) clients by using Java Web Start.
  - Downloading the multiplatform client installer and the Collector Manager.
- Use a single multiplatform client installer to install the Sentinel Control Center, the Solution Designer, and the Sentinel Data Manager.
- Use the Collector Manager installer to install additional Collector Managers for a distributed environment.
- Use JasperReports in Solution Packs.

2.2 Comparing Sentinel 6.1 and Sentinel 6.1 Rapid Deployment Features and Capabilities

This section compares the features and capabilities of Novell Sentinel 6.1 Rapid Deployment to Novell Sentinel 6.1.

Table 2-1 *Feature Comparison*

Features or Capabilities	Sentinel 6.1 Rapid Deployment	Sentinel 6.1
Supported Platforms for Server Installation	SUSE® Linux Enterprise Server	Linux, Solaris*, and Windows.

Features or Capabilities	Sentinel 6.1 Rapid Deployment	Sentinel 6.1
Database	The major difference between Sentinel 6.1 Rapid Deployment and previous versions of Sentinel is the introduction of an embedded Sentinel database, based on the open source PostgreSQL database engine. This new database is installed and configured automatically during the Sentinel Rapid Deployment installation, with no need to provide or manage an external database.	Customer-provided MS SQL or Oracle* database.
Reporting	Sentinel 6.1 Rapid Deployment introduces a new, streamlined reporting system to replace Crystal Reports. This new reporting system is an integral part of Sentinel and allows users to easily run pre-defined reports or custom reports developed using the open source Jasper reporting engine.	Crystal Reports with associated database is installed separately.
Messaging	ActiveMQ	SonicMQ*
Installation architecture	Installation is simplified. You only need to provide a Sentinel password, a database password, and an optional set of credentials for the Sentinel Advisor service. Server components, including the embedded database, the reporting engine, a Collector Manager, and a Web console are all included in the package, and are installed and configured automatically on a single machine. This allows you deploy and begin using the product very quickly and with a minimum amount of effort. Additional Collector Managers can be installed as needed.	The database is installed separately by the customer. Server components can be installed together or distributed across multiple machines.
Web-based application launch and installation	The Web console used for Sentinel 6.1 Rapid Deployment reporting and full text search also includes the option to launch and install the Sentinel client applications. You can now launch the Sentinel Control Center, the Sentinel Solution Designer, and the Sentinel Data Manager from a Web browser without the need to install these client applications locally. The Web console also includes the option to install the client applications and the Sentinel Collector Manager without the need to manually retrieve the installation package.	Not supported.

Features or Capabilities	Sentinel 6.1 Rapid Deployment	Sentinel 6.1
Reporting	Reports can be generated, scheduled, published, and viewed in a browser-based Web interface. New or updated reports can be uploaded by using the Web interface or the Solution Manager.	Reports can be viewed in the Sentinel Control Center. Reports can be scheduled in the Crystal server interface. New or updated reports can be uploaded by using the Crystal server interface or the Solution Manager.
Search	A new Web-based search tool allows you to quickly search for strings and patterns within the Sentinel event database. You can search for text in a specific Sentinel event field, or across all fields. Data within the search results is hyperlinked to narrow down the search results with a single click. You can also run the search by using the Sentinel Control Center.	Event searches can be run in the Sentinel Control Center.
Communication channel	The Collector Manager connects directly to the message bus.	Collector Manager can connect directly to the message bus or use an SSL proxy.

Sentinel 6.1 Rapid Deployment System Requirements

3

For best performance and reliability, you must install the Sentinel components on approved software and hardware, as listed below, that have been fully quality assured and certified. For the most up-to-date information on the minimum requirements, look for updates at the Novell Documentation site (http://www.novell.com/documentation/sentinel61).

3.1 Software Requirements

NOTE: Sentinel 6.1 Rapid Deployment is not supported on the Open Enterprise Server® installs of SLES® 10 SP2.

Table 3-1 *Software and Operating System Combinations*

Platforms	Sentinel Server Components	Sentinel Client Applications	Collector Manager	Collector Builder
SLES 10 SP2 (64-bit)	Certified	Certified	Certified	Not Supported
Windows XP* (32-bit)	Not Supported	Certified	Not Supported	Not Supported
Windows Vista* (32-bit)	Not Supported	Certified	Not Supported	Certified
Windows Server* 2003 (32-bit)	Not Supported	Not Supported	Certified	Certified
Windows Server* 2008 (64-bit)	Not Supported	Not Supported	Certified	Not Supported

Platforms	Sentinel Server Components	Sentinel Client Applications	Collector Manager	Collector Builder
SLES 10 SP2 (32-bit)	Limited Support **NOTE:** A demo-only package of Novell® Sentinel™ Rapid Deployment is designed for limited-scale demonstration and testing environments by using 32-bit hardware and operating systems. Customers or partners with a contract for Sentinel Rapid Deployment support can receive limited support on this platform from Novell Technical Support to the extent that the issues can be reproduced on the 64-bit production platform. Due to the inherent limitations of 32-bit hardware, Novell Technical Support does not troubleshoot performance or scalability issues with the 32-bit demo version. The 32-bit demo versions are unsupported in a production environment.	Limited Support	Certified	Limited Support

NOTE: For Sentinel 6.1 Rapid Deployment server, use SLES 10 SP2 (64-bit) OS with ext3 file system. 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*.

3.2 Supported Web Browsers

- Mozilla* Firefox* 2.0.0.10
- Mozilla Firefox 3.*x*
- Internet Explorer* 8.*x*

3.3 Hardware Requirements

The Sentinel server components run on x86-64 (64-bit) hardware. Sentinel is certified on AMD Opteron and Intel Xeon hardware. Itanium servers are not supported.

This section includes some general hardware recommendations for Sentinel system design. In general, design recommendations are based on event rate ranges. However, these recommendations are based on the following assumptions:

- The event rate is at the high end of the EPS range.
- The average event size is 600 bytes.

- All events are stored in the database (that is, there are no filters to drop events).
- Ninety days worth of data is stored online in the database.
- Storage space for Advisor data is not included in the specifications in Table 3-2 on page 25 and Table 3-3 on page 26.
- The Sentinel Server has a default 5 GB of disk space for temporarily caching event data that fails to be inserted into the database.
- The Sentinel Server also has a default 5 GB of disk space for events that fail to be written to aggregation event files.

NOTE: The Advisor subscription requires an additional 50 GB of disk space on the server.

The hardware recommendations for a Sentinel implementation can vary based on the individual implementation, so it is recommended that Novell Consulting Services or any of Novell Sentinel partners be consulted prior to finalizing the Sentinel architecture. The recommendations below can be used as a guideline.

NOTE: Because of high event loads and local caching, the Sentinel Server is required to have a local or shared striped disk array (RAID) with a minimum of 4 disk spindles.

Table 3-2 *Single Machine Configuration*

Components	RAM	Space	CPU
Machine 1: Sentinel 6.1 Rapid Deployment Server (Maximum EPS - 3200) ◆ Collector Manager (1200 MB) ◆ DAS_Core (1024 MB) ◆ DAS_Binary (512MB) ◆ Correlation Engine (512 MB) ◆ 9 General Event Collectors ◆ 4 eDirectory Event Sources (generating 250 eps each) ◆ 3 Syslog Event Sources (generating 350 eps each) ◆ 2 WMS Event Sources (generating 500 eps each) ◆ 10 Correlation Rules Deployed ◆ 10 unique Active Views ◆ 3 simultaneous users ◆ 2 Maps Deployed	16 GB	1 TB, SAS (15K rpm) Hard Disk(s) Hardware RAID 10	SLES10 SP2- Dell PowerEdge 2900,2 x Quad-Core Intel® Xeon® E5310 (1.6 GHz) with Gigabit Ethernet NIC

Table 3-3 *3 Machine Configuration*

Components	RAM	Space	CPU
Machine 1: Sentinel 6.1 Rapid Deployment Server (Maximum EPS - 3750) ◆ Collector Manager (1200 MB) ◆ DAS_Core (1024MB) ◆ DAS_Binary (512MB) ◆ Correlation Engine (512 MB) ◆ 4 General Event Collectors ◆ 4 eDirectory Event Sources (generating 250 eps each)	16 GB,	1 TB, SAS (15K rpm) Hard Disk(s) Hardware RAID 10	SLES10 SP2- Dell PowerEdge 2900,2 x Quad-Core Intel® Xeon® E5310 (1.6 GHz) with Gigabit Ethernet NIC
Machine 2: Collector Manager ◆ Collector Manager/Collectors	4 GB	300 GB,SATA (3 Gbit/s) Hard Disk	Windows or Linux - Intel® Core 2 Duo E6750 (2.66 GHz) with Gigabit Ethernet NIC
Machine 3: Collector Manager ◆ Collector Manager/Collectors	4 GB	300 GB,SATA (3 Gbit/s) Hard Disk	Windows or Linux - Intel® Core 2 Duo E6750 (2.66 GHz) with Gigabit Ethernet NIC

3.4 Virtualization

Sentinel 6.1 Rapid Deployment has been extensively tested on VMWare ESX Server and Novell fully supports Sentinel 6.1 Rapid Deployment in this environment. 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, CPU, diskspace, and I/O as the physical machine recommendations.

Installing Sentinel 6.1 Rapid Deployment

4

The Sentinel installation package provides you with a simplified single machine server installer to install everything you need to run Sentinel. This section helps you install the major components of the Sentinel™ 6.1 Rapid Deployment system.

4.1 Installer Overview

The Sentinel 6.1 Rapid Deployment installation package installs the following:

- PostgreSQL database to store events and configuration information
- A Web-based user interface for reporting and searching functionalities
- ActiveMQ Communication bus for messaging
- Advisor sample data
- Jasper reporting engine for reporting

You can distribute the Collector Manager to other locations, other machines and other operating systems by using the Collector Manager installer available through the Sentinel 6.1 Rapid Deployment Web interface. For example, you can install an additional Collector Manager on a Windows* machine to collect Windows events.

The Sentinel Server installer installs the following components:

4.1.1 Server Components

Table 4-1 *Sentinel Server Components and Applications*

Component	Description
Database	The Sentinel database stores configuration and event data.
Message Bus	A JMS-based message bus handles communication between components of the Sentinel system.
Correlation Engine	The correlation engine performs real-time event analysis.
Advisor	Advisor provides real-time correlation between detected IDS attacks and vulnerability scan output in order to immediately indicate increased risk to an organization. An Advisor data snapshot is installed by default if you have an Advisor licence. You need an Advisor license to subscribe to the ongoing Advisor data updates.
Data Access Service	Includes data storage, query, display, and processing components.
Web Server	Supports the Web interface for Sentinel Rapid Deployment.
Collector Manager	A service that handles connections to event sources, data parsing, mapping, and so on.
iTRAC™	Sentinel provides an iTRAC™ workflow management system to define and automate processes for incident response. Incidents that are identified in Sentinel, either by a correlation rule or manually, can be associated with an iTRAC workflow.

4.1.2 Client Applications

You can launch the client applications - the Sentinel Control Center, the Sentinel Data Manager, and the Solution Designer by using any of the following methods:

- Launch Java Webstart by using the Sentinel 6.1 Rapid Deployment Web interface
- Download the installers from the Sentinel 6.1 Rapid Deployment Web interface, run them, and launch them as client applications

Table 4-2 *Sentinel Client Applications*

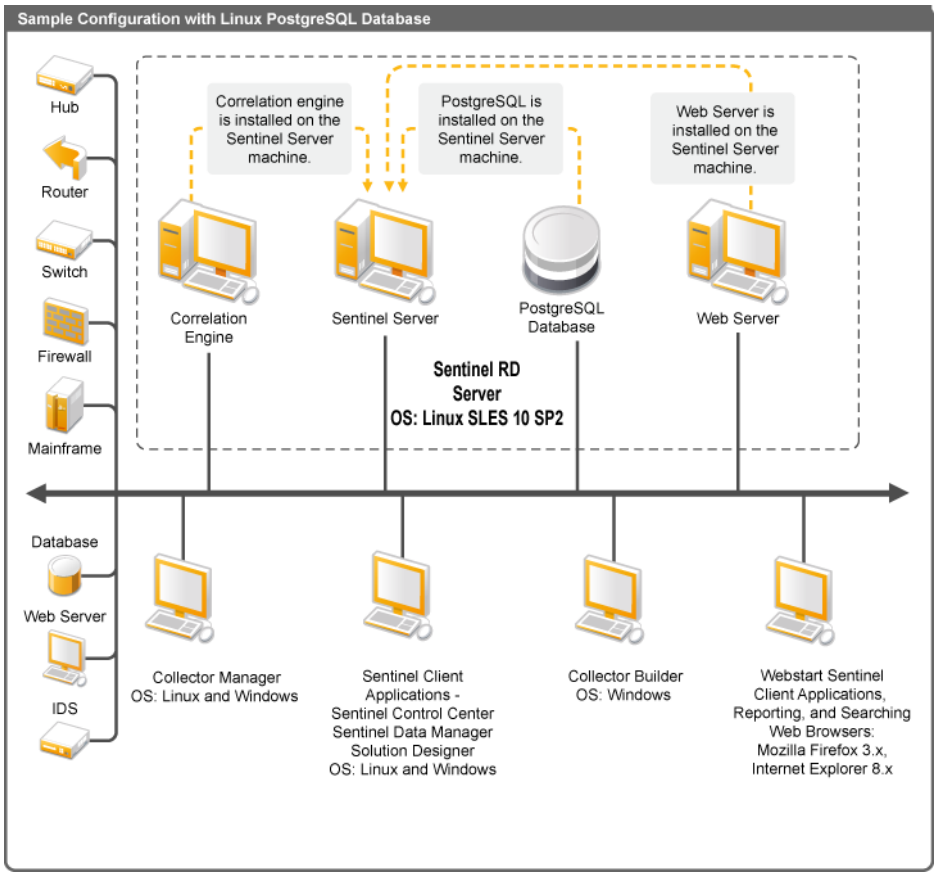
Component	Description
Sentinel Control Center	Main console for security or compliance analysts.
Sentinel Data Manager	Database management utility.
Solution Designer	Application for creating Solution Packs.

Component	Description
Sentinel Collector Manager	Service that handles connections to event sources, data parsing, mapping, and so on. A Collector Manager is installed on the Sentinel server, but additional Collector Managers can be installed on remote Windows or Linux* machines by using a downloadable installer.

4.2 Sentinel 6.1 Rapid Deployment Configuration

The following is the configuration set-up for Sentinel 6.1 Rapid Deployment.

Figure 4-1 *Sentinel 6.1 Rapid Deployment Configuration*



4.3 Port Numbers for Sentinel 6.1 Rapid Deployment Client Components

Use the following ports to configure your firewall setting to allow access between the Sentinel 6.1 Rapid Deployment server and the client components.

Table 4-3 Compatible Port Numbers for Sentinel RD Components

Port Number	Description
61616	The remote Collector Managers use this port number to connect to the Sentinel 6.1 Rapid Deployment server via ActiveMQ.
10013	The Sentinel Control Center uses this port number to connect to the Sentinel 6.1 Rapid Deployment server via a proxy.
5432	The Sentinel Data Manager uses this port number to connect to the PostgreSQL database.
8443	The Web clients use this port number to connect to the Sentinel 6.1 Rapid Deployment server.

4.4 Prerequisites

The following are several steps that should be taken before installing Sentinel. For more information about many of these prerequisites (including the list of certified platforms), see Chapter 3, "Sentinel 6.1 Rapid Deployment System Requirements," on page 23.

IMPORTANT: Sentinel installations using the full installer should always take place on a clean system. If Sentinel was previously installed on any of the machines, you must first uninstall it. For information on uninstalling previous versions of Sentinel, see the relevant Installation guides on the Novell Documentation Website (http://www.novell.com/documentation/).

4.4.1 Server

- Ensure that each server machine meets the minimum system requirements. For more information on prerequisites, see Chapter 3, "Sentinel 6.1 Rapid Deployment System Requirements," on page 23
- Install and configure an SMTP server if you want to be able to send mail notifications from the Sentinel system.

4.4.2 Client

- Ensure that each client machine meets the minimum system requirements.
- Ensure that you create a directory with ASCII-only characters (and no special characters) from which to run the installer.
- When you install remote Collector Manager or Client Applications on Linux OS machines, ensure that there are no folder-level restrictions set on the `/tmp` folder for the Admin user.

- Ensure that you provide Power user privileges to the Domain User for the Collector Manager on Windows because normal user rights are not sufficient for the Collector Manager installation.
- If you install the Collector Manager on a 64-bit machine, ensure that 32-bit libraries are available. The 32-bit libraries are required when running a Collector that is written in the proprietary collector language (which includes almost all Collectors written before June 2008) as well as when running certain Connectors (such as the LEA Connector). JavaScript-based Collectors and the remainder of Sentinel are 64-bit enabled. Verifying that these libraries are available is particularly important on Linux platforms, which might not include them by default.

4.4.3 Advisor

If you want to install Advisor, you must purchase the optional Sentinel Exploit Detection and Advisor Data Subscription. After you have purchased the subscription, use your Novell eLogin to download and update the Advisor data.

4.5 Installing the Sentinel 6.1 Rapid Deployment Server

The Sentinel 6.1 Rapid Deployment Server can be installed in the following ways:

- Section 4.5.1, “Single Script Installation with Root Privileges,” on page 31
- Section 4.5.2, “Non-Root Installation,” on page 33

4.5.1 Single Script Installation with Root Privileges

1. Log in as `root` to the server where you want to install Sentinel.
2. Select the `sentinel6_rd_x86-64.tar.gz` installer tar file, then download or copy it to a temporary directory.
3. Extract the install script from the file by using the following command:

   ```
   tar xfz sentinel6_rd_x86-64.tar.gz sentinel6_rd_x86-64/setup
   ```
4. Run the `root_install_all.sh` script with root privileges.

   Based on the directory you are in, on the system, run either of the following commands:

   - `sentinel6_rd_x86-64/setup/root_install_all.sh sentinel6_rd_x86-64.tar.gz`
   - `./root_install_all.sh ../../sentinel6_rd_x86-64.tar.gz`

   You can either log in as `root` and run the command or use the `sudo` command.
5. Choose one of the following languages by entering the corresponding number:

Serial Number	Language
1	Czech
2	English
3	French
4	German

Serial Number	Language
5	Italian
6	Japanese
7	Netherlands
8	Poland
9	Portuguese
10	Simplified Chinese
11	Spanish
12	Traditional Chinese

The End User License agreement is displayed in the selected language.

If the selected language is not available for the installer, the installer continues in English.

6. Read the End User License, then enter `1` or `y` if you agree to the terms and want to continue the installation.
7. Specify the license key.
8. Enter a password for the database administrator (`dbauser`).

   The `dbauser` credentials are used to create tables and partitions in the PostgreSQL database.
9. Re-enter the password to confirm.
10. Enter a password for the admin user.
11. Re-enter the password to confirm.
12. Specify your e-mail address. The Advisor e-mail notifications are sent to this address.

    IMPORTANT: Ensure that you configure the SMTP integrator to receive e-mail notifications for Advisor. For more information on configuring SMTP integrator, see Section 4.8.1, "Configuring an SMTP Integrator to Send Sentinel Notifications," on page 40.
13. You are prompted to specify if you have the Advisor User account. Do one of the following:
    - Enter 1 if you have purchased the Advisor account subscription.
    - Enter 2 if you have not purchased the account.
14. (Conditional) If you have purchased subscription for the Advisor account, specify the username and password for your Advisor account, which is the username and password for your Novell elogin account.

After installation, you can:

- Launch the Sentinel 6.1 Rapid Deployment Web interface by using the URL: `https://<SERVER_IP>:8443/sentinel`. The <*SERVER_IP*> is the IP of the machine where Sentinel is installed.
- Launch the Sentinel Control Center by running `/opt/novell/sentinel6_rd_x86-64/bin/control_center.sh` as the `novell` user.

4.5.2 Non-Root Installation

If your organizational policy prohibits running the full installation process as `root`, the installation can be completed in two steps. The first part of the installation procedure must be performed with `root` privileges, and the second part is performed as the administrative user (created during the first part).

1. Log in as `root` to the server where you want to install Sentinel.
2. Select the installer `sentinel6_rd_x86-64.tar.gz` tar file, then download or copy to a temporary directory.
3. If the `novell` user and `novell` group do not exist on the server, do the following:
   - **3a** Extract the script to create the `novell` user and `novell` group from the Sentinel tar file.

     For example:

     ```
     tar xfz sentinel6_rd_x86-64.tar.gz sentinel6_rd_x86-64/setup/
     root_create_novell_user.sh
     ```
   - **3b** As `root`, execute the script by using the following command:

     ```
     sentinel6_rd_x86-64/setup/root_create_novell_user.sh
     ```

     The `novell` user and `novell` group own the installation and the running processes of Sentinel.
4. Create a directory for Sentinel. For example:

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

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

   ```
   su - novell
   ```
7. Extract the installer tar file to installation directory you have created. For example:

   ```
   cd /opt/novell
   ```

   ```
   tar xfz sentinel6_rd_x86-64.tar.gz
   ```
8. Run the installation script as follows:

   ```
   /opt/novell/sentinel6_rd_x86-64/setup/install.sh
   ```
9. Log out and then log in again to load the environment variable changes made by the `install.sh` script.
10. Enable the software startup as a service by running the following script as `root`.

    ```
    sudo /opt/novell/sentinel6_rd_x86-64/setup/root_install_service.sh
    ```
11. Specify the number associated with the language to select the language for installation.

    The End User License agreement is displayed in the selected language.

    If the selected language is not available for the installer, the installer continues in English.
12. Read the end user license, then enter `1` or `y` if you agree to the terms and want to continue with the installation.
13. Specify the license key.
14. Enter a password for the database administrator (`dbauser`).

    The `dbauser` credentials are used to create tables and partitions in the PostgreSQL database.

15 Re-enter the password to confirm.

16 Enter a password for the admin user.

17 Re-enter the password to confirm.

18 Specify your e-mail address. The Advisor e-mail notifications are sent to this address.

19 Specify if you have an Advisor User account.

- Enter 1 if you have an account. This prompts you to enter your username and password.
- Enter 2 if you do not have an account.

IMPORTANT: Ensure that you configure the SMTP integrator to receive e-mail notifications for Advisor. For more information on configuring SMTP integrator, see Section 4.8.1, "Configuring an SMTP Integrator to Send Sentinel Notifications," on page 40.

---

20 Specify your Advisor username.

For example: Novell Bugzilla Account username.

21 Specify your password for the Advisor account.

After installation, you can:

- Launch the Sentinel 6.1 Rapid Deployment Web interface by using the URL: `https://<SERVER_IP>:8443/sentinel`. The <*SERVER_IP*> is the IP of the machine where Sentinel is installed.
- Launch the Sentinel Control Center by running `/opt/novell/sentinel6_rd_x86-64/bin/control_center.sh` as the `novell` user.

4.6 Installing the Client Applications

Use the Novell Sentinel 6.1 Rapid Deployment Web interface to download the Collector Manager installer and the Client installer.

4.6.1 Accessing Novell Sentinel 6.1 Rapid Deployment Web Interface

1 Open a Web browser to the following URL:

`https://<svrname.example.com>:8443/sentinel`

Replace <*svrname.example.com*> with the actual DNS name or IP address of the server where Sentinel is running.

IMPORTANT: The URL is case sensitive.

---

2 If you are prompted to verify the certificates, review the certificate information, then click *Yes* if it is valid.

3 Specify the username and password to access the Sentinel account.

4 Use the *Languages* drop-down list to select the language.

This is the same language as the language code of the Sentinel server and your local computer. Ensure that your browser's languages setting is configured to support the desired language.

5 Click *Sign in*.

6 Select *Applications*.

You can download the following:

Options	Description	Action
Collector Manager Installer	The Collector Manager Installer allows you install the Sentinel Collector Manager on supported Windows and Linux platforms.	Click *download Collector Manager installer* and follow the on-screen instructions.
Client Installer	The Client Installer allows you install the Sentinel Control Center, Sentinel Collector Builder, Sentinel Solution Designer, and Sentinel Data Manager on supported platforms.	Click *download Client installer* and follow the on-screen instructions.

4.6.2 Installing the Sentinel Client Applications

1 In the Applications page, click *download Client installer* to download `client_installer.zip` file.

2 Extract the install script from the file:

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

3 Go to the install directory and start the installation:

Platform	Action
Windows	Run `disk1\setup.bat` **NOTE:** On a Windows Vista machine, launch the command prompt by using the *Run as Administrator* option from the right-click menu options.

Platform	Action
Linux	• **GUI mode:** <*Install_Directory*>/disk1/setup.sh • **Console mode:** <*Install_Directory*>/disk1/setup.sh –console

4 Click the down-arrow and select one of the languages.

5 In the Welcome screen, click *Next*.

6 Read and accept the End User License Agreement. Click *Next*.

7 Accept the default install directory or click *Browse* to specify your installation location. Click *Next*.

IMPORTANT: You cannot install into a directory that uses special characters or non-ASCII characters in its name. For example, when installing Sentinel on Windows x86-64, the default path is `C:\\Program Files (x86)`. You must change this default path to avoid the special characters like (x86) if you want to continue the installation.

8 Select the Sentinel applications you want to install.

The following options are available:

Component	Description
Sentinel Collector Builder	Helps you develop new Collectors from scratch. **NOTE:** Collector Builder is supported only on Windows.
Sentinel Control Center	The main console for security or compliance analysts.
Sentinel Data Manager (SDM)	Used for manual database management activities.
Solution Designer	Helps you create Solution packs.

9 If you chose to install Sentinel Control Center, the installer prompts you for the maximum memory space to be allocated to Sentinel Control Center. Specify the maximum JVM* heap size (MB) to be used only by Sentinel Control Center.

The allowed range is 64-1024 MB.

10 Specify the Sentinel Administrator username and the path to the corresponding home directory.

This option is not available if any Sentinel applications are already installed.

This is the username of the user who owns the installed Sentinel product. If the user does not exist, a user is created along with a home directory in the specified directory.

- **OS Sentinel Administrator Username:** The default is `esecadm`.
- **OS Sentinel Administrator User Home Directory:** The default path is `/export/home`. If the username is esecadm, the corresponding home directory is `/export/home/esecadm`.

Set a password to log in as the `esecadm` user.

11 Specify the following information:

- **Message bus port:** The port on which the communication server is listening. Components connecting directly to the communication server use this port. The default port number is 61616.
- **Sentinel Control Center Proxy Port:** The port on which the SSL proxy server (Data Access Server Proxy) listens to accept the username and password. The SSL proxy server accepts the credentials based on the authenticated connections. Sentinel Control Center uses this port to connect to the Sentinel Server. The default port number is 10013.
- **Communication Server host name:** The machine IP or hostname where the Sentinel 6.1 Rapid Deployment server is installed.

Ensure that the port numbers are the same as on the Sentinel server at `/opt/novell/<Install_Directory>/config/configuration.xml` to enable communications. Make a note of these ports for future installations on other machines.

12 Click *Next*.

13 A summary of the installation is displayed. Click *Install*.

14 Click *Finish* to complete installation.

NOTE: When you log in again, use the username you specified in Step 10.

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

```
env | grep ESEC_USER
```

This command returns the username if the user is already created and the environment variables are already set.

4.6.3 Installing the Sentinel Collector Manager

The Sentinel Collector Manager is available for download in the Applications page of the Sentinel 6.1 Rapid Deployment Web interface.

1 In the Web interface, click *download Collector Manager installers* to download `scm_installer.zip` file.

2 Extract the install script from the file:

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

3 Go to the install directory and start the installation:

Platform	Action
Windows	Run the following command: `disk1\setup.bat`
Linux	◆ **GUI mode:** `<Install_Directory>/disk1/setup.sh` ◆ **Console mode:** `<Install_Directory>/disk1/setup.sh –console`

4 Select a language to proceed with the installation.

5 Read the Welcome screen, then click *Next*.

6 Read and accept the End User License Agreement. Click *Next*.

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

IMPORTANT: You cannot install into a directory that uses special characters or non-ASCII characters in its name. For example, when installing Sentinel on Windows x86-64, the default path is `C:\\Program Files (x86)`. You must change the default path to avoid the special characters like (x86) if you want to continue the installation.

8 Specify the Sentinel Administrator username and path to the corresponding home directory.

This option is not available if any Sentinel applications are already installed.

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

  This is the username of the user who owns the installed Sentinel product. If the user does not already exist, a user is created with corresponding home directory in the specified directory.

- **OS Sentinel Administrator User Home Directory:** The default is `/export/home`. If `esecadm` is the username, the corresponding home directory is `/export/home/esecadm`.

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

9 Specify the following, then click *Next*.

- **Message bus port:** The port on which the communication server is listening. Components connecting directly to the communication server use this port. The default port number is 61616.
- **Communication Server hostname:** The machine IP or hostname where the Sentinel 6.1 Rapid Deployment server is installed.

Ensure that the port numbers are the same on every machine in the Sentinel system to enable communications. Make a note of these ports for future installations on other machines.

10 Specify the following:

- **Automatic Memory Configuration:** Select the total amount of memory to allocate to the Collector Manager. The installer automatically determines the optimal distribution of memory across components, considering the estimated operating system and database overhead.

IMPORTANT: You can modify the -Xmx value in the `configuration.xml` file to change the RAM allocated to the Collector Manager process. The `configuration.xml` file is placed in the `<Install_Directory>/config` on Linux or `<Install_Directory>\config` on Windows.

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

11 Click *Next*.

A summary screen with the features selected for installation is displayed.

12 Click *Install*.

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

Use the username collectormanager, and its corresponding password that is available in the `/opt/novell/sentinel6_rd_x86-64/config/activemqusers.properties` file on the Sentinel server.

An example for the credentials available in the `activemqusers.properties` is given below:

```
collectormanager=cefc76062c58e2835aa3d777778f9295
```

Where, `collectormanager` is the username and `cefc76062c58e2835aa3d777778f9295` is the corresponding password.

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

14 After installation, you are prompted to reboot or to log in again and start the Sentinel services manually. Click *Finish* to reboot your system.

NOTE: When you log in again, use the username you specified in Step 8.

If you forget the username you have set, open a terminal console and enter the following command with `root` credentials.

```
env | grep ESEC_USER
```

This command returns the username if the user is already created and the environment variables are already set.

4.7 Manually Starting and Stopping the Sentinel Services

To start the Sentinel services manually, use either of the following commands:

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

To stop the Sentinel services manually, use either of the following commands:

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

4.8 Post-Installation Configuration

This section helps you understand the post-installation configuration for the Sentinel 6.1 Rapid Deployment services.

4.8.1 Configuring an SMTP Integrator to Send Sentinel Notifications

In Sentinel 6.1 Rapid Deployment, a JavaScript `SendEmail` Action works with an SMTP integrator to send mail messages from various contexts within the Sentinel interface to mail recipients. The recipients of the mail message and the message contents are configured in the action parameters.

A single action instance of the `SendEmail` action plugin is created automatically in every Sentinel installation. This action is used internally by Sentinel to send mail in the following situations:

- When a Correlation rule deployed with a Send Email action is triggered. The Send Email action referred here is the action indicated by the gear icon, which is only valid for correlation (as opposed to the JavaScript `SendEmail` Action, which is indicated by the JS JavaScript icon).
- Workflow includes a Mail Step or Activity that is configured to send email.
- User opens an incident and selects to execute an Activity that is configured to send email.
- User right-clicks an event and selects *Email*.
- User opens an incident and selects *Email Incident*.
- Advisor download sends a notification.

No configuration is necessary to the *SendEmail* Action, but the SMTP Integrator must be configured with valid connection information before it works. For more information, see “Sending an E-mail” in the *Sentinel 6.1 Rapid Deployment User Guide*.

4.8.2 Collector Manager Services

Additional Collectors

During the installation of the Collector Manager, a Collector called the Generic Collector is configured. By default, it creates events at the rate of 5 events per second (eps). This Collector can be used to test the installation. Additional Collectors can be downloaded from the Novell Web site (http://support.novell.com/products/sentinel/collectors.html).

Starting the Collector Manager Services

Table 4-4 *Starting the Collector Manager Service*

Using the Admin Tab in SCC	Using the Event Source Management Option in Sentinel Control Center
1. Launch Sentinel Control Center 2. Select *Admin tab* > *Servers View*. You can also click *Servers View* in Navigator pane. 3. Expand the *Servers view* to view the list of processes. 4. Right-click the Collector Manager you must start, then select *Actions* > *Start*.	1. Launch the Sentinel Control Center. 2. Click *Event Source Management* > *Live View*. 3. In the *Event Source Management (Live View)* window, right-click the Collector Manager you want to start, then select *Start*.

Installing Additional Load Balancing Nodes for a Collector Manager

Collector managers for Sentinel manage all the data collection processes and data parsing.Occasionally, it might be necessary to add an additional Sentinel Collector Manager node to a Sentinel environment in order to load-balance across machines. Remote collector managers provide several benefits:

- Allow distributed event parsing and processing to improve system performance.
- Allow filtering, encryption, and data compression at the source system through collocation with event sources. This reduces network bandwidth requirements and provides additional data security.
- Allow installation on additional operating systems. For example, installing a Collector Manager node on Microsoft Windows* to enable data collection by using the WMI protocol.
- Allow file caching that enables the remote collector manager to cache large amounts of data when the server is temporarily busy with archiving or processing a spike in events. This is an advantage for protocols, such as syslog, that do not natively support event caching.

The Collector Manager components can be load-balanced by installing instances of these components on additional machines. To do this, simply run the installer on the new machine as described in the Section 4.6.3, “Installing the Sentinel Collector Manager,” on page 37.

4.8.3 Managing Time

You must connect the Sentinel Server to an NTP (Network Time Protocol) server or other type of time server. If the system time across machines is not synchronized, the Sentinel Correlation Engine and Active Views do not work properly. The events from the Collector Managers are not considered to be real-time and are therefore not sent directly to the Sentinel database, bypassing the Sentinel Control Centers and Correlation Engines.

By default, the threshold for real-time data is 120 seconds. This can be modified by changing the value of `esecurity.router.event.realtime.expiration` in the `event-router.properties` file. The Sentinel event time populates based on the Trust Device Time or the Collector Manager Time. You can select the Trust Device Time while configuring a collector. Trust Device Time is the time when the log was generated by the device and the Collector Manager Time is the local system time of the Collector Manager system.

4.9 LDAP Authentication

4.9.1 Configuring Sentinel 6.1 Rapid Deployment Server for LDAP Authentication

A Sentinel 6.1 Rapid Deployment server can be configured for LDAP authentication to enable users to log in to Sentinel by using a Novell eDirectory™ username or Microsoft* Active Directory* sAMAccountName and password.

NOTE: LDAP authentication is currently supported only on systems that have Sentinel 6.1 Rapid Deployment Hotfix 2 or later installed.

To configure Sentinel 6.1 Rapid Deployment for LDAP authentication:

1 Export the self-signed certificate of the Certificate Authority (CA) for the eDirectory/Active Directory tree to a base64-encoded file.

For more information on exporting an eDirectory CA certificate, see Exporting an Organizational CA's Self-Signed Certificate (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html).

NOTE: For exporting an eDirectory CA certificate in iManager, the Novell Certificate Server Plug-ins for iManager must be installed. For more information on installing an iManager plug-in, see Downloading and Installing Plug-in Modules (http://www.novell.com/documentation/imanager27/imanager_admin_273/?page=/documentation/imanager27/imanager_admin_273/data/hk42s9ot.html).

For more information on exporting an Active Directory CA certificate, see Exporting the certificate on the Active Directory server (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itame.doc_5.1/am51_install213.htm).

NOTE: For LDAP authentication, Active Directory must additionally be configured to allow anonymous queries. For more information, see Configuring Active Directory to Allow Anonymous Queries for NSL LDAP Client (http://www.novell.com/coolsolutions/appnote/15120.html).

2 Copy the certificate file to the following directory on Sentinel 6.1 Rapid Deployment server:

```
/opt/novell/<Install_Directory>/config
```

3 Set the ownership and permissions of the certificate file as follows:

```
chown novell:novell /opt/novell/<Install_Directory>/config/<certificate-file>
```

```
chmod 700 /opt/novell/<Install_Directory>/config/<certificate-file>
```

4 Log in to Sentinel 6.1 Rapid Deployment server as `novell` user:

```
su - novell
```

5 Change to the following directory:

```
/opt/novell/<Install_Directory>/bin
```

6 Run the ldap_auth_config.sh script:

```
./ldap_auth_config.sh
```

NOTE: The script takes a backup of the configuration files `auth.login` and `configuration.xml` present in the /opt/novell/<Install_Directory>/config directory as `auth.login.sav` and `configuration.xml.sav` respectively in the same directory before modifying them for LDAP authentication.

7 Specify the following information:

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

Parameter	Description/Action
Sentinel install location	The installation directory of Sentinel 6.1 Rapid Deployment server. The default location is: `/opt/novell/<Install_Directory>`
LDAP directory	The value is 1 for Novell eDirectory or 2 for Active Directory. The default value is 1.
LDAP server hostname or IP address	The hostname or the IP address of the machine where the LDAP server is installed. The default value is localhost.
LDAP server port	The port number for a secured LDAP connection. The default port number is 636.

Parameter	Description/Action

LDAP subtree to search for users	The subtree in the directory that has the user objects.
	The following are examples for specifying the subtree in eDirectory and Active Directory:
	◆ eDirectory:
	`ou=users, o=novell`
	NOTE: For eDirectory, if no subtree is specified, then the search is run on the entire directory.
	◆ Active Directory:
	`CN=users, DC=TEST AD, DC=provo, DC=novell, DC=com`
	NOTE: For Active Directory, the subtree cannot be blank.

Filename of the LDAP server certificate	The filename of the eDirectory/Active Directory CA certificate that you have copied in Step 2 on page 43.

8 Enter one of the following:

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

9 Enter `y` to restart the Sentinel 6.1 Rapid Deployment server.

NOTE: If there are any errors, revert the changes made to the configuration files `auth.login` and `configuration.xml` in the /opt/novell/<Install_Directory>/config directory:

```
cp -p auth.login.sav auth.login
cp -p configuration.xml.sav configuration.xml
```

10 Log in to Sentinel Control Center as `admin` and create a domain user with the same username as the eDirectory username or Active Directory sAMAccountName.

For more information on creating a domain user, see "Creating a User Account" in the *Sentinel 6.1 Rapid Deployment User Guide*.

You have successfully configured Sentinel 6.1 Rapid Deployment server for LDAP authentication and the user can log in to Sentinel Control Center and Sentinel Solution Designer by using the eDirectory username or Active Directory sAMAccountName and password.

4.9.2 Configuring LDAP Failover Servers

To configure one or more Sentinel servers as failover servers for LDAP authentication:

1 Log in to the Sentinel server as the administrator.

2 Stop the Sentinel services.

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

3 Change to the `<Install_Directory>/config` directory:

```
cd <Install_Directory>/config
```

4 Open the `auth.login` file for editing.

```
vi auth.login
```

4a Update the userProvider in the LdapLogin section to specify multiple LDAP URLs. Separate each URL by a blank space.

For more information on setting up multiple LDAP URLs, see Class LdapLogin Module (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

4b Save the changes.

5 Add each failover LDAP server certificate to the keystore that you have already created.

```
<Install_Directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
-file <ldap_certfile.b64> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

where *<ldap_certfile.b64>* is the ldap certificate filename in b64 encoding format and *<alias_name>* is the alias name for the certificate to be imported.

IMPORTANT: Ensure that you specify the alias. If no alias is specified, the keytool takes `mykey` as the alias by default. Therefore, when you import multiple certificates into the keystore without specifying an alias, the keytool reports an error that the alias already exists.

---

6 Start the Sentinel services.

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

4.9.3 Modifying the LDAP Authentication Configuration

1 Log in to a Sentinel 6.1 RD server as novell user:

```
su - novell
```

2 Change to the following directory:

```
cd /opt/novell/<Install_Directory>/config
```

3 Delete the following lines from the image attribute of the DAS Query process element in the configuration.xml file:

```
-Djavax.net.ssl.trustStore=/opt/novell/sentinel6_rd_x86/config/
ldap_server.keystore
```

```
-Djavax.net.ssl.trustStorePassword=sentinel
```

4 Delete the keystore file, `ldap_server.keystore`:

```
rm ldap_server.keystore
```

5 Perform Step 1 on page 44through Step 9 on page 44 in the Section 4.9.1, “Configuring Sentinel 6.1 Rapid Deployment Server for LDAP Authentication,” on page 42.

4.10 Updating the License Key from an Evaluation Key to a Production Key

If you purchase the product after evaluation, follow the procedure given below to update your license key to avoid re-installation:

1. Log into the machine where Sentinel is installed as the Sentinel Administrator operating system user (the default is `admin`).
2. At the command prompt, change directory to the `<Install_Directory>/bin`.
3. Enter the following command:

   ```
   ./softwarekey.sh
   ```
4. Specify number 1 to set your primary key. Press Enter.
5. Enter your new licence key.

Security Considerations for Sentinel 6.1 Rapid Deployment

5

This section provides specific instructions on how to securely install, configure, and maintain Novell® Sentinel™ 6.1 Rapid Deployment.

5.1 Securing Communication Across the Network

Communication between the various components of Sentinel 6.1 Rapid Deployment is across the network, and there are different kinds of communication protocols used throughout the system.

5.1.1 Communication between Sentinel Server Processes

Sentinel server processes include DAS Core, DAS Binary, Correlation Engine, Collector Manager, and the Web server. They communicate with each other by using ActiveMQ.

The communication between these server processes is by default over SSL via the ActiveMQ message bus. To configure SSL, specify the following information in `<Install_Directory>/configuration.xml`:

```
 <jms brokerURL="ssl://
localhost:61616?wireFormat.maxInactivityDuration=0&amp;jms.copyMessageOnSend=
false" interceptors="compression" keystore="../config/
.activemqclientkeystore.jks" keystorePassword="password"
password="1fef3bcdd3fbcbc5cd795346a9f04ddc" username="system"/>
```

For more information on setting up custom server and client certificates, see ““Processes” in the *Sentinel 6.1 Rapid Deployment User Guide*.

5.1.2 Communication between the Sentinel Server and the Sentinel Client Applications

Sentinel Client applications such as the Sentinel Control Center (SCC), Sentinel Data Manager (SDM), and Solution Designer use SSL communication by default via the SSL Proxy Server.

To enable communication between the Sentinel server and the SCC, the SDM and the Solution Designer running as client applications on the server, specify the following information in the `<Install_Dirirectory>/configuration.xml`:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory">
      <transport type="ssl">
        <ssl host="localhost" keystore="/opt/novell/sentinel6_rd_x86-64/
config/.proxyClientKeystore" port="10013" usecacerts="false"/>
      </transport>
    </strategy>
```

To enable communication between the Sentinel server and the SCC, the SDM, and the Solution Designer running through Web Start, the communication strategy is defined on the server in the `<Install_Dirirectory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml` file as follows:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory" >
      <transport type="ssl">
        <ssl host="164.99.18.162" port="10013" keystore="./.novell/sentinel/
.proxyClientKeystore" />
      </transport>
    </strategy>
```

For more information on setting up custom server and client certificates, see “Processes” in the *Sentinel 6.1 Rapid Deployment User Guide*.

5.1.3 Communication between the Server and the Database

The protocol used for communication between the server and the database is defined by the JDBC driver and is used for the communication with the database. Some drivers are capable of encrypting the communication with the database.

Sentinel Rapid Deployment uses the PostgreSQL driver (`postgresql-<version>.jdbc3.jar`) provided at PostgreSQL Download Page (http://jdbc.postgresql.org/download.html), to connect to the PostgreSQL database, which is a Java (Type IV) implementation. This driver supports encryption for data communication. To configure encryption for the data communication, refer to PostgreSQL Encryption Options (http://www.postgresql.org/docs/8.1/static/encryption-options.html).

NOTE: Turning encryption on has a negative impact on the performance of the system. Therefore, this security concern needs to be weighed against your performance needs. The database communication is not encrypted by default for this reason.

5.1.4 Communication between the Collector Managers and Event Sources

You can configure Sentinel to collect data from the event source in a secure manner depending on the protocols that the event source supports. For example, the LEA WMS, SYSLOG, and AUDIT Connector can be configured to encrypt their communication with their respective devises. For more information on the possible security features that can be enabled, refer to the Connector and Event source vendor documentation given in the Novell Sentinel Content Page (http://support.novell.com/products/sentinel/secure/sentinel61.html).

5.1.5 Communication with the Web Browsers

The Web server is by default configured to communicate via HTTPS. For more information, see the Tomcat documentation (http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html).

5.1.6 Communication between the Database and Other Clients

You can configure the PostgreSQL SIEM database to allow connection from any client machine by using the Sentinel Data Manager or by using any third-party application such as Pgadmin*.

To allow the Sentinel Data Manager to connect from any client machine, add the following line in the `<Install_Dirirectory>/3rdparty/postgresql/data/pg_hba.conf` file:

```
host    all         all         0.0.0.0/0             md5
```

If you want to limit the client connections that are allowed to run and connect to the database through the SDM, replace the line above with the IP address of the host.

The following line in `pg_hba.conf` is an indicator to PostgreSQL to accept connections from the local machine so that the Sentinel Data Manager is allowed to run only on the server.

```
host all all 127.0.0.1/32 md5
```

In order to limit connections from other client machines, you can add additional `host` entries.

5.2 Securing Users and Passwords

5.2.1 Operating System Users

Server Installation

The Sentinel 6.1 Rapid Deployment Server installation creates a `novell` system user and novell group that own the installed files within the <*install_directory*>. If the user does not exist, it is created and its home directory is set to `/home/novell`. If a new user is created, the password for the user is not set by default in order to maximize security. If you want to log in to the system as the novell user, you must set a password for the user after installation.

Collector Manager Installation

Linux: The installer prompts you to specify the name of the system user who will own the installed files, as well as the location to create its home directory. By default, the system user is `esecadm`; however, you can change this system username. If the user does not exist, it is created along with its home directory. If a new user is created, the password for the user is not set by default to maximize security. If you want to log in to the system as the user, you must set a password for the user after installation.The default group is `esec`.

During the client installation, if the user already exists, the installer does not prompt for the user again. This behavior is similar to the behavior during uninstallation or reinstallation of software. If you want the installer to prompt for the user again:

1. Delete the user and group created at the time of first installation
2. Clear the environment variables ESEC_USER from `/etc/profile`

Windows: No users are created.

The password policies for system users are defined by the operating system that is being used.

5.2.2 Sentinel Application and Database Users

All Sentinel 6.1 Rapid Deployment application users are native database users and their passwords are protected by using procedures followed by the native database platform. These users have only read access to certain tables in the database so that they can execute queries against the database.

The admin user is the administrator user for all Sentinel applications to login.

By default the following database users are created during installation:

The dbauser is created as a superuser who can manage the database. The password for the dbauser is accepted at the time of installation. This password is stored in the <user home directory>/.pgpass. The system follows the PostgreSQL database password policies.

The appuser is the non-superuser that is used by the Sentinel applications to connect to the database. By default, the appuser uses a password that is randomly generated during installation, and is stored encrypted in the <*Install_directory*>/config container xml files (`das_core.xml`, `das_binary.xml`, etc.). To change the password for the appuser, use the <install_directory>/bin/dbconfig utility.

NOTE: There is also a postgreSQL database user that owns the entire database including system database tables. By default, the postgres database user is set to NOLOGIN so that no one can login as the postgreSQL user.

5.3 Securing Sentinel Data

IMPORTANT: Because of the highly sensitive nature of the data on the Sentinel Server, you should keep the machine physically secure and in a secure area of the network. To collect data from event sources outside the secure network, use a remote Collector Manager.

For certain components, passwords must be stored so that they are available when the system needs to connect to a resource such as the database or an event source. In this case, when the password is stored, it is first encrypted to avoid unauthorized access to the clear text password.

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

FILES

`advisor_client.xml`

Database Credentials

The Database credentials are stored in the `<Installation_Directory>/config/server.xml` file

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Advisor Credentials

```
<obj-component id="DownloadComponent">
          <class>esecurity.ccs.comp.advisor.feed.NewAdvClientDownload</class>
      <property name="advisor.downloadfrom.url">https://secure-www.novell.com/
sentinel/advisor/advisordata</property>
      <property name="username">kveerareddy</property>
      <!-- Set the password (encrypted) using the adv_change_password script -
->
      <property name="password">jqhlWIX8HD6GDHVX9FApWg==</property>
<property name="compression.enabled">true</property>
      <!--
        Set the following properties to connect through an HTTP proxy.
       Set the proxy password (encrypted) using the adv_change_password script
(make a
        copy of the script and add "-x" to the java cmd line to set the proxy
password
        instead of the advisor password.
      -->
      <!--
      <property name="proxy_host"></property>
      <property name="proxy_port"></property>
      <property name="proxy_username"></property>
      <property name="proxy_password"></property>
      -->
        </obj-component>
```

Configuration.xml

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.Ac
tiveMQStrategyFactory" name="ActiveMQ">
      <jms brokerURL="ssl://
localhost:61616?wireFormat.maxInactivityDuration=0&amp;jms.copyMessageOnSend=
false" interceptors="compression" keystore="../config/
.activemqclientkeystore.jks" keystorePassword="password"
password="ebccfebf4ec3dac874494b992a91a3c9" username="system"/>
    </strategy>
```

das_binary.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

das_core.xml

```
 <class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Some database tables store passwords and certificates. This sensitive data is encrypted and is stored in the tables listed below. you must limit the access to these tables.

- **EVT_SRC:** ect_src_config column data
- **evt_src_collector:** columns: evt_src_collector_props
- **evt_src_grp (doubt):** columns: evt_src_default_config
- **md_config:** column : data
- **integrator_config:** column : integrator_properties
- **md_view_config:** column : view_data
- **esec_content :** column: content_context, content_hash
- **esec_content_grp_content :** columns: content_hash
- **sentinel_plugin:** columns: content_pkg, file_hash

Sentinel 6.1 Rapid Deployment stores both configuration data and event data. This data is stored in the following locations:

Table 5-1 *Locations for Configuration Data and Event Data*

Components	Location for Configuration Data	Location for Event Data
Sentinel 6.1 Rapid Deployment Server	Database tables and the file system (<*Install_Directory*>/config) This configuration information includes the encrypted database, event source, integrators, and passwords.	Database (EVENTS, CORRELATED_EVENTS, and EVT_SMRY_*, AUDIT_RECORD tables) and the file system at <*Install_Directory*>/data/eventdata and <*Install_Directory*>/data/raw data Event data can be archived to the file system as part of the partition management job.
Correlation Engine	File system (<*Install_Directory*>/config). The only sensitive configuration information is the client key pair used to connect to the message bus.	correlation_engine.cache
DAS Core	<*Install_Directory*>/config	das_core.cache
DAS Binary	<*Install_Directory*>/config	Event data might be cached if the database is down das_binary.cache
Collector Manager	File system (<*Install_Directory*>/config). The only sensitive configuration information is the client key pair used to connect to the message bus.	Event data might be cached on the file system during error conditions such as the message bus being down or event overflow. This event data is stored in the <*Install_Directory*>/data/collector_mgr.cache directory
Client Applications	File system (*Install_Directory*/config). The client applications don't store any sensitive information in their configuration files . For example, client applications can export ESM data to a local file system. The exported file contains encrypted passwords, if they are present in the configuration of the event sources that were exported. Although the passwords are encrypted, the ESM export permission should only be given to users that can be trusted with this privilege.	None

5.4 Backing Up Information

- Events should be archived regularly. The backup media should be stored in a secure offsite facility.

  Periodically do the following:

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

    If the changes such as updating plug-ins or adding nodes are made to ESM later, you must export the configuration and save it again.
  - Save all the report, rules, and actions in Solution Designer.
  - Back up the entire installation directory, instead of particular sections, so there is no risk of manual mistakes and so the process is quicker.
  - Back up the database. For more information on backing up the PostgreSQL database, see PostgreSQL: Backup and Restore (http://www.postgresql.org/docs/8.1/static/backup.html).
  - Back up the `/opt/novell/<install_directory>/config` directory.
- For sensitive data, use one of the following methods to encrypt the data backup:
  - Encrypt the data itself if the application that creates the data supports encryption. For example, database products and third-party tools support data encryption. Use backup software that is able to encrypt data as you back it up. This method has performance and manageability challenges, especially for managing encryption keys.
  - Use an encryption appliance that encrypts sensitive backup media as data is backed up.
- If you transport and store media offsite, use a company that specializes in media shipment and storage. Make sure that your tapes are tracked via bar codes, stored in environmentally friendly conditions, and are handled by a company whose reputation rests on its ability to handle your media properly.
- Load Recovery Certificates. The Novell Sentinel service by default is not configured for the Recovery agent. During server configuration via YaST, ensure that the Recovery agent path is configured. This path should contain the list of certificates that the service can load for the users to select from. For more information, see “Certificate Management for Sentinel 6.1 Rapid Deployment Server” in the Sentinel 6.1 Rapid Deployment Reference Guide.

  YaST contains modules for the basic management of X.509 certificates. This mainly involves the creation of CAs, sub-CAs, and their certificates. For more information about how to manage and update certificates, see the Managing X.509 Certification (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html) in the *SUSE Linux Enterprise Server 10 Installation and Administration Guide* (http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html).
- If you want to back up filters and workflows you must back up specific tables. You must build your system in a control-based fashion, For example, create specific sets of content that implement a desired control. You can then store these content in a Solution Pack, which can then be backed up. This ensures that a lot of other information is captures along with filters and Active Views.

5.5 Securing the Operating System

- Sentinel 6.1 Rapid Deployment is supported on SUSE® Linux Enterprise Server (SLES) 10 SP2 or later. For more information on securing a SLES machine, see the SuSE Linux Enterprise Server 10 documentation (http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html).
- Secure access to the Sentinel 6.1 Rapid Deployment server with a firewall. If the Sentinel server is accessible from outside the corporate network, a firewall should be employed to prevent direct access by an intruder.

  Enable the following ports in the firewall:

Components	Port
ActiveMQ	61616*
PostgreSQL	5432
Tomcat	8443*
Sentinel Control Center Proxy Client port	10013*
Proxied trusted client	10014*
internal_gateway_server and internal_gateway Used between engine and manager	5556
internal_router_server and internal_router_client Used between event router client and server	5558
Event listener port configured in `config/collector_mgr.properties` as "`esecurity.agentmanager.event.port`"	35000

NOTE: Ports marked with the asterisk might be different if they were already in use on the system at the time of installation. If they were in use at the time of installation, substitute in the port numbers that were prompted for at the time of installation.

For more information on enabling a firewall on SLES 10, see Configuring Firewalls with YaST (http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html) in the *SLES 10 Administration Guide*.

5.6 Auditing Sentinel

Sentinel automatically generates events for many of its internal actions. These events can be viewed in the Active Views or accessed through a search or report. For more information, see ""Viewing Real-Time Events" in the *Sentinel 6.1 Rapid Deployment User Guide*.

5.7 Generating an SSL Certificate for the Server

You can replace the self-signed certificate with a certificate signed by a major Certificate Authority (CA), such as VeriSign*, Thawte*, or Entrust*. You can also replace the self-signed certificate with a certificate signed by a less common CA, such as a CA within your company or organization. For more information, see “Certificate Management for Sentinel 6.1 Rapid Deployment Server” in the Sentinel 6.1 Rapid Deployment Reference Guide.

Advisor Configuration

6

This section discusses loading Advisor data and configuring regular updates to the Advisor data.

6.1 Advisor Overview

Advisor is a subscription service that provides device-level correlation between real-time events from intrusion detection and prevention systems and enterprise vulnerability scan results. By providing normalized attack information, Advisor acts as an early warning service to detect attacks against vulnerable systems (exploit detection). It also provides associated remediation information.

Advisor is a necessary component if you want to use the Sentinel Exploit Detection. Advisor is a subscription-based data service and requires an additional license from Novell. For evaluation purpose, a snapshot of the Advisor data by default is installed with the Sentinel 6.1 Rapid Deployment database if you have an Advisor licence. You need to procure this licence to receive the benefit of ongoing Advisor data updates and exploit-vulnerability mappings.

6.2 Installing Advisor

A snapshot of the Advisor data is installed as part of the Sentinel 6.1 Rapid Deployment installation. However, to download and install the ongoing Advisor data updates from the Advisor server, you need a current subscription and valid credentials. During the installation, you can specify the credentials to access the Advisor server. After sentinel installation, Advisor new feed files from the Internet are routinely downloaded, if available. This action is triggered by the automatic cron job installed on the Sentinel 6.1 Rapid Deployment server. When the cron job executes the `advisor.sh` script, it starts processing the initial Advisor data. By default, downloading the Advisor data updates is scheduled to run every 6 hours.

For more information on installing Advisor data, see Step 18 thru Step 21 on page 34 in the Section 4.5.1, “Single Script Installation with Root Privileges,” on page 31.

6.2.1 Updating Advisor Data in a Secured Environment

When the Sentinel 6.1 Rapid Deployment server is installed on a machine in a secured environment, it requires a manual update to the Advisor data. Installations in a secure environment frequently do not have internet connections; therefore, you must manually download and copy the Advisor data to the machine.

The Advisor data can be manually downloaded from the following location by using the Novell eLogin and password for the user who is entitled to the Advisor subscription:

Advisor Data (https://secure-www.novell.com/sentinel/advisor/advisordata)

6.3 Maintaining Advisor

Several maintenance tasks for Advisor that are described in the Sentinel user guide:

- Changing the password Advisor uses for automatic data updates, if needed
- Changing the configuration for Advisor notification mail.
- Changing the scheduled data update time.
- Updating Advisor data manually to be effective, the Advisor data must be updated on a regular basis as new attacks and vulnerabilities are added to the data feed. If these updates are not taking place by default, they must be performed manually. For more information, see Section 6.2.1, “Updating Advisor Data in a Secured Environment,” on page 57.

Testing the Sentinel 6.1 Rapid Deployment Installation

7

Sentinel™ Rapid Deployment is installed with a Generic Collector that can be used to test many of the basic functions of the system. You can use the Collector to test Active Views, Incident creation, Correlation rules, and Reports.

7.1 Testing the Rapid Deployment Installation

The following procedure describes the steps to test the system and the expected results. You might not see the same events, but your results should be similar to the results below.

At a basic level, these tests allow you to confirm the following:

- Sentinel Services are up and running
- Communication over the message bus is functional
- Internal audit events are being sent
- Events can be sent from a Collector Manager
- Events are inserted into the database and can be retrieved by using a report
- Incidents can be created and viewed
- Rules are evaluated and correlated events are triggered by the Correlation Engine
- The Sentinel Data Manager is connected to the database and can read the partition information

If any of these tests fail, review the installation log and other log files, and contact Novell Technical Support (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) if necessary.

To test the installation:

1. Log in to a Sentinel 6.1 Rapid Deployment Web interface.

   For more information, see ““Accessing the Novell Sentinel Web Interface” in the *Sentinel 6.1 Rapid Deployment User Guide*.

2. Select the Search page and search for any internal event. One or more events should be returned.

   For example, to search internal events within the severity range 3-5, select *Include System Events*, then enter *sev:[3 TO 5]* in the *Search* field.

   For more information on Search, refer to “Running an Event Search” in the *Sentinel 6.1 Rapid Deployment User Guide*.

3. Select the Reports page, specify the parameters, and run a report.

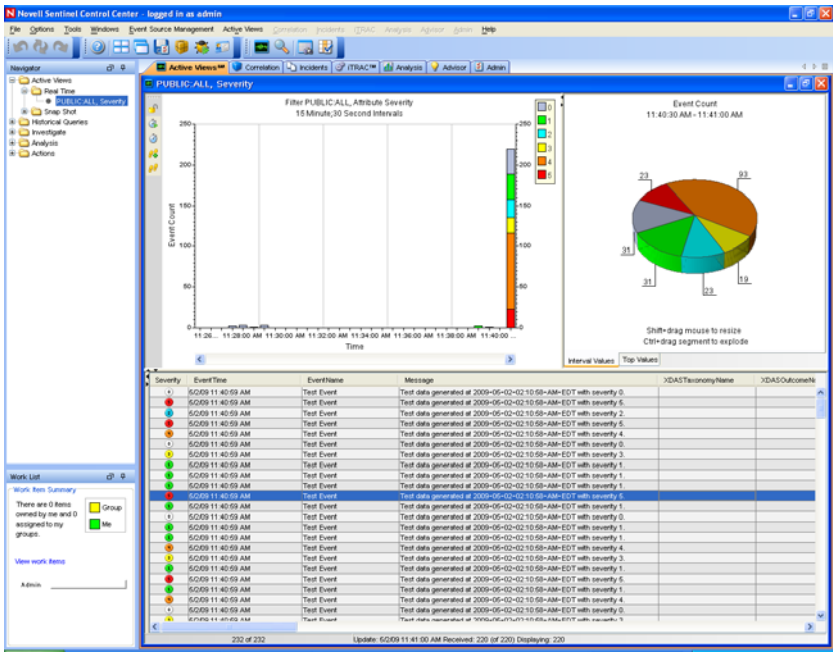
   For example, click the *Run* button next to Sentinel Core Event Configuration 6.1r1, then specify the desired parameters, and click *Run*.

For more information, refer to "Running Reports" in the *Sentinel 6.1 Rapid Deployment User Guide*.

4 In the Applications page, click *Launch Sentinel Control Center*.

5 Log into the system by using the Sentinel Administrative User specified during installation (admin by default).

The Sentinel Control Center opens and you can see the *Active Views* tab with the events filtered by the public filters *Internal_Events* and *High_Severity*.



6 Go to the *Event Source Management* menu and select *Live View*.

7 In the Graphical view, right-click *5 eps event source* and select *Start*.

8 Close the Event Source Management Live View window.

9 Click the *Active Views* tab.

You can view the Active window titled PUBLIC: High_Severity, Severity. It might take some time for the Collector to start and the data to be displayed in this window.

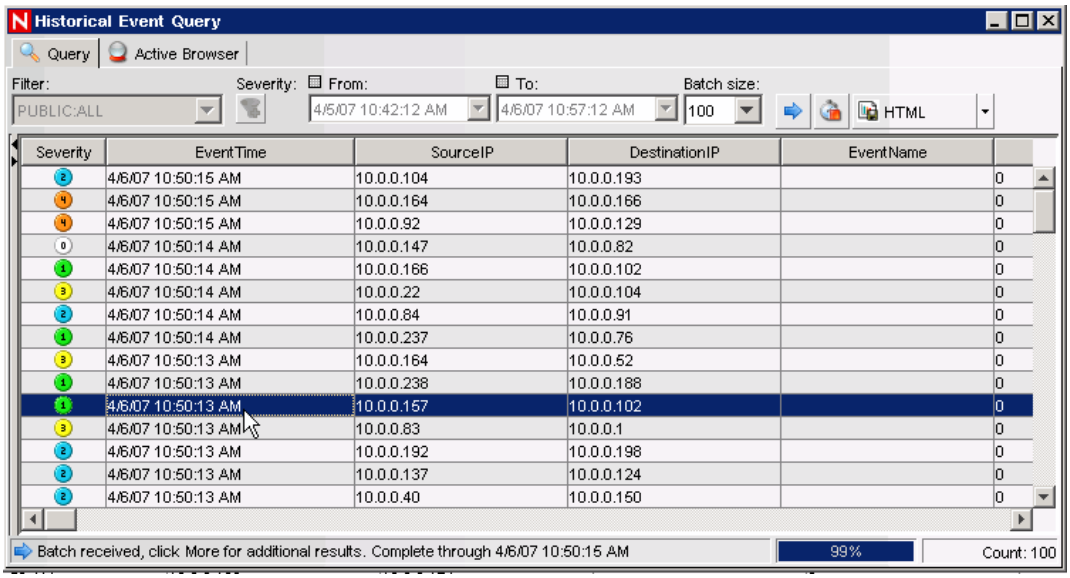
10 Click the *Event Query* button in the toolbar. The Historical Event Query window is displayed.

11 In the *Historical Event Query* window, click the *Filter* down-arrow to select the filter. Select *Public: All* filter.

12 Select a time period that covers the time that the Collector has been active. Use the *From* and *To* drop-down arrow to select the date range.

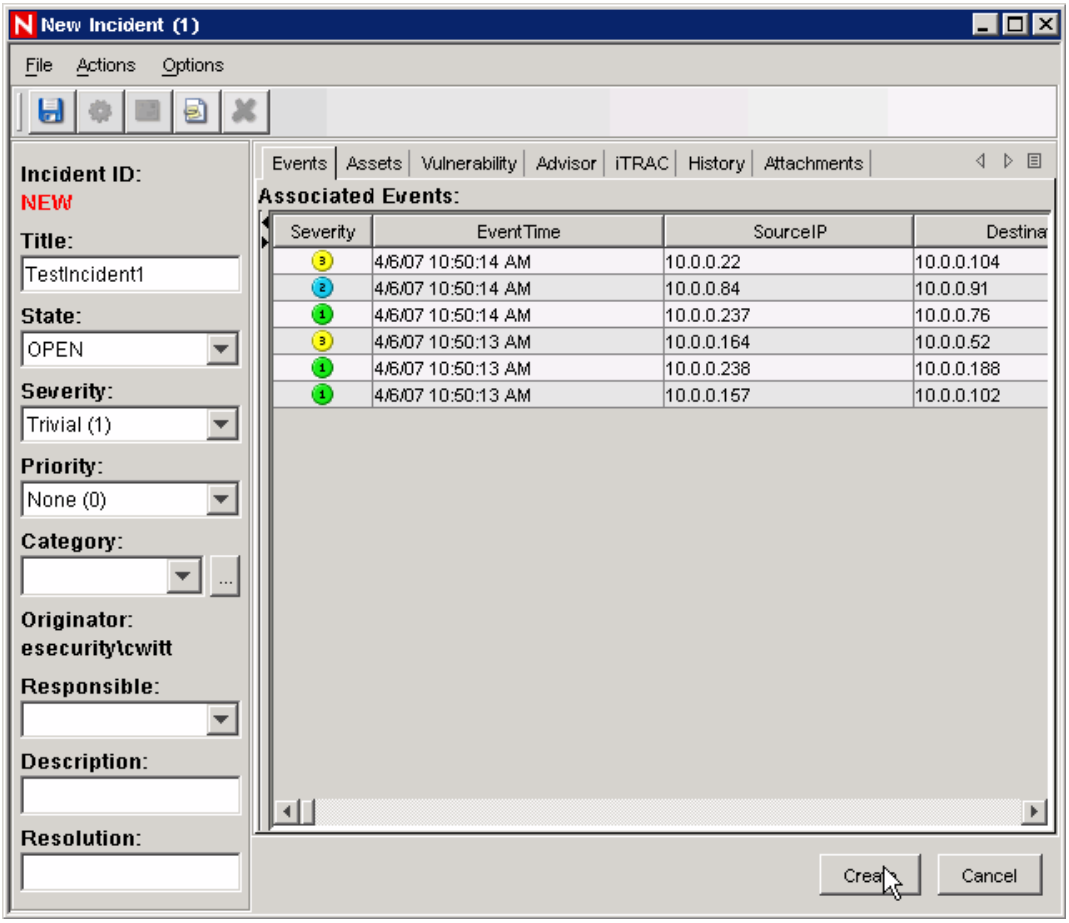
13 Select a batch size.

14 Click the magnifying glass icon to run the query.



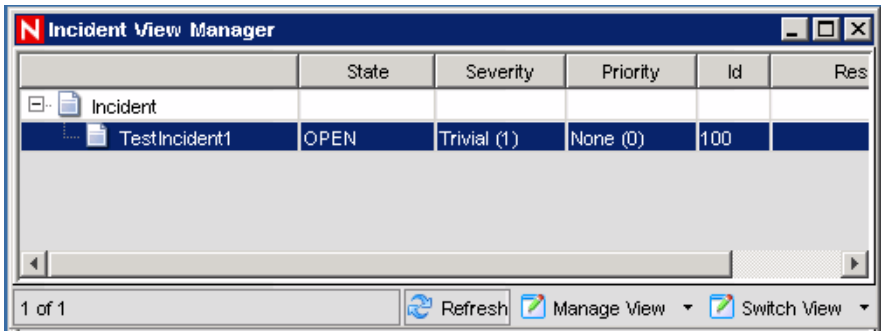
15 Hold down the Ctrl or Shift key and select multiple events from the Historical Event Query window.

16 Right-click and select *Create Incident*.

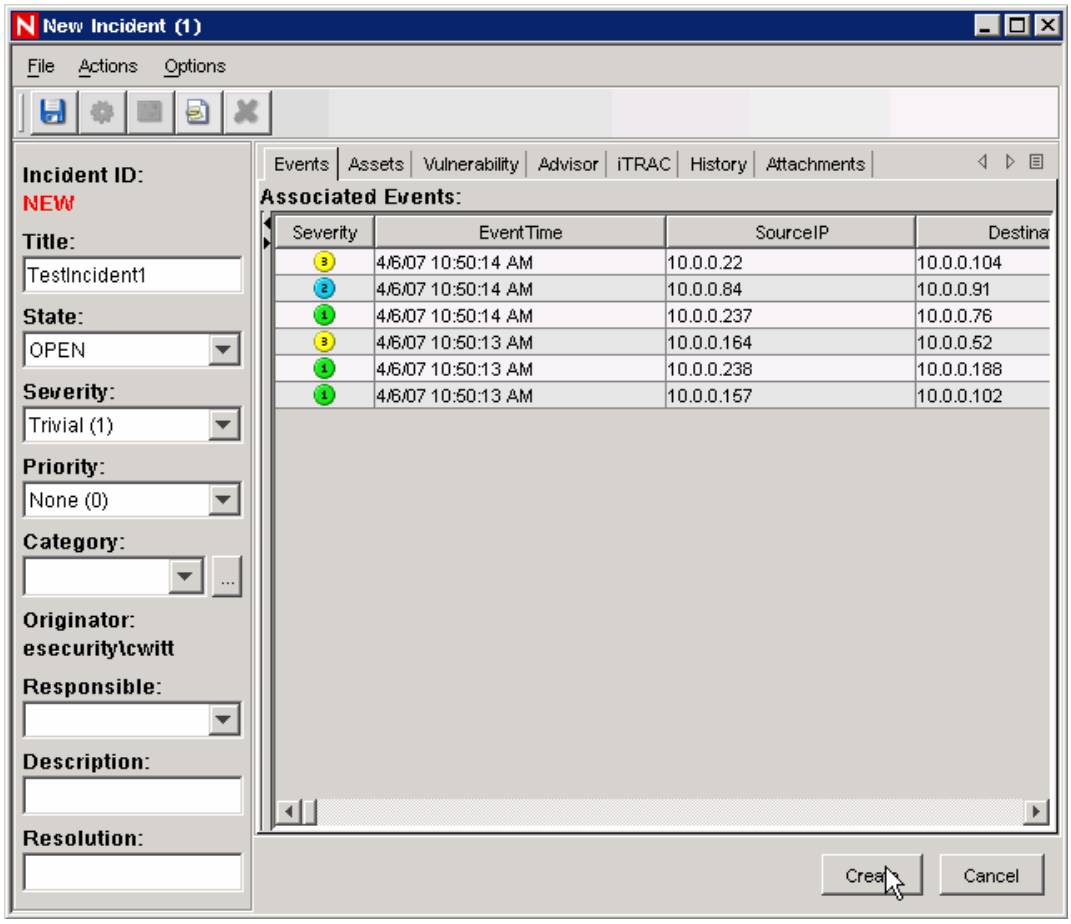


17 Name the incident TestIncident1 and click *Create*. When a success notification displays, click *OK*.

18 Click the *Incident* tab to see the incident you just created in the Incident View Manager.



19 Double-click the incident to display.



20 Close the *Incident* Window.

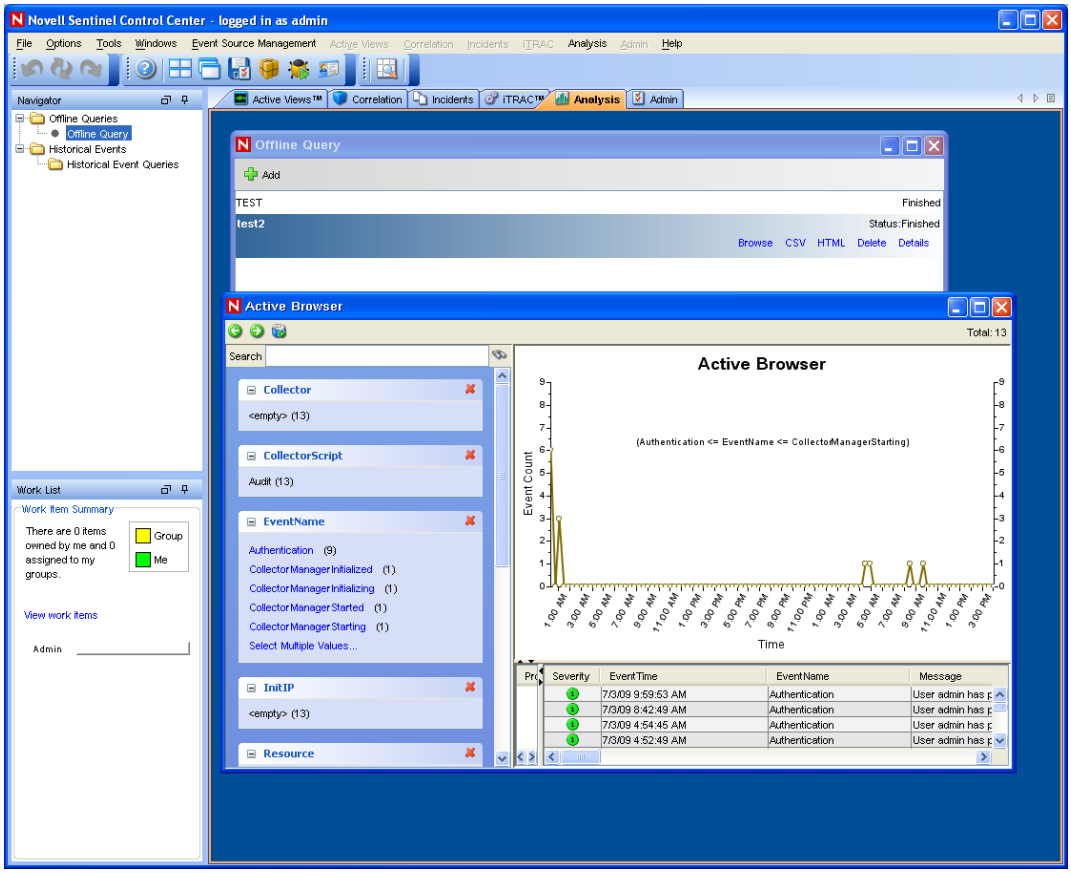
21 Click the *Analysis* tab.

22 Click *Offline Queries* from the Analysis menu or from the Navigator.

23 In the Offline Query window, click *Add*.

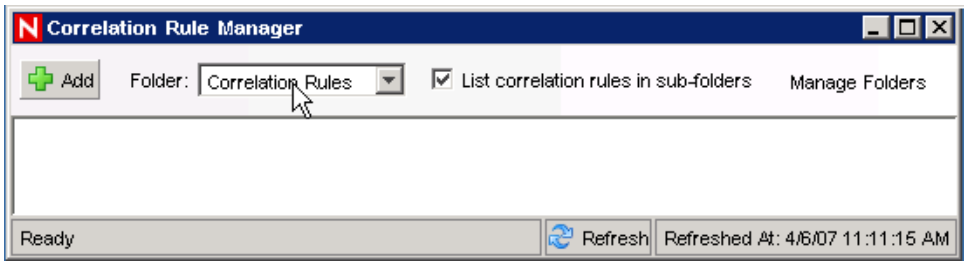
24 Specify a name, select a filter, select a time period, then click *OK*.

25 Click *Browse* to view the list of events and associated details in the Active Browser window.

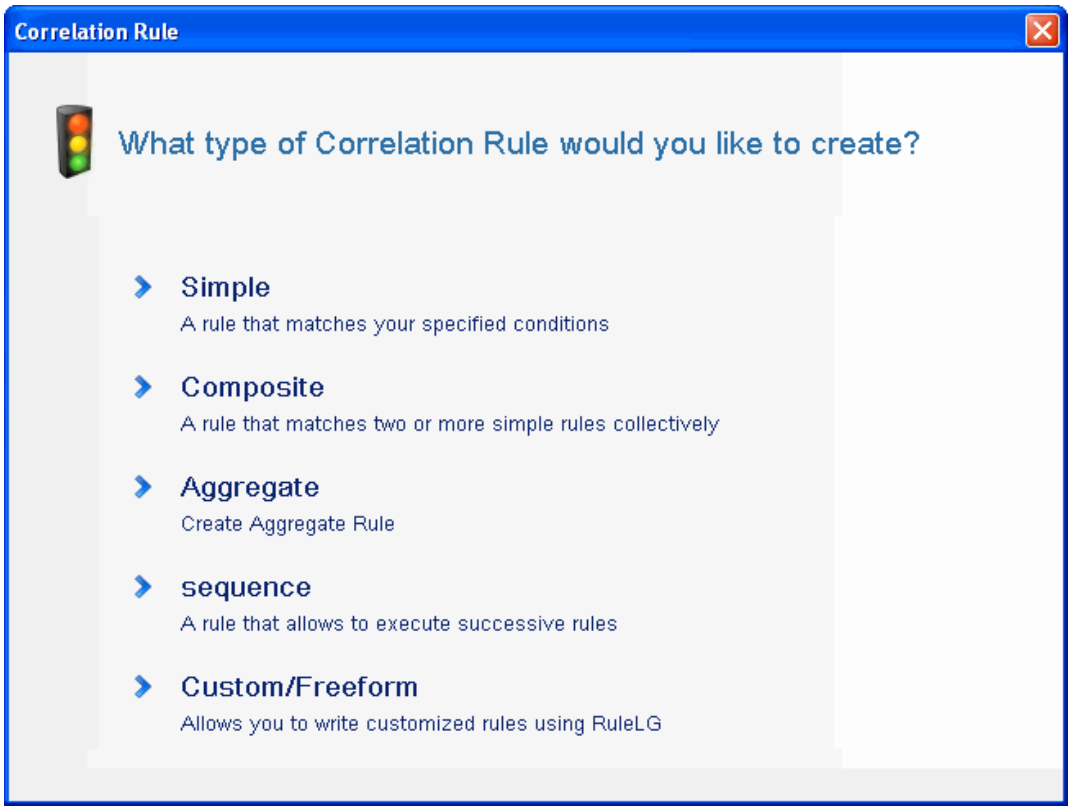


You can view the details such as Collector, Target IP, Severity, Target Service Port, Resource etc.

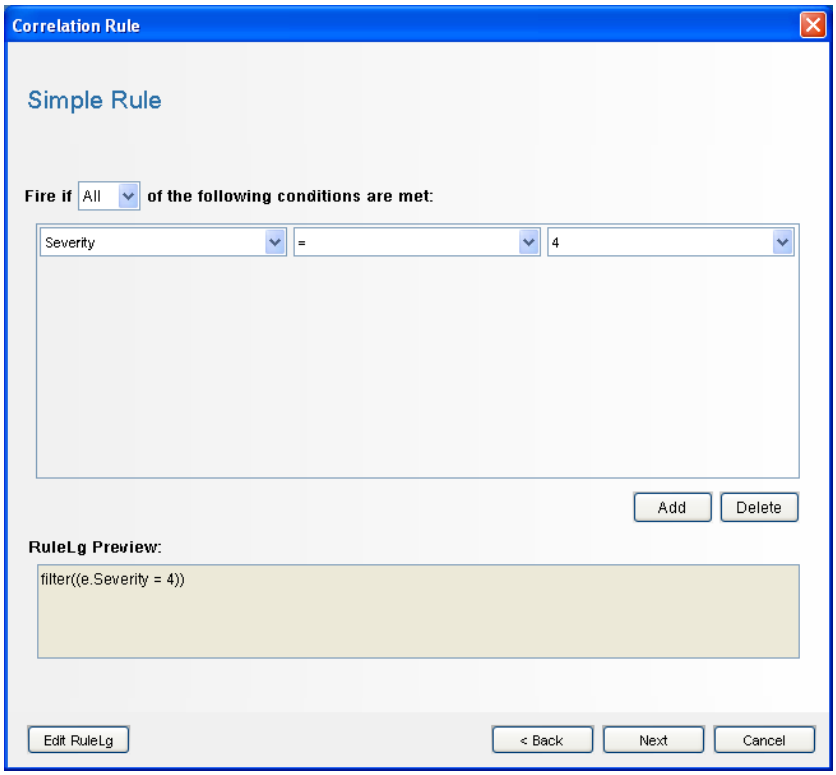
26 Select the *Correlation* tab. The Correlation Rule Manager is displayed.



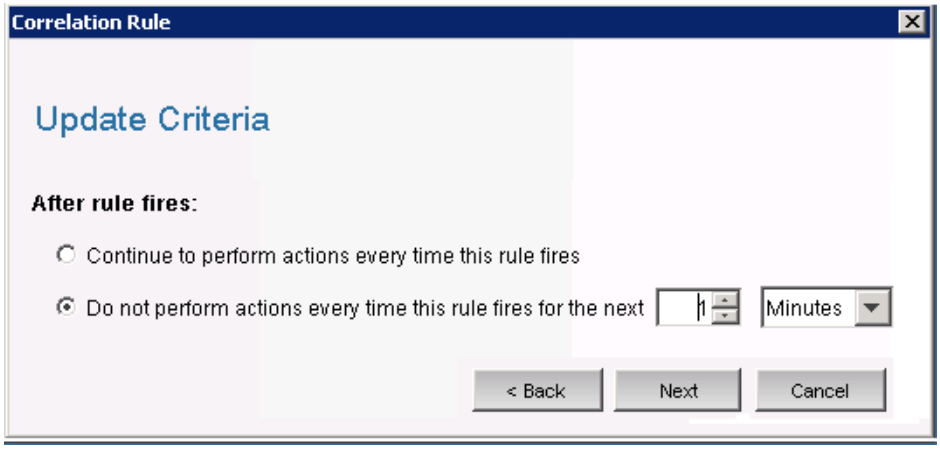
27 Click *Add*. The Correlation Rule Wizard displays.



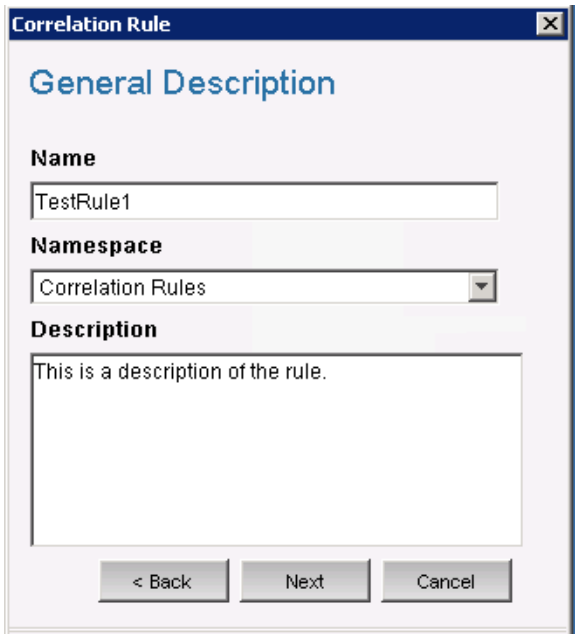
28 Click *Simple*. Simple Rule window displays.



29 Use the drop-down menus to set the criteria to Severity=4, then click *Next*. The Update Criteria window displays.



30 Select *Do not perform actions every time this rule fires* and use the drop-down menu to set the time period to 1 minute. Click *Next*. The General Description window displays.



31 Name the rule as *TestRule1*, provide a description, and click *Next*.

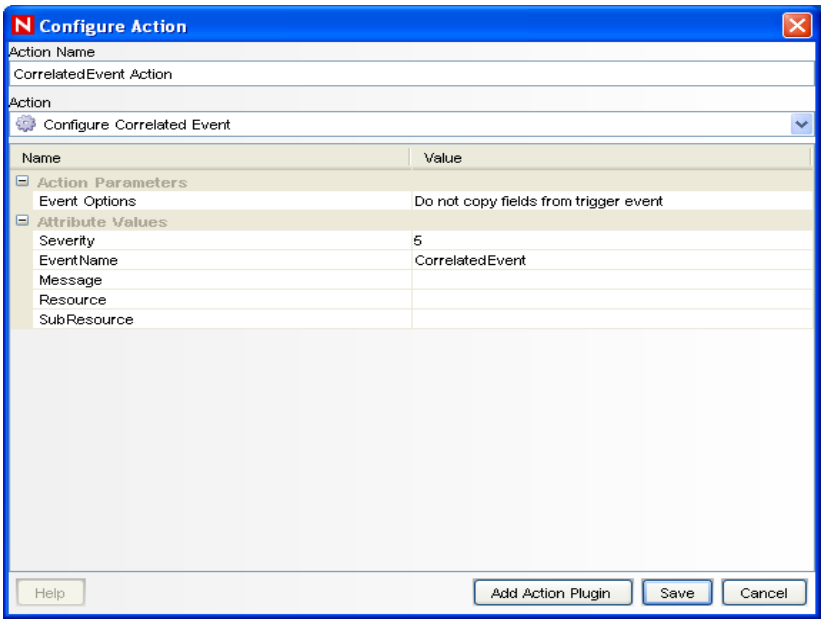
32 Select *No, do not create another rule* and click *Next*.

33 Create an action to associate with the rule you have created:

33a Perform either of the following:

- Select *Tools* > *Action Manager* > *Add*.
- In the Deploy Rule window, click *Add Action*. For more information, see Step 34 thru Step 35 on page 66.

The Configure Action window is displayed.



33b In the Configure Action window, specify the following:

- Specify the action name. For example, CorrelatedEvent Action.
- Select *Configure Correlated Event* from the *Action* drop-down list.
- Set the *Event Options*.
- Set the *Severity* to 5.
- Specify the *EventName*. For example, CorrelatedEvent.
- Specify a message if required.

For more information on creating an action, see "Creating Actions" in the *Sentinel 6.1 Rapid Deployment User Guide*.

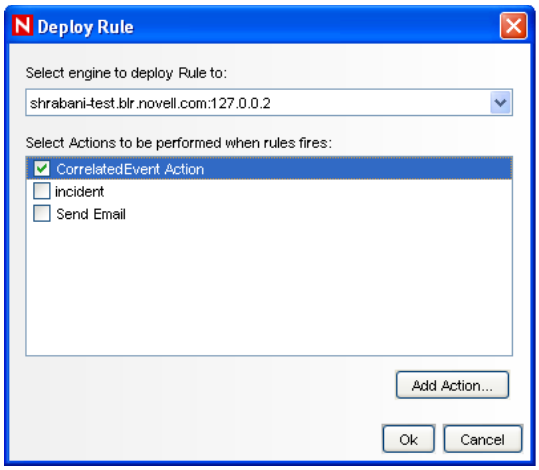
33c Click *Save*.

34 Open the Correlation Rule Manager window.

35 Select a rule and click *Deploy Rules* link. The Deploy Rule window displays.

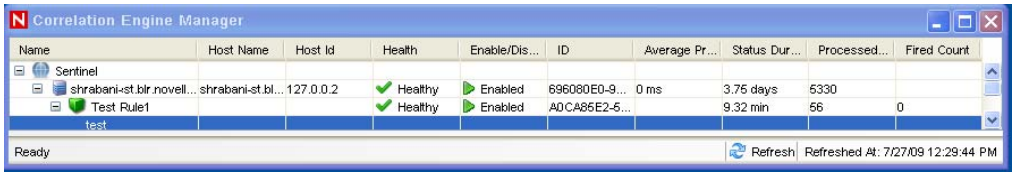
36 In the Deploy Rule window, select the Engine to deploy the rule.

37 Select the action you have created in Step 33 on page 65 to associate with the rule and click *OK*.



38 Select *Correlation Engine Manager*.

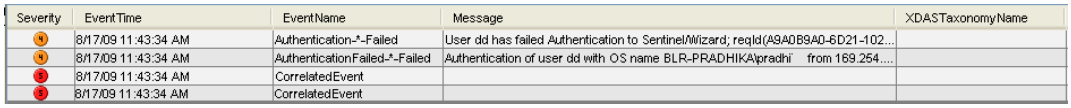
Under the Correlation engine, you can see the rule is deployed and enabled.



39 Trigger an event of severity 4 such as failed authentication to fire the deployed correlation rule.

For example, open a Sentinel Control Center login window and give wrong user credentials to generate such an event.

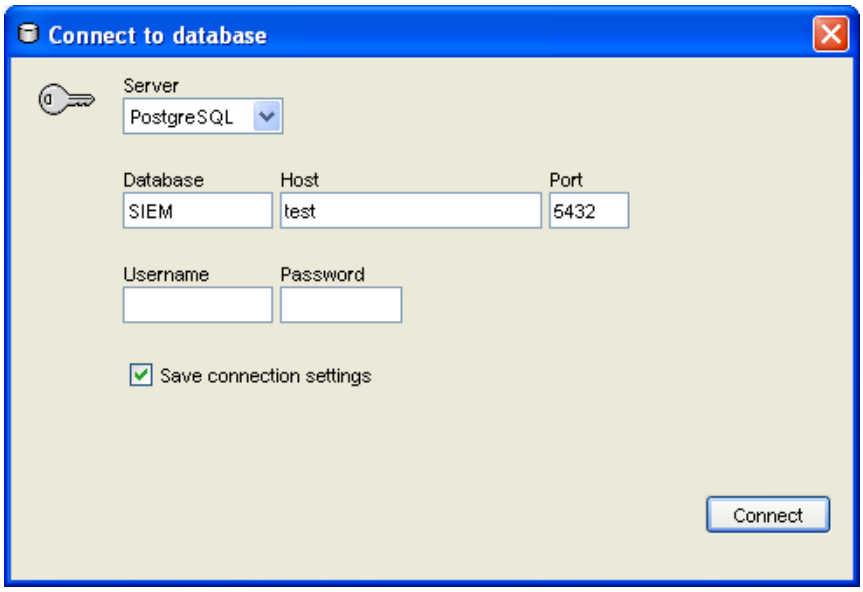
40 Click the *Active Views* tab and verify that the Correlated Event is generated.



41 Close the Sentinel Control Center.

42 In the Applications page, click *Launch Sentinel Data Manager*.

43 Log into Sentinel Data Manager by using the Database Administrative User specified during installation (dbauser by default).



44 Click each tab to verify that you can access it.

45 Close Sentinel Data Manager.

If you proceeded through all of these steps without errors, you have completed a basic verification of the Sentinel system installation.

7.2 Cleaning Up after Testing

After completing the system verification, you should remove the objects created for the tests.

1 Log into the system using the Sentinel Administrative User specified during installation (admin by default).

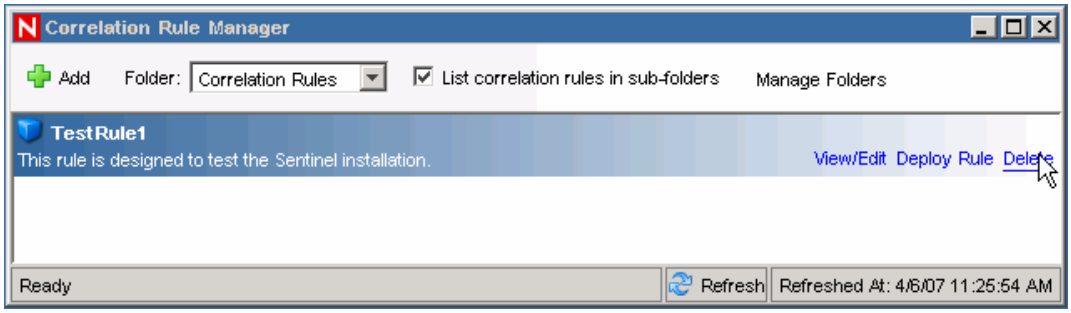
2 Select the *Correlation* tab.

3 Open the Correlation Engine Manager.

4 Right-click *TestRule1* in the Correlation Engine Manager and select *Undeploy*.

5 Open the Correlation Rule Manager.

6 Select *TestRule1* and click *Delete*.



7 Select the *Event Source Management* menu and select *Live View*.

8 In the Graphical event source hierarchy, right-click *General Collector* and select *Stop*.

9 Close the Event Source Management window.

10 Click the *Incidents* tab.

11 Open the Incident View Manager.

12 Select *TestIncident1*, right-click, and select *Delete*.

7.3 Getting Started

To get started with real data, you will need to import and configure Collectors that are appropriate for your environment, configure your own rules, build iTRAC workflows, and so on. For more information, see *Sentinel 6.1 Rapid Deployment User Guide*. Sentinel Solution Packs can help you get started quickly. See The Sentinel Content Page (http://support.novell.com/products/sentinel/sentinel61.html) for more details.

Uninstalling Sentinel 6.1 Rapid Deployment

8

Before performing a new Sentinel™ 6.1 Rapid Deployment installation, it is highly recommended that you uninstall any previous installation of Sentinel 6, to ensure that there are no files or system settings remaining from the earlier version.

For information on uninstalling previous versions of Sentinel, see the relevant Installation guides on the Novell Documentation Web site (http://www.novell.com/documentation/).

8.1 Uninstalling the Sentinel 6.1 Rapid Deployment Server

1. Run the following command to stop the Sentinel services:

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

2. Run the following command to ensure that all the Sentinel processes have stopped working:

   ```
   ps -ef | grep novell
   ```

3. Stop any remaining processes manually by entering the following command:

   ```
   kill -9 pid
   ```

4. Use the following command with necessary `root` permissions to uninstall the Sentinel service:

   ```
   sudo /opt/novell/sentinel6_rd_x86-64/setup/root_uninstall_service.sh
   ```

5. Verify with necessary `root` permissions that the services are removed:

   ```
   chkconfig | grep sentinel
   ```

6. Uninstall the Advisor cron job from the novell user's crontab:

   ```
   sudo /opt/novell/sentinel6_rd_x86-64/setup/root_uninstall_cron.sh
   ```

7. Verify with necessary root permissions that the `advisor.sh` script is removed from the crontab:

   ```
   crontab -u novell -l
   ```

8. Delete the Installation directory:

   ```
   rm -rf /opt/novell/sentinel6_rd_x86-64
   ```

   IMPORTANT: Unless you remove the `sentinel6_rd_x86-64` directory, the uninstallation of Sentinel 6.1 Rapid Deployment is not complete.

9. Remove the environment variable entries that were added to the novell user's profile:

   9a Open the `.bashrc` file with vi:

   ```
   vi ~novell/.bashrc
   ```

   9b Remove the following lines from the file:

```
APP_HOME=/opt/novell/sentinel6_rd_x86-64
export PATH=$APP_HOME/bin:$PATH
```

9c Save your changes.

10 Remove the `dbauser` entry from the `.pgpass` file from the home directory of the novell user:

```
vi ~novell/.pgpass
```

After uninstalling Sentinel, certain system settings remain, which you can manually remove. These settings should be removed before performing a clean installation of Sentinel, particularly if the Sentinel uninstallation encountered errors.

1. Log in as the `root` user.
2. Ensure that all the Sentinel processes are stopped.
3. Make sure that nobody is logged in as the Sentinel Administrator user, then remove the user, corresponding home directory, and group by using the following commands.
   - `userdel -r novell`
   - `groupdel novell`

8.2 Uninstalling the Remote Collector Manager and Sentinel Client Applications

8.2.1 Linux

1. Log in as `root`.
2. Go to the following location:

   `<Install_Directory>/_uninst`
3. Perform any of the following:

Mode	Command
GUI	`./uninstall.bin` Continue with Step 4 on page 72.
Console	`./uninstall.bin -console` Continue with the on-screen instructions.

4. Select a language and click *OK*.
5. In the Sentinel UninstallShield Wizard, click *Next*.
6. Select the components you want to uninstall and click *Next*.
7. Ensure that any running Sentinel applications are stopped and click *Next*.

   A summary of the features selected for uninstall is displayed.

8 Click *Uninstall*.

9 Click *Finish*.

8.2.2 Windows

1 Log in as an Administrator user.

2 Do either of the following:

- Select *Start* > *All Programs* > *Sentinel* > *Uninstall Sentinel*.
- Select *Start* > *Run*, enter `<Install_Directory>\_uninst`, then double-click `uninstall.exe`.

3 Select a language and click *OK*.

The Sentinel 6.1 Rapid Deployment UninstallShield Wizard is displayed.

4 Click *Next*.

5 Select the components you want to uninstall and click *Next*.

6 Ensure that any running Sentinel applications are stopped and click *Next*.

A summary of the features selected for uninstalling is displayed.

7 Click *Uninstall*.

8 Select to reboot the system and click *Finish*.

8.2.3 Post-Uninstallation Procedures

After uninstalling the applications, certain systems settings remain, which can be manually removed. These settings should be removed before performing a clean installation of Sentinel, particularly if the Sentinel uninstallation encountered errors.

NOTE: On Linux, uninstalling Collector Manager or Client Applications does not remove the Sentinel Administrator User from the operating system. You need to manually remove that user, if desired.

- "Linux" on page 73
- "Windows" on page 74

Linux

1 Log in as `root`.

2 Remove the contents of the `<Install_Directory>` where Sentinel software is installed.

3 Remove the following files in the `/etc/init.d` directory, if they exist:

`sentinel`

This is applicable only if Collector Manager is installed.

4 Make sure nobody is logged in as the Sentinel Administrator user (esecadm by default), then remove the user, home directory,and esec group:

- Run `userdel -r esecadm`
- Run `groupdel esec`

5 Remove the `/root/InstallShield`.directory.

6 Remove the InstallShield section of `/etc/profile`.

7 Restart the machine.

Windows

1 Delete the `%CommonProgramFiles%\InstallShield\Universa`l folder and all of its contents.

2 Delete the <*`Install_Directory`*> folder (by default: `C:\Program Files\Novell\Sentinel6`).

3 Right-click *My Computer* > *Properties* > *the Advanced* tab.

4 Click the *Environment Variables* button.

5 If they exist, delete the following variables:

- ESEC_HOME
- ESEC_VERSION
- ESEC_JAVA_HOME
- ESEC_CONF_FILE
- WORKBENCH_HOME

6 Remove any entries in the PATH environment variable that point to the Sentinel installation.

7 Delete all Sentinel shortcuts from the desktop.

8 Delete the shortcut *Start* > *Programs* > *Sentinel* folder from the *Start* menu.

9 Restart the machine.

Updating the Sentinel 6.1 Rapid Deployment Hostname

A

A.1 Server

On the Sentinel™ server, hostname changes are automatically updated during run time or during the installation. If the server does not properly function after a hostname update, you must manually verify the following:

- All `jnlp` files and the `configuration.xml` file are updated on Sentinel restart.
- The hostname entry in the `sentinel_host` database table is updated.
- All references to the local loop (localhost or 127.0.0.1) in the `install_home/config/configuration.xml` file remain unaffected.

A.2 Client Applications

For the client applications, you must manually change the server hostname or IP address at the following locations to point to the correct server:

- `install_home/config/configuration.xml`.

  The Sentinel Control Center and the Solution Designer use this information.
- The help URL given in the `install_home/config/SentinelPreferences.properties` file.
- Run the following command to update the hostname in the `sdm.connect` file:

  ```
  sdm -action saveConnection -server <postgresql> -host <hostIpaddress/
  hostName> -port <portnum> -database <databaseName/SID> [-driverProps
  <propertiesFile] {-user <dbUser> -password <dbPass> | -winAuth} -
  connectFile <filenameToSaveConnection>
  ```

Troubleshooting Tips

B

This section gives you a list of troubleshooting suggestions that can help you resolve some of the Sentinel 6.1 Rapid Deployment installation issues.

B.1 Database Authentication Fails on Entering Invalid Credentials

Common Cause: Database authentication fails if an invalid LDAP server hostname or IP address is entered while configuring Sentinel 6.1 Rapid Deployment server for LDAP authentication.

Action: Ensure that a valid LDAP server hostname or IP address is entered.

B.2 Sentinel Web Interface Fails to Start Up

Common Cause: You have installed Sentinel 6.1 Rapid Deployment on a machine where an Identity Audit process is either running, or its uninstall is incomplete.

Action: Sentinel 6.1 Rapid Deployment and Novell® Identity Audit cannot be installed on a same machine. Before you install Sentinel 6.1 Rapid Deployment on the machine where Identity Audit is installed, ensure that you uninstall Identity Audit completely.

If the Identity Audit processes are not completely stopped, the Identity Audit uninstall cannot be completed successfully. In this case, there are chances for conflicts either in installing Sentinel 6.1 Rapid Deployment or in starting its applications.

1. Run the following command to shut down the Identity Audit services:

   ```
   /etc/init.d/identity_audit stop
   ```

2. Run the following command to ensure that all the Identity Audit have stopped working:

   ```
   ps -ef | grep novell
   ```

3. Stop any remaining processes manually if necessary.

   ```
   kill -9 pid
   ```

4. Uninstall Identity Audit with necessary `root` permissions.

   For more information, see Identity Audit Guide (http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/).

B.3 Remote Collector Manager Throws Exception on Windows 2008 When UAC is Enabled

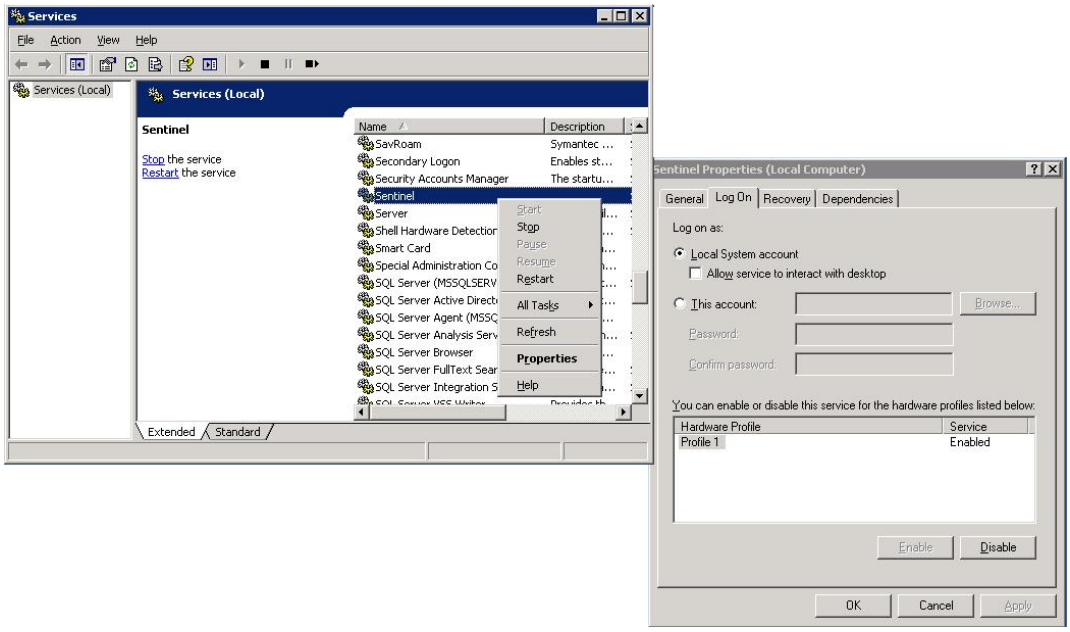
Problem: Log in as any user who belongs to the Administrator group. Execute the `setup.bat` command in a terminal prompt to install the collector Manager. Restart the system or start the Collector Manager services manually, then log in with the same user credentials. You can observe an exceptions in the Collector Manager log, `collector_manager0.0.log` which impacts the following Collector Manager functionalities:

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

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

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

1. Run `services.msc` to open the *Services* window.
2. Right-click Sentinel, then select *Properties*.



3. In the Sentinel Properties window, select the *Log On* tab.
4. Select *This Account*, then provide the credentials for the current user that you have used to install the Collector Manager.

Documentation Updates

C

This section contains information about documentation content changes made to the *Installation Guide for Novell Sentinel 6.1 Rapid Deployment*. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date that appears on title page to determine the release date of this guide. For the most recent version of the *Novell Sentinel 6.1 Rapid Deployment Installation Guide*, see the Novell Sentinel 6.1 Rapid Deployment documentation Web site (http://www.novell.com/documentation/sentinel61rd/).

In this section, content changes appear in reverse chronological order, according to the publication date. Within a dated entry, changes are grouped and sequenced, according to where they appear in the document itself. Each change entry provides a link to the related topic and a brief description of the change.

This document was updated on the following dates:

C.1 November 2009

Updates were made to the following section. The changes are explained below:

Table C-1 *Updates*

Location	Changes
Section 3.4, “Virtualization,” on page 26	Added support statement for virtualization on Sentinel 6.1 Rapid Deployment.
Section 4.9, “LDAP Authentication,” on page 42	Added information on LDAP authentication.

C.2 August 2009

Updates were made to the following section. The changes are explained below:

Table C-2 *Updates*

Location	Changes
Entire Book	Organizational and editorial changes were made in all the sections.

Location	Changes
Section 3.3, “Hardware Requirements,” on page 24	Updated the section with the latest test matrix available in the Sentinel twiki. Fixed the following bugs: ◆ Defect#518925 (http://bugzilla.novell.com/show_bug.cgi?id=518925) ◆ Defect#519934 (https://bugzilla.novell.com/show_bug.cgi?id=519934)
Chapter 4, “Installing Sentinel 6.1 Rapid Deployment,” on page 27	Added a new section on configuring Sentinel for LDAP authentication. Updated the sections for technical accuracy. Fixed Defect#516084 (https://bugzilla.novell.com/show_bug.cgi?id=516084) Fixed Defect#530507 (https://bugzilla.novell.com/show_bug.cgi?id=530507)
Chapter 5, “Security Considerations for Sentinel 6.1 Rapid Deployment,” on page 47	Updated the following sections for technical accuracy: ◆ Section 5.2.1, “Operating System Users,” on page 49 ◆ Section 5.2.2, “Sentinel Application and Database Users,” on page 50 ◆ Section 5.3, “Securing Sentinel Data,” on page 51 ◆ Section 5.4, “Backing Up Information,” on page 54
Chapter 7, “Testing the Sentinel 6.1 Rapid Deployment Installation,” on page 59	Updated Section 7.1, “Testing the Rapid Deployment Installation,” on page 59 to fix the Defect #518495 (http://bugzilla.novell.com/show_bug.cgi?id=518495).
Chapter 6, “Advisor Configuration,” on page 57	Updated the sections for technical accuracy.
Appendix A, “Updating the Sentinel 6.1 Rapid Deployment Hostname,” on page 75	Updated the section for technical accuracy.