

Installation Guide

Novell® Sentinel 6.1 Rapid Deployment

SP2

May 2011

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 \(http://www.novell.com/info/exports/\)](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.

Copyright © 1999-2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the [Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	9
1 Product Overview	11
1.1 Sentinel 6.1 Rapid Deployment Overview	11
1.2 Sentinel 6.1 Rapid Deployment Configuration	12
1.3 Sentinel Rapid Deployment User Interfaces	13
1.3.1 Sentinel 6.1 Rapid Deployment Web Interface	13
1.3.2 Sentinel Control Center	14
1.3.3 Sentinel Data Manager	14
1.3.4 Sentinel Solution Designer	14
1.3.5 Sentinel Plug-In SDK	15
1.4 Sentinel Server Components	15
1.4.1 Data Access Service	15
1.4.2 Message Bus	15
1.4.3 Sentinel Database	15
1.4.4 Sentinel Collector Manager	16
1.4.5 Correlation Engine	16
1.4.6 iTRAC	16
1.4.7 Sentinel Advisor and Exploit Detection	16
1.4.8 Web Server	16
1.5 Sentinel Plug-Ins	16
1.5.1 Collectors	17
1.5.2 Connectors and Integrators	17
1.5.3 Correlation Rules and Actions	18
1.5.4 Reports	18
1.5.5 iTRAC Workflows	18
1.5.6 Solution Packs	18
1.6 Language Support	18
2 System Requirements	19
2.1 Supported Platforms	19
2.1.1 Supported Operating Systems	19
2.2 Hardware Requirements	20
2.3 Supported Web Browsers	22
2.4 Virtual Environment	22
2.5 Recommended Limits	22
2.5.1 Collector Manager Limits	23
2.5.2 Reports Limits	23
2.6 Test Results	23
3 Installation	27
3.1 Overview	27
3.1.1 Server Components	27
3.1.2 Client Applications	28
3.2 Installation on SUSE Linux Enterprise Server	28
3.2.1 Prerequisites	29
3.2.2 Installing Sentinel Rapid Deployment	30

3.3	Installing the Collector Manager and Client Applications	34
3.3.1	Downloading the Installers.	35
3.3.2	Port Numbers for Sentinel Rapid Deployment Client Components	35
3.3.3	Installing the Sentinel Client Applications	36
3.3.4	Installing the Sentinel Collector Manager on SLES or Windows	38
3.4	Manually Starting and Stopping the Sentinel Services	40
3.5	Post-Installation Configuration	41
3.5.1	Changing the Date and Time Settings.	41
3.5.2	Configuring an SMTP Integrator to Send Sentinel Notifications	41
3.5.3	Collector Manager Services.	42
3.5.4	Managing Time	42
3.6	LDAP Authentication	43
3.6.1	Overview	43
3.6.2	Prerequisites	43
3.6.3	Configuring the Sentinel Server for LDAP Authentication	44
3.6.4	Configuring Multiple LDAP Servers for Failover	47
3.6.5	Configuring LDAP Authentication for Multiple Active Directory Domains	49
3.6.6	Logging in by Using LDAP User Credentials.	50
3.7	Updating the License Key from an Evaluation Key to a Production Key	50
4	Upgrading Sentinel Rapid Deployment	51
4.1	Prerequisites	51
4.2	Installing the Patch on the Server	51
4.3	Upgrading the Collector Manager and Client Applications	52
4.3.1	Upgrading the Collector Manager	52
4.3.2	Upgrading the Client Applications	53
5	Security Considerations for Sentinel Rapid Deployment	55
5.1	Hardening.	55
5.1.1	Out-of-the-Box Hardening	55
5.1.2	Securing Sentinel Rapid Deployment Data	56
5.2	Securing Communication across the Network	56
5.2.1	Communication between Sentinel Server Processes	56
5.2.2	Communication between the Sentinel Server and Sentinel Client Applications	56
5.2.3	Communication between the Server and the Database	57
5.2.4	Communication between the Collector Managers and Event Sources	57
5.2.5	Communication with Web Browsers	58
5.2.6	Communication between the Database and Other Clients	58
5.3	Securing Users and Passwords.	58
5.3.1	Operating System Users	58
5.3.2	Sentinel Application and Database Users	59
5.3.3	Enforcing a Password Policy for Users	59
5.4	Securing Sentinel Data	60
5.5	Backing Up Information	63
5.6	Securing the Operating System.	64
5.7	Viewing Sentinel Audit Events	64
5.8	Using a CA Certificate	65
6	Testing the Functionalities of Sentinel Rapid Deployment	67
6.1	Testing the Rapid Deployment Installation.	67
6.2	Cleaning Up after Testing	77
6.3	Using Real Data.	78

7	Uninstalling Sentinel Rapid Deployment	79
7.1	Uninstalling the Sentinel Rapid Deployment Server.	79
7.2	Uninstalling the Remote Collector Manager and Sentinel Client Applications	79
7.2.1	Linux	79
7.2.2	Windows	80
7.2.3	Post-Uninstallation Procedures	80
A	Updating the Sentinel Rapid Deployment Hostname	83
A.1	Server.	83
A.2	Client Applications	83
B	Troubleshooting Tips	85
B.1	Database Authentication Fails on Entering Invalid Credentials	85
B.2	Sentinel Web Interface Fails to Start Up	85
B.3	Remote Collector Manager Throws Exception on Windows 2008 When UAC is Enabled . . .	86
B.4	UUID Does Not Get Created for Imaged Collector Managers	87
C	Best Practices for Maintaining PostgreSQL Database	89
C.1	Modifying the Memory Configuration Parameters	89
C.2	Reducing the I/O Impact of Vacuum/Analyze	90

About This Guide

The purpose of this guide is to provide an introduction to Novell Sentinel 6.1 Rapid Deployment Service Pack 2 and to describe the installation procedures.

- ♦ Chapter 1, “Product Overview,” on page 11
- ♦ Chapter 2, “System Requirements,” on page 19
- ♦ Chapter 3, “Installation,” on page 27
- ♦ Chapter 4, “Upgrading Sentinel Rapid Deployment,” on page 51
- ♦ Chapter 5, “Security Considerations for Sentinel Rapid Deployment,” on page 55
- ♦ Chapter 6, “Testing the Functionalities of Sentinel Rapid Deployment,” on page 67
- ♦ Chapter 7, “Uninstalling Sentinel Rapid Deployment,” on page 79
- ♦ Appendix A, “Updating the Sentinel Rapid Deployment Hostname,” on page 83
- ♦ Appendix B, “Troubleshooting Tips,” on page 85
- ♦ Appendix C, “Best Practices for Maintaining PostgreSQL Database,” on page 89

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 Rapid Deployment Installation Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html)
- ♦ *Novell Sentinel Rapid Deployment User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html)
- ♦ *Novell Sentinel Rapid Deployment Reference Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/bookinfo.html)
- ♦ *Novell Sentinel Installation Guide* (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/)
- ♦ *Novell Sentinel User Guide* (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/)
- ♦ *Novell Sentinel Reference Guide* (http://www.novell.com/documentation/sentinel61/s61_reference/?page=/documentation/sentinel61/s61_reference/data/)

- ♦ *Sentinel SDK* (http://www.novell.com/developer/develop_to_sentinel.html)

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

Contacting Novell

- ♦ *Novell Web site* (<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>)
- ♦ *Sentinel Community Support Forums* (<http://forums.novell.com/novell-product-support-forums/sentinel/>)
- ♦ *Sentinel Plug-in Web site* (<http://support.novell.com/products/sentinel/secure/sentinelplugins.html>)
- ♦ *Notification E-mail List*: Sign up through the Sentinel Plug-in Web site

Product Overview

1

Sentinel 6.1 Rapid Deployment is a simplified version of Novell Sentinel that leverages the open source PostgreSQL, activeMQ, and JasperReports components.

The following sections help you understand the major components of the Sentinel 6.1 Rapid Deployment system. This *Sentinel Rapid Deployment Installation Guide* has detailed information about installation and configuration procedures. The *Sentinel Rapid Deployment User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) has detailed architecture, operation, and administrative procedures.

- ♦ Section 1.1, “Sentinel 6.1 Rapid Deployment Overview,” on page 11
- ♦ Section 1.2, “Sentinel 6.1 Rapid Deployment Configuration,” on page 12
- ♦ Section 1.3, “Sentinel Rapid Deployment User Interfaces,” on page 13
- ♦ Section 1.4, “Sentinel Server Components,” on page 15
- ♦ Section 1.5, “Sentinel Plug-Ins,” on page 16
- ♦ Section 1.6, “Language Support,” on page 18

1.1 Sentinel 6.1 Rapid Deployment Overview

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

Sentinel automates the 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 also 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 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.

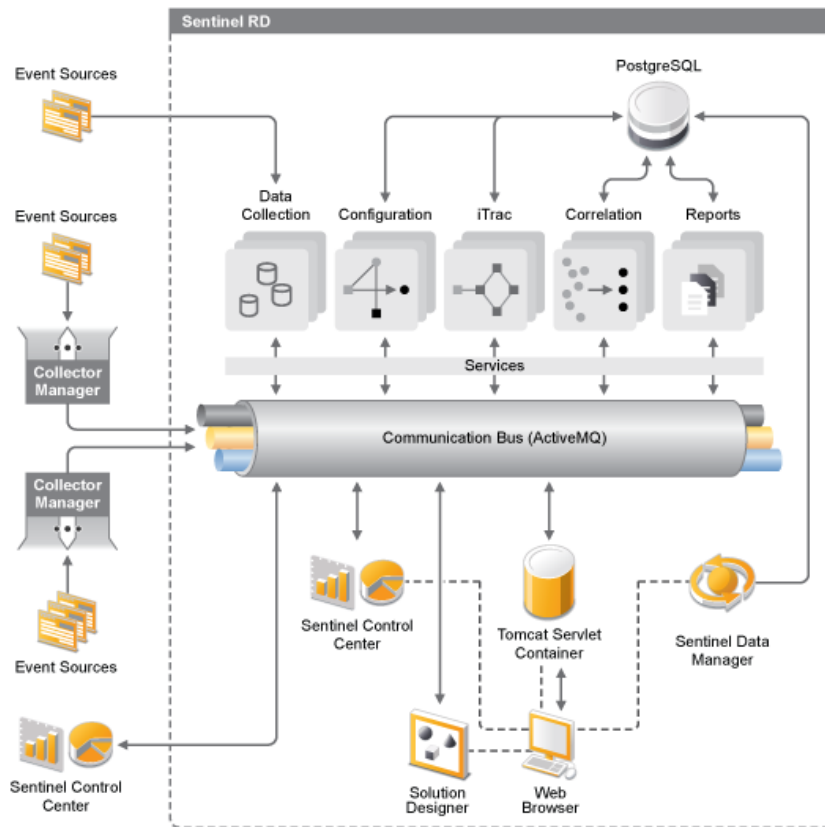
With Sentinel Rapid Deployment, you get:

- ♦ Integrated, automated real-time security management and compliance monitoring across all systems and networks.

- ◆ A framework that enables business policies to drive IT policies and actions.
- ◆ 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, and FISMA. 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 Rapid Deployment, which shows the components involved in performing security and compliance management.

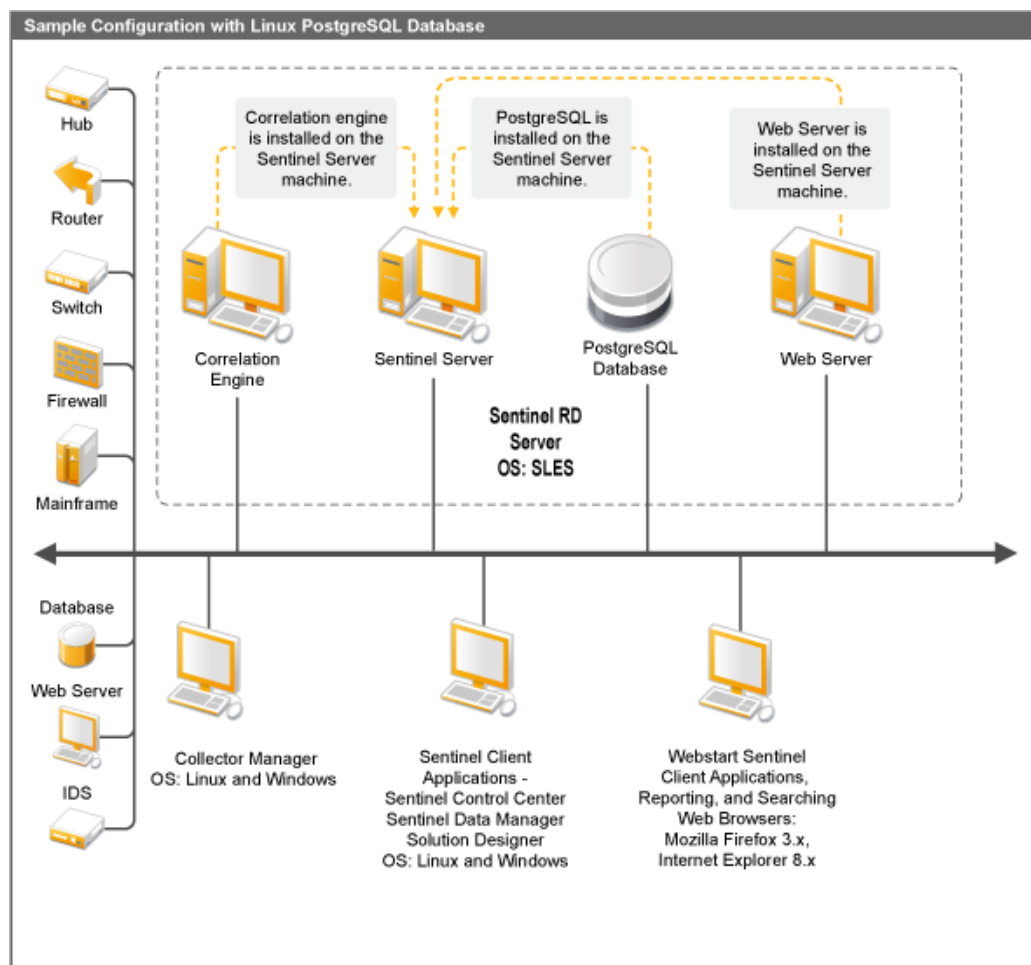
Figure 1-1 Conceptual Architecture of Sentinel



1.2 Sentinel 6.1 Rapid Deployment Configuration

The following illustration shows the configuration setup for Sentinel 6.1 Rapid Deployment.

Figure 1-2 Sentinel 6.1 Rapid Deployment Configuration



1.3 Sentinel Rapid Deployment User Interfaces

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

- ◆ [Sentinel 6.1 Rapid Deployment Web Interface](#)
- ◆ [Sentinel Control Center](#)
- ◆ [Sentinel Data Manager](#)
- ◆ [Sentinel Solution Designer](#)
- ◆ [Sentinel Plug-In SDK](#)

1.3.1 Sentinel 6.1 Rapid Deployment Web Interface

With the Novell Sentinel 6.1 Rapid Deployment Web interface, you can manage reports and launch the Sentinel Control Center (SCC), the Sentinel Data Manager, and the Solution Designer. You can also download the Collector Manager installer and the Client installer from the *Applications* page of the Sentinel 6.1 Rapid Deployment Web interface.

For more information, see “[Managing Sentinel Rapid Deployment Through the Web Interface](#)” in the *Sentinel Rapid Deployment User Guide*.

1.3.2 Sentinel Control Center

The 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.

The key features of the SCC include:

- ◆ **Active Views:** Provides real-time analytics and visualization
- ◆ **Analysis:** Runs and saves offline queries
- ◆ **Incidents:** Provides incident creation and management
- ◆ **Correlation:** Provides correlation rules definition and management
- ◆ **iTRAC:** Provides process management for documenting, enforcing, and tracking incident resolution processes
- ◆ **Reporting:** Provides historical reports and metrics
- ◆ **Event Source Management:** Provides collector deployment and monitoring
- ◆ **Solution Manager:** Installs, implements, and tests the Solution Pack contents

For more information, see “[Sentinel Control Center](#)” in the *Sentinel Rapid Deployment User Guide*.

1.3.3 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 Rapid Deployment User Guide*.

1.3.4 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 workflows, and reports.

Sentinel content is the extended functionality of the Sentinel system. This content includes 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 Packs](#)” in the *Sentinel Rapid Deployment User Guide*.

1.3.5 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 that you can use to develop your own projects. For more information, see the [Sentinel SDK \(http://www.novell.com/developer/develop_to_sentinel.html\)](http://www.novell.com/developer/develop_to_sentinel.html).

1.4 Sentinel Server Components

Sentinel is made up of the following components:

- ♦ [Section 1.4.1, “Data Access Service,” on page 15](#)
- ♦ [Section 1.4.2, “Message Bus,” on page 15](#)
- ♦ [Section 1.4.3, “Sentinel Database,” on page 15](#)
- ♦ [Section 1.4.4, “Sentinel Collector Manager,” on page 16](#)
- ♦ [Section 1.4.5, “Correlation Engine,” on page 16](#)
- ♦ [Section 1.4.6, “iTRAC,” on page 16](#)
- ♦ [Section 1.4.7, “Sentinel Advisor and Exploit Detection,” on page 16](#)
- ♦ [Section 1.4.8, “Web Server,” on page 16](#)

1.4.1 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 “[Data Access Service](#)” in the *Sentinel Rapid Deployment Reference Guide*.

1.4.2 Message Bus

Sentinel 6.1 Rapid Deployment uses an open source message broker called Apache Active MQ. The message bus is capable of moving thousands of message packets in a second, between the components of Sentinel. Apache Active MQ architecture is built around the Java Message Oriented Middleware (JMOM), which 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 Rapid Deployment User Guide*

1.4.3 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 Rapid Deployment User Guide*.

1.4.4 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 “[Collector Manager](#)” in the *Sentinel Rapid Deployment User Guide*.

1.4.5 Correlation Engine

The Correlation Engine 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 Rapid Deployment User Guide*.

1.4.6 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 Rapid Deployment User Guide*.

1.4.7 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, provides 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 the 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 Rapid Deployment User Guide*.

1.4.8 Web Server

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

1.5 Sentinel Plug-Ins

Sentinel supports a variety of plug-ins to expand and enhance system functionality. Some of these plug-ins are preinstalled. Additional plug-ins (and updates) are available for download at the [Sentinel 6.1 Plug-ins Web site \(http://support.novell.com/products/sentinel/secure/sentinelplugins.html\)](http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

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

- ◆ [Section 1.5.1, “Collectors,” on page 17](#)
- ◆ [Section 1.5.2, “Connectors and Integrators,” on page 17](#)
- ◆ [Section 1.5.3, “Correlation Rules and Actions,” on page 18](#)
- ◆ [Section 1.5.4, “Reports,” on page 18](#)
- ◆ [Section 1.5.5, “iTRAC Workflows,” on page 18](#)
- ◆ [Section 1.5.6, “Solution Packs,” on page 18](#)

1.5.1 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 following types of devices and more:

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

JavaScript Collectors can be written by using the standard JavaScript development tools and the Collector SDK.

1.5.2 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 Rapid Deployment User Guide*.

1.5.3 Correlation Rules and Actions

Correlation rules identify important patterns in the event stream. When a correlation rule is triggered, 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 Rapid Deployment User Guide*.

1.5.4 Reports

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

1.5.5 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 Rapid Deployment User Guide*.

1.5.6 Solution Packs

Solution Packs are packaged sets of related Sentinel content, such as correlation rules, actions, iTRAC workflows, and reports. Novell provides Solution Packs that focus on specific business needs, such as the PCI-DSS Solution Pack, which addresses compliance with the Payment Card Industry Data Security Standard. 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 Rapid Deployment User Guide*.

1.6 Language Support

Sentinel components are available in the following languages:

- ◆ Czech
- ◆ English
- ◆ French
- ◆ German
- ◆ Italian
- ◆ Japanese
- ◆ Dutch
- ◆ Polish
- ◆ Portuguese
- ◆ Simplified Chinese
- ◆ Spanish
- ◆ Traditional Chinese

System Requirements

2

For best performance and reliability, you must install the Sentinel Rapid Deployment components on approved software and hardware, as listed in this section. The requirements mentioned in this section have been fully quality assured and certified.

- ◆ [Section 2.1, “Supported Platforms,” on page 19](#)
- ◆ [Section 2.2, “Hardware Requirements,” on page 20](#)
- ◆ [Section 2.3, “Supported Web Browsers,” on page 22](#)
- ◆ [Section 2.4, “Virtual Environment,” on page 22](#)
- ◆ [Section 2.5, “Recommended Limits,” on page 22](#)
- ◆ [Section 2.6, “Test Results,” on page 23](#)

2.1 Supported Platforms

[Table 2-1](#) lists the combinations of software and operating system that are certified or supported by Novell. Certified combinations have been tested with Novell Engineering’s full test suite. Supported combinations are expected to be fully functional.

2.1.1 Supported Operating Systems

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

The Sentinel Rapid Deployment server components include the Communication Server, Correlation Engine, Data Access Service (DAS), Web server, and the Advisor data subscription service.

The Sentinel client applications include Sentinel Control Center (SCC), Sentinel Data Manager (SDM), and Sentinel Solution Designer (SSD).

The Collector Manager has specific platform requirements.

Table 2-1 *Supported and Certified Operating Systems*

Platforms	Server Components	Sentinel Client Applications	Collector Manager
SUSE Linux Enterprise Server (SLES) 11 SP1 (64-bit)	Certified	Certified	Certified
SUSE Linux Enterprise Server (SLES) 11 SP1 (32-bit)	Not Supported	Supported	Supported
SUSE Linux Enterprise Server (SLES) 10 SP3 (64-bit)	Certified	Supported	Supported

Platforms	Server Components	Sentinel Client Applications	Collector Manager
SUSE Linux Enterprise Server (SLES) 10 SP3 (32-bit)	Supported	Supported	Supported
Windows Server 2008 R2 (64-bit)	Not Supported	Certified	Certified
Windows Server 2003 R2 (64-bit)	Not Supported	Supported	Supported
Windows Server 2003 R2 (32-bit)	Not Supported	Supported	Supported
Windows XP SP3 (32-bit)	Not Supported	Supported	Not Supported
Windows Vista SP2 (32-bit)	Not Supported	Supported	Not Supported
Windows 7	Not Supported	Certified	Not Supported

Follow these guidelines for optimal performance, stability, and reliability:

- ♦ For SLES, the operating system for the Sentinel Rapid Deployment server machine must include at least the Base Server and X Window components of SLES.
- ♦ For the Sentinel Rapid Deployment server, use the ext3 file system. For more information on file systems, see [Overview of File Systems in Linux \(http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html\)](http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) in the *Storage Administration Guide*.

NOTE:

- ♦ Sentinel Rapid Deployment is not supported on the Open Enterprise Server installs of SLES.
 - ♦ The 32-bit demo version of the Sentinel 6.1 Rapid Deployment server 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 6.1 Rapid Deployment support can receive limited support on this platform from Novell Technical Support for issues that 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.
-

2.2 Hardware Requirements

The Sentinel Rapid Deployment server components run on x86-64 (64-bit) hardware, with some exceptions based on operating system, as described in the [Section 2.1.1, “Supported Operating Systems,” on page 19](#). 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. 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 events per second (EPS) range.
- ♦ The average event size is 1 KB.
- ♦ 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 2-2 on page 21](#) and [Table 2-3 on page 22](#).
- ◆ The Sentinel Server has a default 5 GB of disk space for temporarily caching event data that cannot be immediately inserted into the database.
- ◆ The Sentinel Server also has a default 5 GB of disk space for events that cannot be immediately inserted into the aggregation event files.
- ◆ The optional Advisor subscription requires an additional 1GB 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.

In SLES version, the database is embedded with the Sentinel Rapid Deployment server and is installed on the same machine along with the server.

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 2-2 *Single Machine Configuration (up to 2000 eps)*

Components	RAM	Space	CPU
Machine 1: Sentinel Rapid Deployment Server	16 GB	1 TB, SAS (15K rpm) Hard Disk(s)	Dell PowerEdge 2900, 2 x Quad-Core Intel Xeon E5310 (1.6 GHz) with Gigabit Ethernet NIC
◆ Embedded PostgreSQL database (3 GB)			
◆ Collector Manager (1228 MB)		Hardware	
◆ DAS_Core (1579 MB)		RAID 10	
◆ DAS_Binary (1404 MB)			
◆ Correlation Engine (1073 MB)			
◆ 4 Collectors (Generic, Cisco, Snort, and IBM generating 500 eps each)			
◆ 10 Correlation Rules Deployed			
◆ 10 unique Active Views			
◆ 3 simultaneous users			
◆ 2 Maps Deployed			

Table 2-3 Three Machine Configuration (up to 5000 eps)

Components	RAM	Space	CPU
Machine 1: Sentinel Rapid Deployment Server <ul style="list-style-type: none">◆ Embedded PostgreSQL database (3 GB)◆ Collector Manager (1228 MB)◆ DAS_Core (1579 MB)◆ DAS_Binary (1404 MB)◆ Correlation Engine (1073 MB)◆ 4 Collectors (generating 500 eps each, 1500 EPS from remote Collector Manager 1, and 1500 EPS from remote Collector Manager 2.	16 GB	1 TB, SAS (15K rpm) Hard Disk(s) Hardware RAID 10	Dell PowerEdge 2900, 2 x Quad-Core Intel Xeon E5310 (1.6 GHz) with Gigabit Ethernet NIC
Machine 2: Collector Manager <ul style="list-style-type: none">◆ Collector Manager/Collectors◆ 3 Collectors (generating 500 eps each)	4 GB	300 GB, SATA (3 Gbit/s) Hard Disk	Intel Core 2 Duo E6750 (2.66 GHz) with Gigabit Ethernet NIC
Machine 3: Collector Manager <ul style="list-style-type: none">◆ Collector Manager/Collectors◆ 3 Collectors (generating 500 eps each)	4 GB	300 GB, SATA (3 Gbit/s) Hard Disk	Intel Core 2 Duo E6750 (2.66 GHz) with Gigabit Ethernet NIC

2.3 Supported Web Browsers

- ◆ Mozilla Firefox 3.x
- ◆ Internet Explorer 8.x

2.4 Virtual Environment

Sentinel Rapid Deployment has been extensively tested on VMWare ESX Server and Novell fully supports Sentinel 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, CPUs, disk space, and I/O as the physical machine recommendations.

For information on physical machine recommendations for a SLES system, see [Section 2.2, “Hardware Requirements,”](#) on page 20

2.5 Recommended Limits

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

- ◆ [Section 2.5.1, “Collector Manager Limits,”](#) on page 23
- ◆ [Section 2.5.2, “Reports Limits,”](#) on page 23

2.5.1 Collector Manager Limits

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

Table 2-4 *Collector Manager Performance Numbers*

Attribute	Limit	Comments
Maximum number of Collector Managers	20	This limit assumes each Collector Manager is running at low EPS (e.g, less than 100 EPS). The limit decreases as the events per second increase.
Maximum number of Connectors (fully utilized) on a single Collector Manager	1 per CPU core, with at least 1 CPU core reserved for the operating system and other processing	A fully utilized Connector is one that is running at the highest EPS possible for that type of Connector.
Maximum number of Collectors (fully utilized) on a single Collector Manager	1 per CPU core, with at least 1 CPU core reserved for the operating system and other processing	A fully utilized Collector is one that is running at the highest EPS possible for that type of Collector.
Maximum number of devices on a single Collector Manager	2000	The limit of the Sentinel Rapid Deployment server is also 2000, so if 2000 devices are on a single Collector Manager, then the limit of devices for the overall Sentinel system has been reached with that single Collector Manager.
Maximum number of devices on the Sentinel Rapid Deployment server	2000	The limit of devices on the Sentinel Rapid Deployment server is 2000.

2.5.2 Reports Limits

Table 2-5 *Reports Performance Numbers*

Attribute	Limit	Comments
Maximum number of saved reports	200	This limit might increase or decrease depending on the size of the reports and disk space available on the server that is not being used by the rest of the system.
Maximum number of reports running simultaneously	3	The limit assumes that the server is not already highly utilized performing data collection or other tasks.

2.6 Test Results

Sentinel Rapid Deployment provides the ability to have different configurations depending on the needs of the environment. The following performance testing information is the result of Novell's testing for specific configurations listed in the tables below.

The hardware recommendations for a Sentinel implementation can vary according to each implementation; therefore, we recommend that you consult Novell Consulting Services or any of the Novell Sentinel partner prior to finalizing the Sentinel architecture. The test information below can be used as a guideline.

Linux testing was performed to scale the maximum EPS with a different number of devices and to scale the maximum number of devices for a specific EPS. The following hardware configuration was used:

- ◆ **Number of CPU Cores:** 4
- ◆ **CPU Model:** Intel Xeon CPU X5770 @ 2.93 GHz
- ◆ **RAM:** 16 GB
- ◆ **Hard Disk Size (+RAID type and number of disks in RAID):** 1.7 TB (RAID 5, 6 disks)

NOTE: All testing was done with syslog-based event sources. Other connectors might offer different performance.

The following table shows the maximum EPS you can scale with a different number of devices on a SLES system:

Table 2-6 *Maximum EPS on a SLES System*

System Setup	Devices	Maximum EPS
4 Collector Managers (one local and three remote) with 10 Collectors, each generating 500 EPS	25	5,000
4 Collector Managers (one local and three remote) with 10 Collectors, each generating 500 EPS	100	5,000
4 Collector Managers (one local and three remote) with 10 Collectors, each generating 500 EPS	1,000	5,000

The following table shows the maximum devices you can scale at different EPS rates on a SLES system:

Table 2-7 *Maximum Devices on a SLES System*

System Setup	EPS	Maximum Devices
1 Collector Manager with 1 Collector generating 500 EPS	500	2,000
1 Collector Manager with 2 Collectors generating 500 EPS each	1,000	2,000
1 Collector Manager with 3 Collectors, each generating 500 EPS	1,500	2,000

NOTE:

- ◆ If you want to scale more EPS or devices, install additional Collector Managers.
 - ◆ The maximum device limits are not hard limits, but are recommendations based on the performance testing done by Novell. They assume a low average events rate per second per device (less than 3 EPS). Higher EPS rates result in lower sustainable maximum devices. You can use the equation (maximum devices) x (average EPS per device) = maximum event rate to arrive at the approximate limits for your specific average EPS rate or number of devices, as long as the maximum number of devices does not exceed the limit indicated above.
-

This section provides the information on installing Sentinel Rapid Deployment and the client components.

- ◆ [Section 3.1, “Overview,” on page 27](#)
- ◆ [Section 3.2, “Installation on SUSE Linux Enterprise Server,” on page 28](#)
- ◆ [Section 3.3, “Installing the Collector Manager and Client Applications,” on page 34](#)
- ◆ [Section 3.4, “Manually Starting and Stopping the Sentinel Services,” on page 40](#)
- ◆ [Section 3.5, “Post-Installation Configuration,” on page 41](#)
- ◆ [Section 3.6, “LDAP Authentication,” on page 43](#)
- ◆ [Section 3.7, “Updating the License Key from an Evaluation Key to a Production Key,” on page 50](#)

3.1 Overview

The Sentinel installation package provides you with a simplified single-machine server installer to install everything you need to run Sentinel Rapid Deployment. The Sentinel Rapid Deployment server installer installs the following components:

- ◆ [Section 3.1.1, “Server Components,” on page 27](#)
- ◆ [Section 3.1.2, “Client Applications,” on page 28](#)

3.1.1 Server Components

Table 3-1 Sentinel Server Components and Applications

Component	Description
	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 to immediately indicate increased risk to an organization.
Data Access Service	Includes data storage, query, display, and processing components.
Web Server	Supports the Web interface for Sentinel Rapid Deployment.

Component	Description
Collector Manager	<p>A service that handles connections to event sources, data parsing, mapping, and so on.</p> <p>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 Rapid Deployment Web interface. For example, you can install an additional Collector Manager on a Windows machine to collect Windows events.</p>
iTRAC	<p>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.</p>

3.1.2 Client Applications

The client applications—the Sentinel Control Center, the Sentinel Data Manager, and the Solution Designer are installed by default on the Sentinel Rapid Deployment server. You can launch the client applications by using any of the following methods:

- ◆ By using the Sentinel Rapid Deployment Web interface. The client systems should have Java 1.6.0_20 or later installed and the JRE path should be set to launch the Sentinel applications through Webstart.

Set the `JAVA_HOME` environment variable to point to the location of the `JRE 6` folder. Set the export path to point to the `bin` folder under the `JRE 6` location.

- ◆ By using the `<install_directory>/bin` as a user who owns the Sentinel Rapid Deployment installation files. For example:

```
./bin/<client_application>.sh
```

Table 3-2 *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.
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.

3.2 Installation on SUSE Linux Enterprise Server

- ◆ [Section 3.2.1, “Prerequisites,” on page 29](#)
- ◆ [Section 3.2.2, “Installing Sentinel Rapid Deployment,” on page 30](#)

3.2.1 Prerequisites

Ensure that you have met the following prerequisites before installing Sentinel Rapid Deployment. For more information about these prerequisites (including the list of certified platforms), see [Chapter 2, “System Requirements,” on page 19](#).

- ♦ “Server” on page 29
- ♦ “Client” on page 29
- ♦ “Advisor” on page 30

IMPORTANT: Sentinel Rapid Deployment installations using the full installer should always take place on a clean system. If you have other versions of Sentinel, such as Sentinel Classic or Sentinel Log Manager previously installed on any of the machines, you must first uninstall them. For information on uninstalling previous versions of Sentinel, see the relevant Installation guides:

- ♦ For uninstalling Sentinel Classic, see the “Uninstalling Sentinel” chapter in the [Sentinel Installation Guide](http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html) (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html).
 - ♦ For uninstalling Sentinel Log Manager, see the “Uninstalling Sentinel Log Manager” chapter in the [Sentinel Log Manager 1.1 Installation Guide](http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html) (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html).
-

Server

- ♦ Ensure that each server machine meets the minimum system requirements. For more information on the system requirements, see [Chapter 2, “System Requirements,” on page 19](#).
- ♦ Configure the operating system in such a way that the `hostname -f` command returns a valid hostname.
- ♦ Install and configure an SMTP server if you want to be able to send mail notifications from the Sentinel system.

Client

- ♦ Ensure that each client machine meets the minimum system requirements. For more information about these prerequisites, see [Chapter 2, “System Requirements,” on page 19](#).
- ♦ Ensure that you create a directory whose name has only ASCII characters (and no special characters) from which to run the installer.
- ♦ When you install remote Collector Manager or client applications on Linux 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 the 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.

Advisor

If you want to install the Advisor, you must purchase the Sentinel Exploit Detection and Advisor Data Subscription. After you have purchased the subscription, use your Novell eLogin to download and update the Advisor data. For more information, see “[Advisor Usage and Maintenance](#)” chapter in the *Sentinel Rapid Deployment User Guide*.

3.2.2 Installing Sentinel Rapid Deployment

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

- ♦ “[Single Script Installation with Root Privileges](#)” on page 30
- ♦ “[Non-root Installation](#)” on page 32

The Sentinel Rapid Deployment installer script provides the following options during installation:

- ♦ **-all:** You must be the `root` user to use this option. This option creates a user (default: `novell`), user group, (default: `novell`), and then installs the Sentinel Rapid Deployment server. It also runs the Sentinel Rapid Deployment services automatically on system startup.
- ♦ **-install:** This option only installs the Sentinel Rapid Deployment server.
- ♦ **-createuser:** You must be the `root` user to use this option. This option only creates the user (default: `novell`), and the user group (default: `novell`).
- ♦ **-createservice:** You must be the `root` user to use this option. This option only enables the Sentinel Rapid Deployment services to run automatically on system startup.
- ♦ **-help:** This option displays help on how to use the install script options.

Single Script Installation with Root Privileges

- 1 Log in as the `root` user.
- 2 Download the `sentinel6_rd_linux_x86-64.tar.gz` installer from the [Novell download site \(http://download.novell.com/\)](http://download.novell.com/) to a temporary directory.
- 3 Extract the installer:

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

IMPORTANT: Ensure that the non-root user (for example, `novell`) which gets created in [Step 6](#) is able to access the directory where the installer is extracted.

- 4 Change to the directory where you extracted the installer:

```
cd sentinel6_rd_linux_x86-64
```
- 5 Run the `install.sh` script with the `-all` option:

```
./install.sh -all
```

The install script first checks for the available memory and disk space. If the available memory is less than one GB, the script automatically terminates the installation. If the available memory is more than one GB but less than four GB, the script displays a message that you have less memory than is recommended. It also asks whether you want to proceed with the installation. Enter `y` if you want to continue with the installation, or enter `n` if you do not want to proceed.

- 6** Specify the username, or press Enter to select the default username. The default username is `novell`.

If the specified username already exists, the installer displays a message that the user exists and lists the user's group. Proceed with [Step 8](#).

If the specified username does not exist, the installer creates the username. Proceed with [Step 7](#).

- 7** Specify the group name or press Enter to select the default group name. The default group name is `novell`.

If the specified group name already exists, the installer continues with the installation. If the specified group name does not exist, the installer creates the group and displays a message that the specified username is created under the specified group.

The specified user and the group own the installation and the running processes of the Sentinel.

- 8** Specify the install path or press Enter to select the default path. The default path is `/opt/novell`.

The install path that you specify should be without space. If there is space, the install script prompts you to provide the install path without the space.

- 9** Choose one of the following languages by entering the corresponding number:

Serial Number	Language
1	Czech
2	English
3	French
4	German
5	Italian
6	Japanese
7	Dutch
8	Polish
9	Portuguese
10	Simplified Chinese
11	Spanish
12	Traditional Chinese

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

- 10** Read the End User License Agreement, then enter 1 if you agree with the license agreement and want to continue the installation. If you want to exit the installation, enter 2.

The installer then starts extracting the files and prompts you for the license.

- 11 Enter 1 to use the 90-day evaluation license key or enter 2 to use the valid license key.
If you enter 2, the installer prompts you to enter the valid Sentinel RD license key. If the license key that you specified is not valid, the installer prompts you to specify the valid license key again. If the specified license key is not valid on the second attempt, the 90-day evaluation license key is automatically installed. You can enter the valid license later.
The script then loads either the trial license or the valid license.
- 12 Specify a password for the `dbauser` user and confirm it by specifying it again.
The `dbauser` credentials are used to create tables and partitions in the PostgreSQL database.
- 13 Specify a password for the `admin` user and confirm it by specifying it again.
When you are prompted to specify passwords for `admin` and `dbauser` users, do not use the backslash (`\`) and apostrophe (`'`) characters in the password because the PostgreSQL database does not allow these characters.
The install script installs the PostgreSQL database, creates tables and partitions, and then install the Sentinel Rapid Deployment server.

After installation, you can:

- ♦ Launch the Sentinel Rapid Deployment Web interface by going to `https://<SERVER_IP>:8443/sentinel`. `<SERVER_IP>` is the IP address of the machine where Sentinel Rapid Deployment is installed.
- ♦ Launch the Sentinel Control Center by running `<install_directory>/bin/control_center.sh` as the user created in [Step 6](#).

Non-root Installation

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

- 1 Log in to the server where you want to install Sentinel Rapid Deployment.
- 2 Download the `sentinel6_rd_linux_x86-64.tar.gz` installer from the [Novell download site \(http://download.novell.com/\)](http://download.novell.com/) to a temporary directory.
- 3 Extract the installer:

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

IMPORTANT: Ensure that the non-root user (for example, `novell`) which gets created in [Step 7](#) is able to access the directory where the installer is extracted.

- 4 Log in as the `root` user.
- 5 Change to the directory where you extracted the installer:

```
cd sentinel6_rd_linux_x86-64
```
- 6 Run the `install.sh` script with `-createuser` option:

```
./install.sh -createuser
```
- 7 Specify the username, or press Enter to select the default username. The default username is `novell`.

If the specified username already exists, the installer displays a message that the user exists and lists the user's group. Proceed with [Step 9](#).

If the specified username does not exist, the installer creates the username. Proceed with [Step 8](#).

- 8** Specify the group name or press Enter to select the default group name. The default group name is novell.

If the specified group name already exists, the installer continues with the installation. If the specified group name does not exist, the installer creates the group and displays a message that the specified username is created under the specified group.

The specified user and the group own the installation and the running processes of the Sentinel.

- 9** Specify the install path or press Enter to select the default path. The default path is /opt/novell.

The install path that you specify should be without space. If there is space, the install script prompts you to provide the install path without the space.

- 10** Log in as the non-root user. For example.

```
su - novell
```

- 11** Run the installation script with the `-install` option:

```
./install.sh -install
```

The install script first checks for the available memory and disk space. If the available memory is less than one GB, the script automatically terminates the installation. If the available memory is more than one GB but less than four GB, the script displays a message that you have less memory than is recommended. It also asks whether you want to proceed with the installation. Enter `y` if you want to continue with the installation, or enter `n` if you do not want to proceed.

- 12** Specify the install path or press Enter to select the default path. The default path is /opt/novell.

The install path that you specify should be without space. If there is a space, the install script prompts you to provide the install path without the space.

- 13** Choose one of the following languages by entering the corresponding number:

Serial Number	Language
1	Czech
2	English
3	French
4	German
5	Italian
6	Japanese
7	Dutch
8	Polish
9	Portuguese
10	Simplified Chinese

Serial Number	Language
11	Spanish
12	Traditional Chinese

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

- 14** Read the End User License Agreement, then enter 1 if you agree with the license agreement and want to continue the installation. If you want to exit the installation, enter 2.

The installer then starts extracting the files and prompts you for the license.

- 15** Enter 1 to use the 90-day evaluation license key or enter 2 to use the valid license key.

If you enter 2, the installer prompts you to enter the valid Sentinel RD license key. If the license key that you specified is not valid, the installer prompts you to specify the valid license key again. If the specified license key is not valid on the second attempt, the 90-day evaluation license key is automatically installed. You can enter the valid license later.

The script then loads either the trial license or the valid license.

- 16** Specify a password for the `dbauser` user and confirm it by specifying it again.

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

- 17** Specify a password for the `admin` user and confirm it by specifying it again.

When you are prompted to specify passwords for the `admin` and `dbauser` users, do not use the backslash (`\`) and apostrophe (`'`) characters in the password because the PostgreSQL database does not allow these characters.

- 18** (Conditional) When the installation is complete, if you want to run the Sentinel Rapid Deployment services automatically on system startup, run the `install.sh` script with the `-createservice` option as the root user:

```
./install.sh -createservice
```

After installation, you can:

- ♦ Launch the Sentinel Rapid Deployment Web interface by going to `https://<SERVER_IP>:8443/sentinel`. `<SERVER_IP>` is the IP address of the machine where Sentinel Rapid Deployment is installed.
- ♦ Launch the Sentinel Control Center by running `<install_directory>/bin/control_center.sh` as the user created in [Step 7](#) above.

3.3 Installing the Collector Manager and Client Applications

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

- ♦ [Section 3.3.1, “Downloading the Installers,”](#) on page 35
- ♦ [Section 3.3.2, “Port Numbers for Sentinel Rapid Deployment Client Components,”](#) on page 35
- ♦ [Section 3.3.3, “Installing the Sentinel Client Applications,”](#) on page 36
- ♦ [Section 3.3.4, “Installing the Sentinel Collector Manager on SLES or Windows,”](#) on page 38

3.3.1 Downloading the Installers

- 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. 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 Rapid Deployment 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 installers:

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

For more information on installing the Collector Manager, see [Section 3.3.4, “Installing the Sentinel Collector Manager on SLES or Windows,” on page 38](#) and for installing Client installer, see [Section 3.3.3, “Installing the Sentinel Client Applications,” on page 36](#).

3.3.2 Port Numbers for Sentinel Rapid Deployment Client Components

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

Table 3-3 *Compatible Port Numbers for Sentinel Rapid Deployment Components*

Port Number	Description
61616	The remote Collector Managers use this port number to connect to the Sentinel Rapid Deployment server via ActiveMQ.
10013	The Sentinel Control Center uses this port number to connect to the Sentinel Rapid Deployment server via a proxy.

Port Number	Description
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 Rapid Deployment server.

3.3.3 Installing the Sentinel Client Applications

You can install Sentinel client application either on Linux or Windows system. To install the client applications:

- 1 Browse to the folder where you have downloaded the client installer.
- 2 Extract the install script from the file:

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

- 3 Go to the install directory and start the installation:

Platform	Action
Windows	Run <code>disk1\setup.bat</code> NOTE: On a Windows Vista machine, launch the command prompt by using the <i>Run as Administrator</i> option from the right-click menu options.
Linux	<ul style="list-style-type: none"> ♦ GUI mode: <code><install_directory>/disk1/setup.sh</code> ♦ Console mode: <code><install_directory>/disk1/setup.sh -console</code>

The steps listed below are only for GUI mode.

- 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 you instal Sentinel Rapid Deployment on Windows x86-64, the default path is C:\Program Files (x86). You must change this default path to avoid the special characters like the parentheses in (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 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.

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

10 Specify the user name or press Enter to select the default user name. The default user name is `esecadm`.

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.

11 Specify the user home directory or press Enter to select the default directory. The default directory is `/export/home`.

If the username is `esecadm`, the corresponding home directory is `/export/home/esecadm`.

12 Specify the password for the user to log in as the `esecadm` user if you have selected the default user name in [Step 10](#). Otherwise, set the password for the user that you have created in [Step 10](#).

13 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 address or hostname where the Sentinel Rapid Deployment server is installed.

Ensure that the port numbers are the same as on the Sentinel Rapid Deployment server at `<install_directory>/config/configuration.xml` to enable communications. Make a note of these ports for future installations on other machines. For more information on port numbers, see [Section 3.3.2, “Port Numbers for Sentinel Rapid Deployment Client Components,”](#) on page 35.

14 Click *Next*.

A summary of the installation is displayed.

15 Click *Install*.

16 Click *Finish* to complete the 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 the `root` user:

```
env | grep ESEC_USER
```

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

3.3.4 Installing the Sentinel Collector Manager on SLES or Windows

The Sentinel Collector Manager installer is available for download on the Applications page of the Sentinel Rapid Deployment Web interface. To install the Collector Manager:

- 1 Browse to the folder where you have downloaded the Collector Manager installer.
- 2 Extract the install script from the file:

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

- 3 Go to the `disk1` directory and start the installation:

Platform	Action
Windows	Run the following command: <pre>disk1\setup.bat</pre>
Linux	<ul style="list-style-type: none">♦ GUI mode: <code><install_directory>/disk1/setup.sh</code>♦ Console mode: <code><install_directory>/disk1/setup.sh -console</code>

- 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 you install 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 the parentheses in (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 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.
- ♦ **Communication Server hostname:** The machine IP or hostname where the Sentinel 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** Click *Next*.

- 11** Specify the following information:

- ♦ **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.

- 12** Click *Next*.

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

- 13** Click *Install*.

- 14** After the installation finishes, 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 `<install_directory>/config/activemqusers.properties` file on the Sentinel server.

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

```
collectormanager=cefc76062c58e2835aa3d777778f9295
```

`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.

After the installation finishes, you are prompted to reboot or to log in again and start the Sentinel services manually.

15 Click *Finish* to reboot your system.

16 Log in again, using the username you specified in [Step 8](#).

If you forget the username, 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.

NOTE: There are a few issues with Collector Manager installation on the Windows 2008 platform, and also on Imaged Collector Managers. For information on troubleshooting these issues, see [Appendix B, “Troubleshooting Tips,” on page 85](#).

3.4 Manually Starting and Stopping the Sentinel Services

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

Platform	Command
Linux	<code><install_directory>/bin/sentinel.sh start</code>
Windows	<code><install_directory>/bin/sentinel.bat start</code>

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

Platform	Command
Linux	<code><install_directory>/bin/sentinel.sh stop</code>
Windows	<code><install_directory>/bin/sentinel.bat stop</code>

You can also use the following command to start or stop the Sentinel services.

```
/etc/init.d/sentinel.sh stop|start
```


3.5 Post-Installation Configuration

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

- ♦ [Section 3.5.1, “Changing the Date and Time Settings,” on page 41](#)
- ♦ [Section 3.5.2, “Configuring an SMTP Integrator to Send Sentinel Notifications,” on page 41](#)
- ♦ [Section 3.5.3, “Collector Manager Services,” on page 42](#)
- ♦ [Section 3.5.4, “Managing Time,” on page 42](#)

3.5.1 Changing the Date and Time Settings

The default date and time format in the Sentinel Control Center can be overridden. For more information about customizing the date and time format to your local time zone, see the [Java Web site \(http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html\)](http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html).

- 1 Edit the `SentinelPreferences.properties` file.

```
<install_directory>/config/SentinelPreferences.properties
```

- 2 Remove the comment from the following line and customize the date and time format for Sentinel Control Center event date/time fields:

```
com.eSecurity.Sentinel.event.datetimetypeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
```

3.5.2 Configuring an SMTP Integrator to Send Sentinel Notifications

In Sentinel 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 SMTP Integrator must be configured with valid connection information before it works. For more information, see [“Sending an E-mail”](#) in the *Sentinel Rapid Deployment User Guide*.

A single action instance of the SendEmail action plug-in is created automatically in every Sentinel installation. No configuration is necessary to the SendEmail action except the recipients of the mail message and the message contents are configured in the action parameters.

This SendEmail action is triggered internally by Sentinel to send mail in the following situations:

- ♦ When a Correlation rule is generated, a SendEmail action is triggered. This SendEmail action 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).
- ♦ When a workflow includes a Mail Step or Activity that is configured to send email.
- ♦ When a user opens an incident and selects to execute an Activity that is configured to send email.
- ♦ When a user right-clicks an event and selects *Email*.
- ♦ When a user opens an incident and selects *Email Incident*.

3.5.3 Collector Manager Services

- ♦ [“Installing Additional Collector Manager” on page 42](#)
- ♦ [“Using the Generic Collector” on page 42](#)

Installing Additional Collector Manager

Collector Managers 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:

- ♦ They allow distributed event parsing and processing to improve system performance.
- ♦ They 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.
- ♦ They 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.
- ♦ They 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. You can install additional Collector Manager by running the installer on a new machine. For more information on installing Collector Manager, see [Section 3.3.4, “Installing the Sentinel Collector Manager on SLES or Windows,” on page 38](#).

Using the Generic Collector

During the installation of the Sentinel Rapid Deployment Server, a Collector called the Generic Collector is configured. By default, it creates events at the rate of 5 events per second (eps).

If you want any additional collectors for your system, you can download them from the [Novell Web site \(http://support.novell.com/products/sentinel/collectors.html\)](http://support.novell.com/products/sentinel/collectors.html).

3.5.4 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.

3.6 LDAP Authentication

Sentinel Rapid Deployment supports LDAP authentication in addition to database authentication. You can enable users to log in to Sentinel Rapid Deployment by using their Novell eDirectory or Microsoft Active Directory credentials by configuring a Sentinel Rapid Deployment server for LDAP authentication.

- ◆ [Section 3.6.1, “Overview,” on page 43](#)
- ◆ [Section 3.6.2, “Prerequisites,” on page 43](#)
- ◆ [Section 3.6.3, “Configuring the Sentinel Server for LDAP Authentication,” on page 44](#)
- ◆ [Section 3.6.4, “Configuring Multiple LDAP Servers for Failover,” on page 47](#)
- ◆ [Section 3.6.5, “Configuring LDAP Authentication for Multiple Active Directory Domains,” on page 49](#)
- ◆ [Section 3.6.6, “Logging in by Using LDAP User Credentials,” on page 50](#)

3.6.1 Overview

You can configure the Sentinel Rapid Deployment server for LDAP authentication over a secure SSL connection with or without using anonymous searches on the LDAP directory.

NOTE: If anonymous search is disabled on the LDAP directory, you must not configure the Sentinel Rapid Deployment server to use anonymous search.

- ◆ **Anonymous Search:** When you create Sentinel Rapid Deployment LDAP user accounts, you must specify the directory username, but you do not need to specify the user distinguished name (DN).

When the LDAP user logs in to Sentinel Rapid Deployment, the Sentinel Rapid Deployment server performs an anonymous search on the LDAP directory based on the specified username, finds the corresponding DN, then authenticates the user login against the LDAP directory by using the DN.

- ◆ **Non-Anonymous Search:** When you create Sentinel Rapid Deployment LDAP user accounts, you must specify both the directory username and the user DN.

When the LDAP user logs in to the Sentinel Rapid Deployment, the Sentinel Rapid Deployment server authenticates the user login against the LDAP directory by using the specified user DN and does not perform any anonymous search on the LDAP directory.

There is an additional approach applicable only for Active Directory. For more information, see [Non-Anonymous LDAP Authentication by Using the UserPrincipalName attribute in Active Directory](#).

3.6.2 Prerequisites

- ◆ [“Exporting the LDAP Server CA Certificate” on page 44](#)
- ◆ [“Enabling Anonymous Search in the LDAP Directory” on page 44](#)

Exporting the LDAP Server CA Certificate

The secure SSL connection to the LDAP server requires the LDAP server CA certificate that you must export to a Base64-encoded file.

- ♦ **eDirectory:** See [Exporting an Organizational CA's Self-Signed Certificate \(http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html\)](http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html).

To export an eDirectory CA certificate in iManager, the Novell Certificate Server plug-ins for iManager must be installed.

- ♦ **Active Directory:** See [How to enable LDAP over SSL with a third-party certification authority \(http://support.microsoft.com/kb/321051\)](http://support.microsoft.com/kb/321051).

Enabling Anonymous Search in the LDAP Directory

To perform LDAP authentication by using anonymous search, you must enable anonymous search in the LDAP directory. By default, anonymous search is enabled in eDirectory and is disabled in Active Directory.

To enable anonymous search in the LDAP directory, refer the following:

- ♦ **eDirectory:** See `ldapBindRestrictions` in section [Attributes on the LDAP Server Object \(http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html\)](http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html).
- ♦ **Active Directory:** The ANONYMOUS LOGON user object must be given appropriate list permission and read access to `sAMAccountName` and `objectclass` attributes. For more information, see [Configuring Active Directory to Allow Anonymous Queries \(http://support.microsoft.com/kb/320528\)](http://support.microsoft.com/kb/320528).

For Windows Server 2003, you must perform additional configuration. For more information, see [Configuring Active Directory on Windows Server 2003 \(http://support.microsoft.com/kb/326690/en-us\)](http://support.microsoft.com/kb/326690/en-us).

3.6.3 Configuring the Sentinel Server for LDAP Authentication

- 1 Make sure you have met the prerequisites in [Section 3.6.2, "Prerequisites," on page 43](#).
- 2 Log in to the Sentinel Rapid Deployment server as the `root` user.
- 3 Copy the exported LDAP server CA certificate file to the `<install_directory>/config` directory.
- 4 Set the ownership and permissions of the certificate file as follows:

```
chown novell:novell <install_directory>/config/<cert-file>
```

```
chmod 700 <install_directory>/config/<cert-file>
```

- 5 Switch to the `novell` user:

```
su - novell
```
- 6 Change to the `<install_directory>/bin` directory.
- 7 Run the LDAP authentication configuration script:

```
./ldap_auth_config.sh
```

The script takes a backup of the `auth.login` and `configuration.xml` configuration files in the `config` directory as `auth.login.sav` and `configuration.xml.sav` before modifying them for LDAP authentication.

8 Specify the following information:

Press Enter to accept the default value or specify a new value to override the default.

- ◆ **Sentinel install location:** The installation directory on the Sentinel server.
- ◆ **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`. However, you should not install the LDAP server on the same machine as the Sentinel server.
- ◆ **LDAP server port:** The port number for a secure LDAP connection. The default port number is `636`.
- ◆ **Anonymous searches on LDAP directory:** Specify `y` to perform anonymous searches. Otherwise, specify `n`. The default value is `y`.

If you specify `n`, complete the LDAP configuration and perform the steps mentioned in the section “[LDAP Authentication Without Performing Anonymous Searches](#)” on page 46.

- ◆ **LDAP Directory used:** This parameter is displayed only if you have specified ‘`y`’ for anonymous searches. Specify `1` for Novell eDirectory or `2` for Active Directory. The default value is `1`.
- ◆ **LDAP subtree to search for users:** This parameter is displayed only if you have specified ‘`y`’ for anonymous searches. 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=TESTAD,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 3](#).

9 Enter one of the following:

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

On successful configuration:

- ◆ The LDAP server certificate is added to a keystore named `<install_directory>/config/ldap_server.keystore`.
- ◆ The `auth.login` and `configuration.xml` configuration files in the `<install_directory>/config` directory are updated to enable LDAP authentication.

10 Enter `y` to restart the Sentinel service.

IMPORTANT: If there are any errors, revert the changes made to the `auth.login` and `configuration.xml` configuration files in the `config` directory:

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

- 11 (Conditional) If you specified `n` for [Anonymous searches on LDAP directory:](#), continue with [“LDAP Authentication Without Performing Anonymous Searches”](#) on page 46.

LDAP Authentication Without Performing Anonymous Searches

While configuring the Sentinel Rapid Deployment for LDAP Authentication, if you have specified `n` for Anonymous searches on LDAP directory, then the LDAP authentication does not perform anonymous search.

When you create the LDAP user account by using the Sentinel Control Center, ensure that you specify *LDAP user DN* for non-anonymous LDAP authentication. You can use this approach for both eDirectory and Active Directory.

For more information, see [“Creating an LDAP User Account for Sentinel”](#) in the *Sentinel Rapid Deployment User Guide*.

Additionally, for Active Directory, there is an alternative approach to perform LDAP authentication without anonymous searches. For more information, see [Non-Anonymous LDAP Authentication by Using the UserPrincipalName attribute in Active Directory](#).

Non-Anonymous LDAP Authentication by Using the UserPrincipalName attribute in Active Directory

For Active Directory, you can also perform LDAP authentication without anonymous searches by using the `userPrincipalName` attribute:

- 1 Ensure that the `userPrincipalName` attribute is set to `<sAMAccountName@domain>` for the Active Directory user.
For more information, see [User-Principal-Name Attribute \(http://msdn.microsoft.com/en-us/library/ms680857\(VS.85\).aspx\)](http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx).
- 2 Ensure that you have performed [Step 1 on page 44](#) through [Step 10 on page 45](#), and ensure that you specified `n` for [“Anonymous searches on LDAP directory:”](#) on page 45.
- 3 On the Sentinel server, edit the `LdapLogin` section in the `<Install Directory>/config/auth.login` file:

```
LdapLogin {
  com.sun.security.auth.module.LdapLoginModule required
  userProvider="ldap://LDAP server IP:636/DN of the Container that contains
the user objects"
  authIdentity="{USERNAME}@Domain Name"
  userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
  useSSL=true;
};
```

For example:

```
LdapLogin {
  com.sun.security.auth.module.LdapLoginModule required
  userProvider="ldap://137.65.151.12:636/DC=Test-
AD,DC=provo,DC=novell,DC=com"
  authIdentity="{USERNAME}@Test-AD.provo.novell.com"
  userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
  useSSL=true;
};
```

4 Restart the Sentinel service:

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

3.6.4 Configuring Multiple LDAP Servers for Failover

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

1 Ensure that you have followed [Step 2 on page 44](#) through [Step 10 on page 45](#) to configure the Sentinel server for LDAP authentication against the primary LDAP server.

2 Log in to the Sentinel server as the novell user.

3 Stop the Sentinel service.

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

4 Change to the `<install_directory>/config` directory:

```
cd <install_directory>/config
```

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

```
vi auth.login
```

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

For example:

```
userProvider="ldap://ldap-url1 ldap://ldap-url2"
```

For Active Directory, ensure that the subtree in the LDAP URL is not blank.

For more information on specifying multiple LDAP URLs, see the description of the `userProvider` option in [Class LdapLogin Module \(http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html\)](http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

7 Save the changes.

8 Export the certificate of each failover LDAP server and copy the certificate file to the `<install_directory>/config` directory on the Sentinel server.

For more information, see [“Exporting the LDAP Server CA Certificate” on page 44](#).

9 Ensure that you set the necessary ownership and permissions of the certificate file for each failover LDAP server.

```
chown novell:novell <install_directory>/config/<cert-file>
chmod 700 <install_directory>/config/<cert-file>
```

10 Add each failover LDAP server certificate to the keystore `ldap_server.keystore` that is created in [Step 8](#) in section [“Configuring the Sentinel Server for LDAP Authentication” on page 44](#).

```
<install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
-file <certificate-file> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

Replace *<certificate-file>* with the LDAP certificate filename in Base64-encoded format and replace *<alias_name>* with 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. When you import multiple certificates into the keystore without specifying an alias, the keytool reports an error that the alias already exists.

11 Start the Sentinel service.

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

The service might not connect to the failover LDAP server if the Sentinel server times out before it finds that the primary LDAP server is down. To ensure that the Sentinel server connects to the failover LDAP server without timing out:

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

2 Open the `sysctl.conf` file for editing:

```
vi /etc/sysctl.conf
```

3 Ensure that the `net.ipv4.tcp_syn_retries` value is set to 3. If the entry does not exist, add the entry. Save the file:

```
net.ipv4.tcp_syn_retries = 3
```

4 Execute the command for the changes to take effect:

```
/sbin/sysctl -p
/sbin/sysctl -w net.ipv4.route.flush=1
```

5 Set the Sentinel server timeout value by adding the `-Desecurity.remote.timeout=60` parameter in `control_center.sh` and `solution_designer.sh` in the `<install_directory>/bin` directory:

control_center.sh:

```
"<install_directory>/jre/bin/java" $MEMORY -
Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
Desecurity.cache.directory="<install_directory>/data/
control_center.cache" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
control_center_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Dice.pilots.html4.baseFontFamily="Arial Unicode MS" -
Desecurity.remote.timeout=60 -jar ../lib/console.jar
```


solution_designer.sh:

```
"<install_directory>/jre/bin/java" -classpath $LOCAL_CLASSPATH $MEMORY -
Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
Dsentinel.installer.jar.location="<install_directory>/lib/
contentinstaller.jar" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
solution_designer_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -Desecurity.cache.directory=../
data/solution_designer.cache -Desecurity.remote.timeout=60
com.esecurity.content.exportUI.ContentPackBuilder
```

3.6.5 Configuring LDAP Authentication for Multiple Active Directory Domains

If the LDAP users to be authenticated are in multiple Active Directory domains, you can configure the Sentinel Rapid Deployment server for LDAP authentication as follows:

- 1 Ensure that you have followed [Step 2 on page 44](#) through [Step 10 on page 45](#) to configure the Sentinel server for LDAP authentication against the Active Directory domain controller of the first domain. Also ensure that you specified `n` for “[Anonymous searches on LDAP directory:](#)” on [page 45](#).

- 2 Log in to the Sentinel server as the `novell` user.

- 3 Stop the Sentinel service.

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

- 4 Change to the `<install_directory>/config` directory:

```
cd <install_directory>/config
```

- 5 Open the `auth.login` file for editing.

```
vi auth.login
```

- 6 Edit the `LdapLogin` section to specify multiple LDAP URLs separating each URL by a blank space.

For example:

```
LdapLogin {
    com.sun.security.auth.module.LdapLoginModule required
    userProvider="ldap://<IP of the domain 1 domain controller>:636
ldap://<IP of the domain 2 domain controller>:636"
    authIdentity="{USERNAME}"
    useSSL=true;
};
```

For more information on specifying multiple LDAP URLs, see the description of the `userProvider` option in [Class LdapLogin Module \(http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html\)](http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

- 7 Save the changes.

- 8 Export the certificate of the domain controller of each domain and copy the certificate files to the `<install_directory>/config` directory on the Sentinel server.

For more information, see “[Exporting the LDAP Server CA Certificate](#)” on [page 44](#).

- 9 Ensure that you set the necessary ownership and permissions of the certificate files.

```
chown novell:novell <install_directory>/config/<cert-file>
chmod 700 <install_directory>/config/<cert-file>
```

- 10 Add each certificate to the keystore `ldap_server.keystore` that is created in [Step 8](#) in section “[Configuring the Sentinel Server for LDAP Authentication](#)” on page 44.

```
<install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
-file <certificate-file> -alias <alias_name> -keystore
ldap_server.keystore -storepass sentinel
```

Replace `<certificate-file>` with the LDAP certificate filename in Base64-encoded format and replace `<alias_name>` with 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. When you import multiple certificates into the keystore without specifying an alias, the keytool reports an error that the alias already exists.

- 11 Start the Sentinel service.

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

3.6.6 Logging in by Using LDAP User Credentials

After you successfully configure the Sentinel server for LDAP authentication, you can create Sentinel LDAP user accounts in Sentinel Control Center. For more information on creating LDAP user accounts, see “[Creating an LDAP User Account for Sentinel](#)” in the *Sentinel Rapid Deployment User Guide*.

After you create the LDAP user account, you can log in to the Sentinel Rapid Deployment Web user interface, Sentinel Control Center, and Sentinel Solution Designer by using your LDAP username and password.

NOTE: To modify an existing LDAP configuration, run the `ldap_auth_config` script again and specify the new values for the parameters.

3.7 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 the license key to avoid re-installation:

- 1 Log in to the machine where Sentinel Rapid Deployment is installed as the Sentinel Administrator operating system user (the default user is `novell`).
- 2 At the command prompt, change directory to the `<install_directory>/bin`.
- 3 Enter the following command:

```
./softwarekey.sh
```
- 4 Specify 1 to set the primary key. Press Enter.
- 5 Enter the new valid license key and follow the on-screen instructions to exit after updating the license key.

Upgrading Sentinel Rapid Deployment

4

This section provides information on upgrading an existing version of Sentinel Rapid Deployment to the latest patch.

NOTE: This patch is applicable only for a 64-bit installation of Sentinel Rapid Deployment. Applying this patch on a 32-bit demo system results in a non-functional installation.

- ♦ [Section 4.1, “Prerequisites,” on page 51](#)
- ♦ [Section 4.2, “Installing the Patch on the Server,” on page 51](#)
- ♦ [Section 4.3, “Upgrading the Collector Manager and Client Applications,” on page 52](#)

4.1 Prerequisites

- ♦ Ensure that the system that you upgrade has Sentinel 6.1 Rapid Deployment SP1 already installed.
- ♦ Ensure that Sentinel Data Manager jobs are enabled so that the Online Current partition never reaches P_MAX. If it reaches P_MAX and if you add partitions manually, Sentinel Control Center does not launch successfully.

4.2 Installing the Patch on the Server

- 1 As a `novell` user log in to the server where you want to install the patch.

Before installing the patch, ensure that you back up the Sentinel database, config folder, and data folder by using the following commands:

Sentinel database:

```
tar -cf backup.tar <install_directory>/3rdparty/postgresql/database_files
tar -cf backupdata.tar <install_directory>/3rdparty/postgresql/data
```

config folder:

```
tar -cf backupconfig.tar <install_directory>/config
```

data folder:

```
tar -cf backupdata.tar <install_directory>/data
```

For more information on these commands, see [File system level back up \(http://www.postgresql.org/docs/8.1/static/backup-file.html\)](http://www.postgresql.org/docs/8.1/static/backup-file.html) on the PostgreSQL Web site.

- 2 Back up the Event Source Management (ESM) configuration and create an ESM export.
For more information, see “[Exporting a Configuration](#)” in the *Sentinel Rapid Deployment User Guide*.
- 3 Download the patch installer for Sentinel Rapid Deployment from the [Novell Patch Finder \(http://download.novell.com/patch/finder/\)](http://download.novell.com/patch/finder/).
- 4 Copy the downloaded installer package to a temporary directory.

5 Stop the Sentinel services:

```
sentinel.sh stop
```

6 Specify the following command to extract the files in the installer package:

```
unzip <install_filename>
```

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

7 Change to the directory where you extracted the installer files:

```
cd <directory_name>
```

Replace *<directory_name>* with the actual name of the directory where the files were extracted.

8 Specify the following command to patch the server, then follow the on-screen instructions:

```
./service_pack.sh
```

After the installation, the Sentinel services start automatically.

9 Apply the patch on all the machines where Collector Manager or Client Applications, or both, are running.

4.3 Upgrading the Collector Manager and Client Applications

- ♦ [Section 4.3.1, “Upgrading the Collector Manager,” on page 52](#)
- ♦ [Section 4.3.2, “Upgrading the Client Applications,” on page 53](#)

4.3.1 Upgrading the Collector Manager

- ♦ [“Linux” on page 52](#)
- ♦ [“Windows” on page 53](#)

Linux

1 Log in to the Sentinel Rapid Deployment Collector Manager machine as the `root` user.

2 Download the patch installer for Sentinel Rapid Deployment from the [Novell Patch Finder](http://download.novell.com/patch/finder/) (<http://download.novell.com/patch/finder/>).

3 Copy the downloaded installer file to a temporary directory.

4 Specify the following command to extract the files in the installer zip package:

```
unzip <install_filename>
```

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

5 Change to the directory where you extracted the installer files:

```
cd <directory_name>
```

Replace *<directory_name>* with the actual name of the directory where the installer files were extracted.

6 Stop the Collector Manager services.

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

7 Run the service pack installer, then follow the on-screen instructions:

```
./service_pack.sh
```

After the installation, Collector Manager services start automatically.

Windows

- 1 Log in to the Sentinel Rapid Deployment Collector Manager machine as an admin user.
- 2 Download the patch installer for Sentinel Rapid Deployment from the [Novell Patch Finder](http://download.novell.com/patch/finder/) (<http://download.novell.com/patch/finder/>).
- 3 Copy the installer file to a temporary directory.
- 4 Extract the files in the installer package.
- 5 Stop the Collector Manager services.

```
<install_directory>\bin\sentinel.bat stop
```

- 6 Navigate to the directory where you extracted the installer files.
- 7 Do one of the following to run the installer:
 - ♦ Double-click the `service_pack.bat` file, then follow the on-screen instructions.
 - ♦ From a command prompt, run the `service_pack.bat` file, then follow the on-screen instructions.

After the installation, Collector Manager services start automatically.

4.3.2 Upgrading the Client Applications

- ♦ “Linux” on page 53
- ♦ “Windows” on page 53

Linux

- 1 As the `root` user, log in to the machine where Novell Sentinel Rapid Deployment Client applications are running.
- 2 Download the patch installer for Sentinel Rapid Deployment from the [Novell Patch Finder](http://download.novell.com/patch/finder/) (<http://download.novell.com/patch/finder/>).
- 3 Copy the downloaded installer package to a temporary directory.
- 4 Specify the following command to extract the files in the installer package:

```
unzip <install_filename>
```

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

- 5 Change to the directory where you extracted the installer files:

```
cd <directory_name>
```

Replace `<directory_name>` with the actual name of the directory where the files are extracted.

- 6 Run the installer, then follow the on-screen instructions:

```
./service_pack.sh
```

Windows

- 1 Log in as an administrator to the machine where Novell Sentinel Rapid Deployment Client applications are running.

- 2** Download the patch installer for Sentinel Rapid Deployment from the [Novell Patch Finder](http://download.novell.com/patch/finder/) (<http://download.novell.com/patch/finder/>).
- 3** Copy the downloaded installer file to a temporary directory.
- 4** Extract the files in the installer package.
- 5** Navigate to the directory where you extracted the installer files.
- 6** Do one of the following to run the installer:
 - ♦ Double-click the `service_pack.bat` file, then follow the on-screen instructions.
 - ♦ From the command prompt, run the `service_pack.bat` file, then follow the on-screen instructions.

Security Considerations for Sentinel Rapid Deployment

5

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

- ◆ [Section 5.1, “Hardening,” on page 55](#)
- ◆ [Section 5.2, “Securing Communication across the Network,” on page 56](#)
- ◆ [Section 5.3, “Securing Users and Passwords,” on page 58](#)
- ◆ [Section 5.4, “Securing Sentinel Data,” on page 60](#)
- ◆ [Section 5.5, “Backing Up Information,” on page 63](#)
- ◆ [Section 5.6, “Securing the Operating System,” on page 64](#)
- ◆ [Section 5.7, “Viewing Sentinel Audit Events,” on page 64](#)
- ◆ [Section 5.8, “Using a CA Certificate,” on page 65](#)

5.1 Hardening

- ◆ [Section 5.1.1, “Out-of-the-Box Hardening,” on page 55](#)
- ◆ [Section 5.1.2, “Securing Sentinel Rapid Deployment Data,” on page 56](#)

5.1.1 Out-of-the-Box Hardening

- ◆ All unnecessary ports are turned off.
- ◆ Whenever possible, a service port listens only for local connections and does not allow for remote connections.
- ◆ Files are installed with the least privileges so that only a small number of users can read the files.
- ◆ Default passwords are not permitted.
- ◆ Reports against the database run as a user that only has select permissions on the database.
- ◆ All Web interfaces require HTTPS.
- ◆ A vulnerability scan is run against the application and all potential security problems are addressed.
- ◆ All communication over the network uses SSL by default and is configured for authentication.
- ◆ User account passwords are encrypted by default when stored on the file system or in the database.

5.1.2 Securing Sentinel Rapid Deployment Data

Because of the highly sensitive nature of the data in Sentinel Rapid Deployment, you must 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 more information on remote Collector Managers, see “[Section 3.3, “Installing the Collector Manager and Client Applications,” on page 34](#)”.

5.2 Securing Communication across the Network

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

- ♦ [Section 5.2.1, “Communication between Sentinel Server Processes,” on page 56](#)
- ♦ [Section 5.2.2, “Communication between the Sentinel Server and Sentinel Client Applications,” on page 56](#)
- ♦ [Section 5.2.3, “Communication between the Server and the Database,” on page 57](#)
- ♦ [Section 5.2.4, “Communication between the Collector Managers and Event Sources,” on page 57](#)
- ♦ [Section 5.2.5, “Communication with Web Browsers,” on page 58](#)
- ♦ [Section 5.2.6, “Communication between the Database and Other Clients,” on page 58](#)

5.2.1 Communication between Sentinel Server Processes

The 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="failover://(ssl://localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system" />
```

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

5.2.2 Communication between the Sentinel Server and 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, when they are all running as client applications on the server, specify the following information in the `<install_directory>/configuration.xml`:


```

<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystategy.ProxiedCl
ientStrategyFactory">
  <transport type="ssl">
    <ssl host="localhost" keystore="<install_directory>/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_directory>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml` file as follows:

```

<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystategy.ProxiedCl
ientStrategyFactory" >
  <transport type="ssl">
    <ssl host="127.0.0.1" port="10013" keystore="./.novell/sentinel/
.proxyClientKeystore" />
  </transport>
</strategy>

```

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

5.2.3 Communication between the Server and the Database

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

Sentinel Rapid Deployment uses the PostgreSQL driver (`postgresql-<version>.jdbc3.jar`) provided on the [PostgreSQL Download Page \(http://jdbc.postgresql.org/download.html\)](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 data communication, refer to [PostgreSQL Encryption Options \(http://www.postgresql.org/docs/8.1/static/encryption-options.html\)](http://www.postgresql.org/docs/8.1/static/encryption-options.html).

NOTE: Turning encryption on affects the performance of the system. Therefore, database communication is not encrypted by default. However, this is not a security concern because the communication between the database and server happens over the loopback network interface and is not exposed to the open network.

5.2.4 Communication between the Collector Managers and Event Sources

You can configure Sentinel Rapid Deployment to securely collect data from various event sources. However, secured data collection is determined by specific protocols supported by the event source. For example, the Check Point LEA, Syslog, and Audit Connectors can be configured to encrypt their communication with event sources.

For more information on the possible security features that can be enabled, refer to the Connector and event source vendor documentation provided on the [Novell Sentinel Plug-ins Web site \(http://support.novell.com/products/sentinel/secure/sentinelplugins.html\)](http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

5.2.5 Communication with Web Browsers

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

5.2.6 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 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_Directory>/3rdparty/postgresql/data/pg_hba.conf` file:

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

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

5.3 Securing Users and Passwords

- ♦ [Section 5.3.1, “Operating System Users,” on page 58](#)
- ♦ [Section 5.3.2, “Sentinel Application and Database Users,” on page 59](#)
- ♦ [Section 5.3.3, “Enforcing a Password Policy for Users,” on page 59](#)

5.3.1 Operating System Users

- ♦ [“Server Installation” on page 58](#)
- ♦ [“Collector Manager Installation” on page 58](#)

Server Installation

The Sentinel Rapid Deployment server installation creates a system user and a group that owns the installed files within `<install_directory>`. If the user does not exist, it is created and its home directory is set to `<install_directory>`. 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 a user created during installation, you must set a password for the user after installation.

Collector Manager Installation

The system users might vary in their level of security depending on the operating system on which the Collector Manager is installed.

Linux: The installer prompts you to specify the name of the system user who owns 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 during installation 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 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. However, you can have the installer prompt for the user again:

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

Windows: No users are created.

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

5.3.2 Sentinel Application and Database Users

All Sentinel 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 installer creates and configures a PostgreSQL database with the following users:

- ♦ **admin:** The admin user is the administrator user for all Sentinel applications to log in.
- ♦ **dbauser:** The dbauser is created as a superuser who can manage the database. The password for dbauser is set at the time of the installation of the Sentinel Rapid Deployment server. This password is stored in the `<user home directory>/.pgpass`. The system follows the PostgreSQL database password policies. For more information, see [Section 5.3.3, “Enforcing a Password Policy for Users,” on page 59](#).
- ♦ **appuser:** 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 and encrypted in the XML files (`das_core.xml`, `das_binary.xml`, and `advisor_client.xml`) in the `<install_directory>/config` directory. To change the password for the appuser, use the `<install_directory>/bin/dbconfig` utility. For more information, see [“DAS Container Files”](#) in the *Sentinel Rapid Deployment Reference Guide*.

NOTE: There is also a PostgreSQL database user that owns the entire database including system database tables. By default, the PostgreSQL database user is set to `NOLOGIN` so that no one can log in as the PostgreSQL user.

5.3.3 Enforcing a Password Policy for Users

Sentinel Rapid Deployment utilizes standards-based mechanisms to make it easier to enforce password policies.

The installer creates and configures a PostgreSQL database with the following users:

dbauser: The database owner (database administrator user). The password is set during the installation process.

appuser: This is the application user who is used to log in to the database from Sentinel Rapid Deployment. The password is randomly generated during the installation process, and it is intended for internal use only.

admin: The administrator credentials can be used to log in to the Sentinel Rapid Deployment Web interface. The password is set during the installation process.

By default, user passwords are stored within the PostgreSQL database, which is embedded in Sentinel Rapid Deployment. PostgreSQL provides the option to utilize a number of standards-based authentication mechanisms, as described in the [Client Authentication \(http://www.postgresql.org/docs/8.3/static/client-authentication.html\)](http://www.postgresql.org/docs/8.3/static/client-authentication.html) section of the PostgreSQL documentation.

Utilizing these mechanisms affects all user accounts in Sentinel Rapid Deployment, including the users of the Web application and accounts used only by back-end services, such as `dbauser` and `appuser`.

A simpler option is to use an LDAP directory to authenticate Web application users. To enable this option on the Sentinel Rapid Deployment server, see [Section 3.6, “LDAP Authentication,” on page 43](#). This option has no effect on the accounts used by back-end services, which continue to authenticate through PostgreSQL unless you change the PostgreSQL configuration settings.

You can achieve robust Sentinel Rapid Deployment password policy enforcement by using these standards-based mechanisms and the existing mechanisms in your environment such as your LDAP directory.

5.4 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 unauthorized 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">admin</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.ActiveMQStrategyFactory" name="ActiveMQ">
<jms brokerURL="failover://(ssl://localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
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:** evt_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 Rapid Deployment stores both configuration data and event data. This data is stored at the following locations:

Components	Location for Configuration Data	Location for Event Data
Sentinel 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 The 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	The 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 Collector Manager user password used to connect to the message bus.	The 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.

Components	Location for Configuration Data	Location for Event Data
Client Applications	<p>File system (<i>install_directory/config</i>). The client applications do not store any sensitive information in their configuration files.</p> <p>For example, client applications can export the 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.</p>	None

5.5 Backing Up Information

- ♦ You must back up the events regularly. The backup media should be stored in a secure off-site facility.
- ♦ Back up the system data. For more information, see “[Backup and Restore Utility](#)” in the *Sentinel Rapid Deployment User Guide*.
- ♦ 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 the data is backed up.
- ♦ If you transport and store media off-site, 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 Rapid Deployment Reference Guide*.

YaST contains modules for the basic management of X.509 certificates, which mainly involves the creation of CAs, sub-CAs, and their certificates. For more information on how to manage and update certificates, see [Managing X.509 Certification \(http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html\)](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)*.

5.6 Securing the Operating System

- ◆ Sentinel Rapid Deployment is supported on SUSE Linux Enterprise Server (SLES) 10 SP3 or later. For more information on securing a SLES machine, see the [SUSE Linux Enterprise Server 10 documentation \(http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html\)](http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html).
- ◆ Secure access to the Sentinel 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	5556
Used between engine and manager	
internal_router_server and internal_router_client	5558
Used between event router client and server	
Event listener port	35000
configured in <code>config/collector_mgr.properties</code> as "security.agentmanager.event.port"	

NOTE: Ports marked with an asterisk might be different if they were already in use at the time of installation. If they were in use at the time of installation, substitute 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 \(http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html\)](http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html) in the *SLES 10 Administration Guide*.

5.7 Viewing Sentinel Audit Events

Sentinel Rapid Deployment generates audit events for many actions performed by users and also for actions performed internally for system activities. These events can be viewed in Active Views or accessed through a search or report. However, you must have the necessary permissions to view the system events.

For more information, see "System Events for Sentinel" in the *Sentinel Rapid Deployment User Guide*.

5.8 Using a CA Certificate

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 Rapid Deployment Reference Guide*.

Testing the Functionalities of Sentinel Rapid Deployment

6

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 this Collector to test Active Views, incident creation, correlation rules, and reports.

- ♦ [Section 6.1, “Testing the Rapid Deployment Installation,” on page 67](#)
- ♦ [Section 6.2, “Cleaning Up after Testing,” on page 77](#)
- ♦ [Section 6.3, “Using Real Data,” on page 78](#)

6.1 Testing the Rapid Deployment Installation

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

At the 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 Rapid Deployment Web interface.

For more information, see “[Accessing the Novell Sentinel Web Interface](#)” in the *Sentinel 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 for 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 Rapid Deployment User Guide*.

The Search feature is not enabled by default in SP2. However, if you want to enable this feature, refer to “[Enabling the Search Option in Web User Interface](#)” in the *Sentinel Rapid Deployment User Guide*.

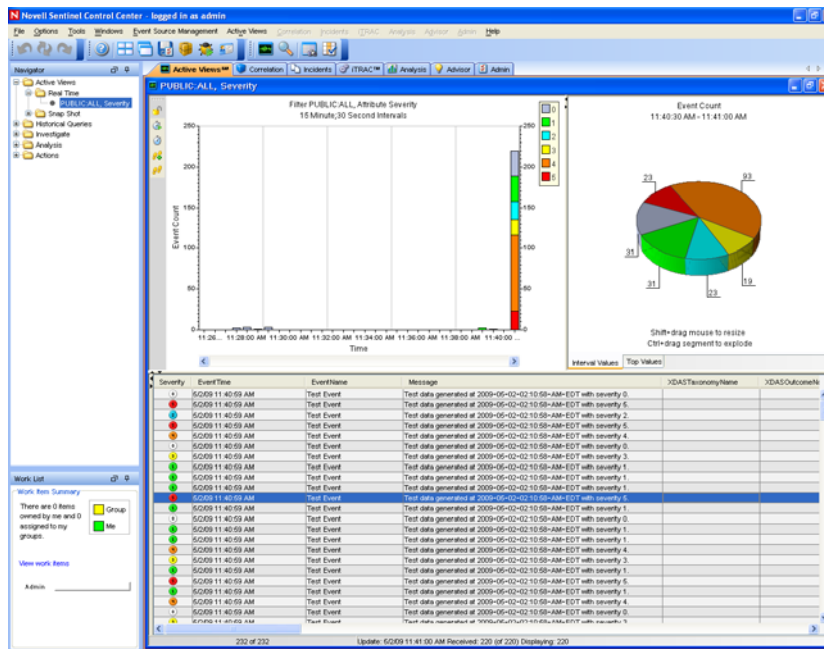
- 3 Select the Reports page, specify the parameters, then run a report.

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

For more information, refer to “[Running Reports](#)” in the *Sentinel Rapid Deployment User Guide*.

- 4 On the Applications page, click *Launch Sentinel Control Center*.
- 5 Log in to 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 *Internal_Events* and *High_Severity* public filters.

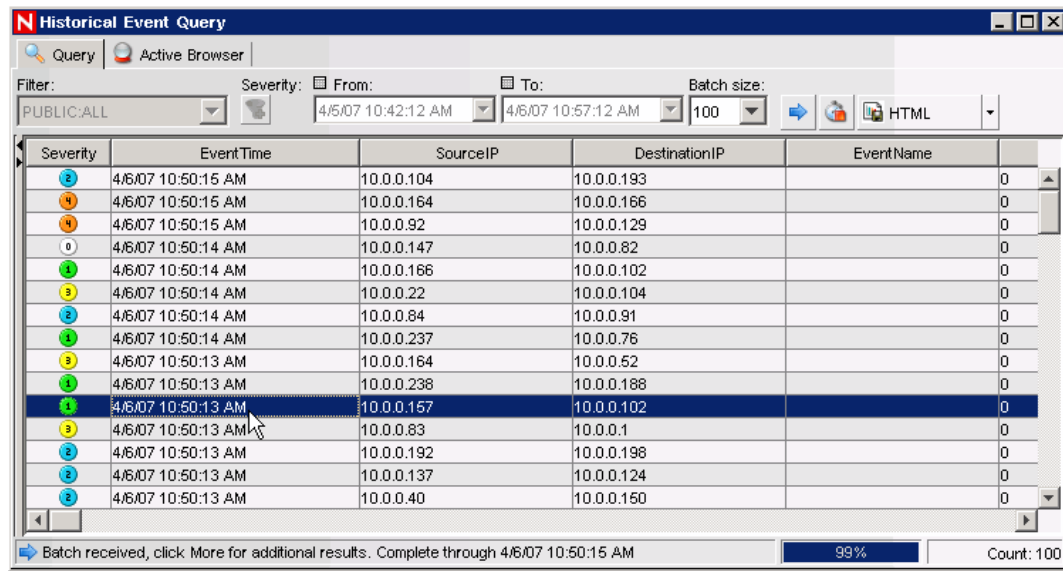


- 6 Go to the *Event Source Management* menu, then select *Live View*.
- 7 In the Graphical view, right-click *5 eps event source*, then select *Start*.
- 8 Close the Event Source Management Live View window.
- 9 Click the *Active Views* tab.

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 on 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 during which the Collector has been active. Use the *From* and *To* drop-down lists to select the date range.
- 13 Select the batch size.

14 Click the magnifying glass icon to run the query.

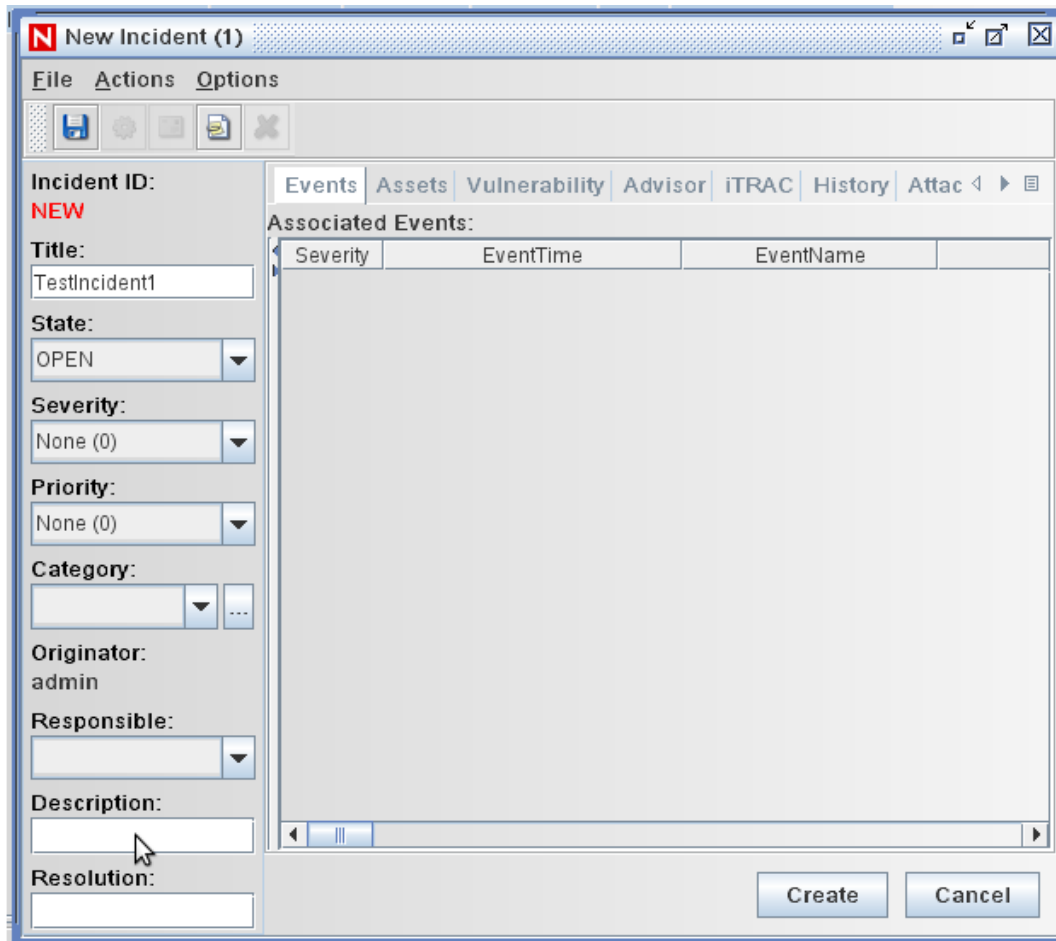


The screenshot shows the 'Historical Event Query' window. At the top, there are tabs for 'Query' and 'Active Browser'. Below the tabs, there are filters for 'Filter: PUBLIC:ALL', 'Severity: [checkbox]', 'From: 4/5/07 10:42:12 AM', 'To: 4/6/07 10:57:12 AM', and 'Batch size: 100'. There are also icons for a magnifying glass, a refresh button, and a dropdown menu set to 'HTML'. The main area is a table with the following columns: Severity, EventTime, SourceIP, DestinationIP, EventName, and a final column with the value '0'. The table contains 15 rows of data. The 10th row is highlighted in blue. At the bottom, there is a status bar that says 'Batch received, click More for additional results. Complete through 4/6/07 10:50:15 AM' and a progress indicator showing '99%' and 'Count: 100'.

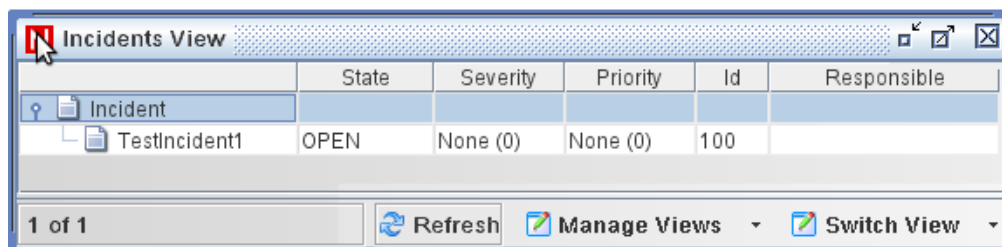
Severity	EventTime	SourceIP	DestinationIP	EventName	
2	4/6/07 10:50:15 AM	10.0.0.104	10.0.0.193		0
4	4/6/07 10:50:15 AM	10.0.0.164	10.0.0.166		0
4	4/6/07 10:50:15 AM	10.0.0.92	10.0.0.129		0
0	4/6/07 10:50:14 AM	10.0.0.147	10.0.0.82		0
1	4/6/07 10:50:14 AM	10.0.0.166	10.0.0.102		0
3	4/6/07 10:50:14 AM	10.0.0.22	10.0.0.104		0
2	4/6/07 10:50:14 AM	10.0.0.84	10.0.0.91		0
1	4/6/07 10:50:14 AM	10.0.0.237	10.0.0.76		0
3	4/6/07 10:50:13 AM	10.0.0.164	10.0.0.52		0
2	4/6/07 10:50:13 AM	10.0.0.238	10.0.0.188		0
1	4/6/07 10:50:13 AM	10.0.0.157	10.0.0.102		0
3	4/6/07 10:50:13 AM	10.0.0.83	10.0.0.1		0
2	4/6/07 10:50:13 AM	10.0.0.192	10.0.0.198		0
2	4/6/07 10:50:13 AM	10.0.0.137	10.0.0.124		0
2	4/6/07 10:50:13 AM	10.0.0.40	10.0.0.150		0

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

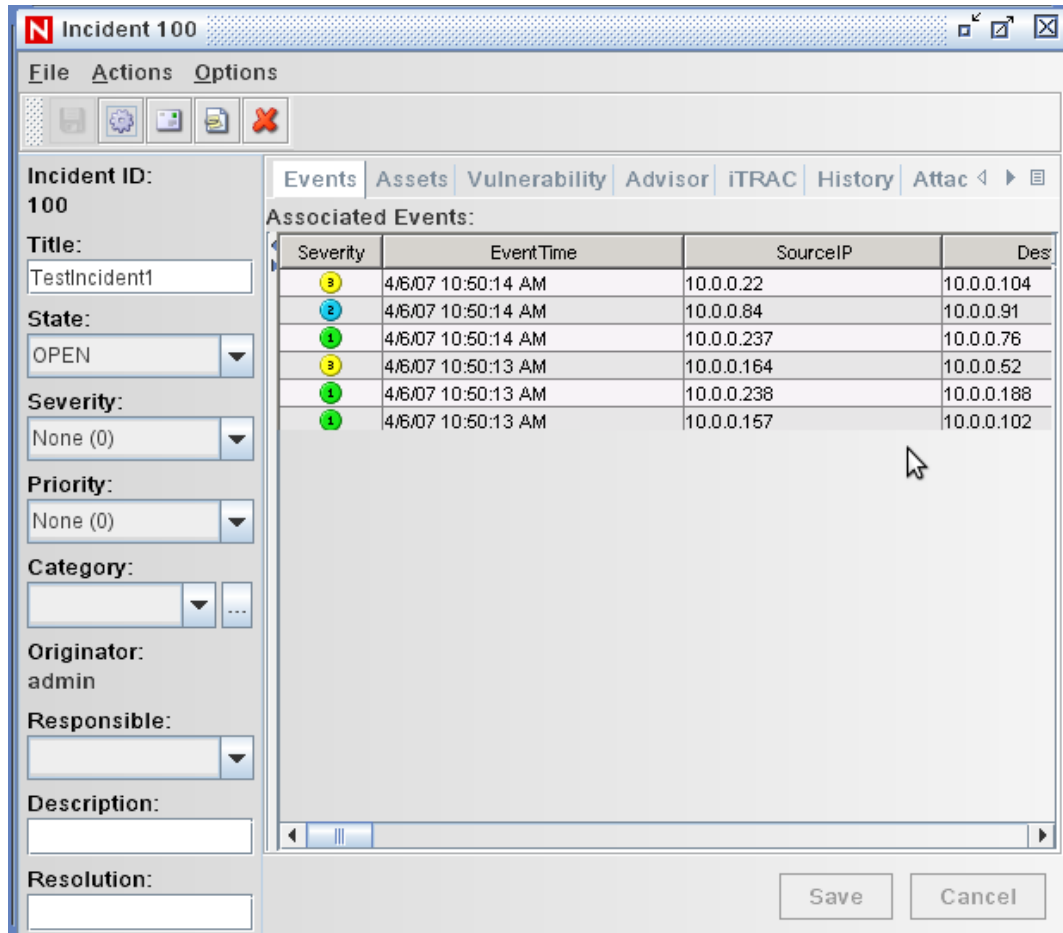
16 Right-click in the window, then select *Create Incident* to display the New Incident window.



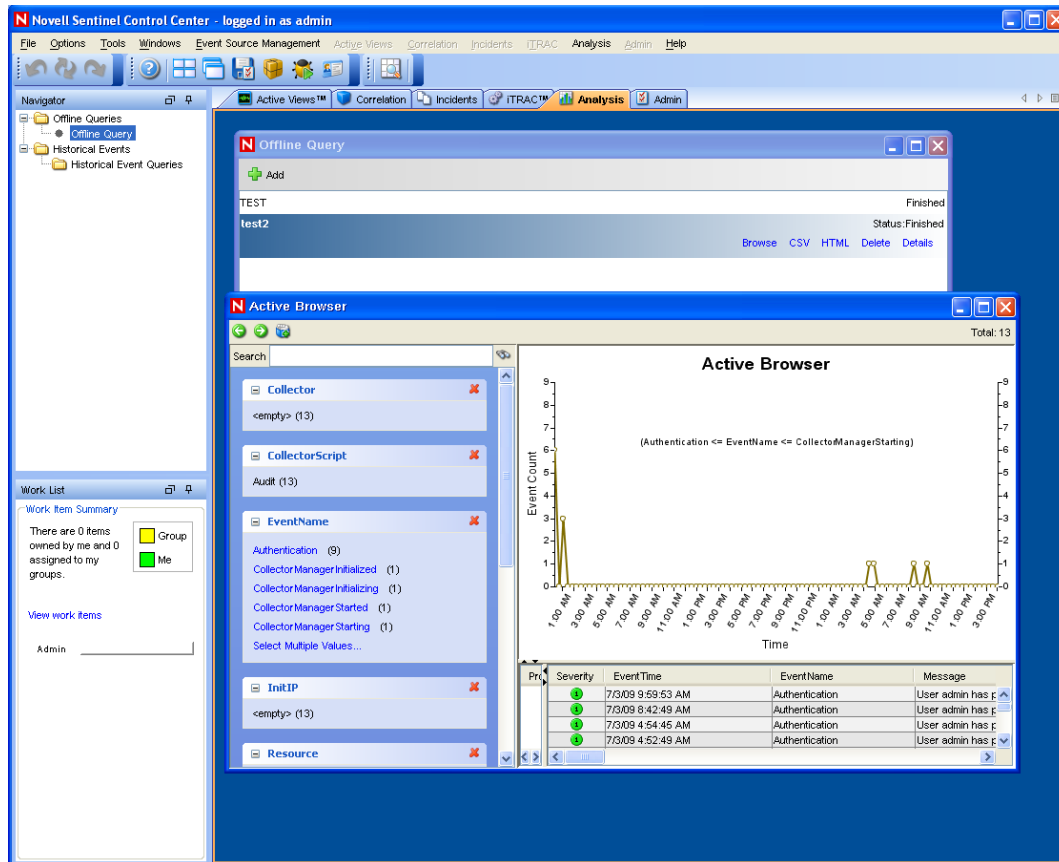
- 17 Name the incident TestIncident1, then click *Create*. When a success notification displays, click *Save*.
- 18 Click the *Incident* tab to see the incident you just created in the Incident View Manager.



- 19 Double-click the incident to display the events.

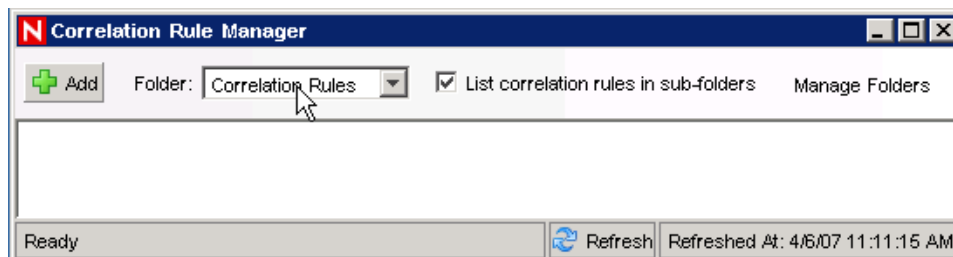


- 20 Close the Incident window.
- 21 Click the *Analysis* tab.
- 22 Click *Offline Queries* from the *Analysis* menu or from the Navigator.
- 23 In the Offline Query window, click *Add*.
- 24 Specify a name, select a filter, select a time period, then click *OK*.
- 25 Click *Browse* to view the list of events and associated details in the Active Browser window.

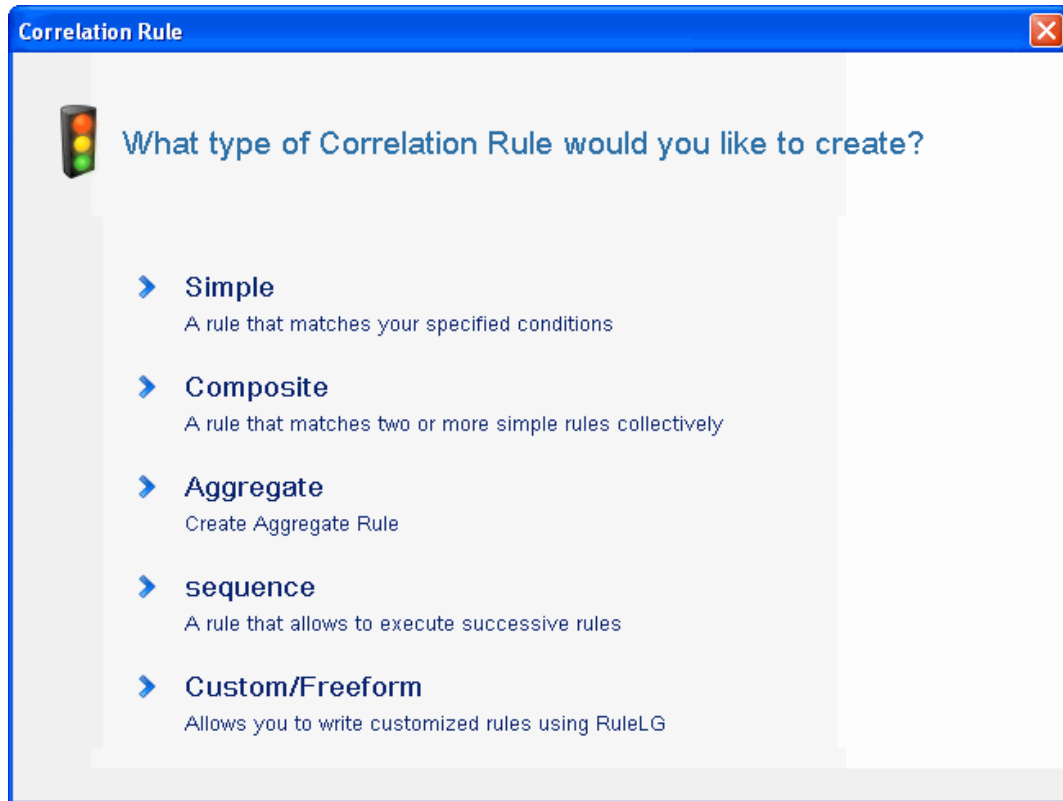


You can view the details such as Collector, Target IP, Severity, Target Service Port, and Resource.

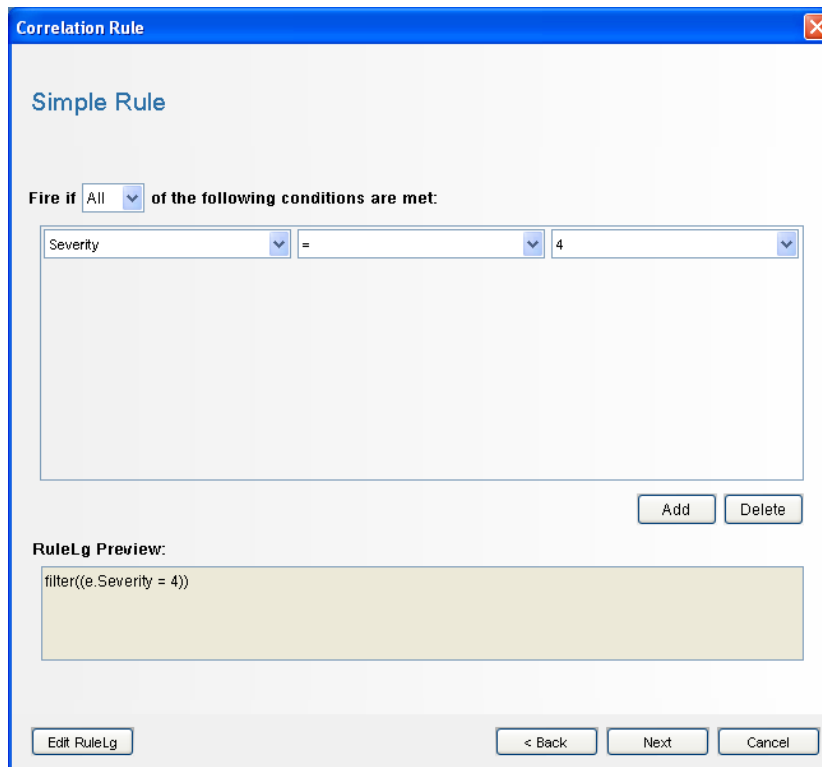
- 26 Select the *Correlation* tab. The Correlation Rule Manager is displayed.



- 27 Click *Add*. The Correlation Rule Wizard is displayed.



28 Click *Simple*. The Simple Rule window is displayed.



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

Correlation Rule

Update Criteria

After rule fires:

Continue to perform actions every time this rule fires

Do not perform actions every time this rule fires for the next

< Back Next Cancel

- 30 Select *Do not perform actions every time this rule fires*, use the drop-down menu to set the time period to 1 minute, then click *Next*. The General Description window is displayed.

Correlation Rule

General Description

Name

TestRule1

Namespace

Correlation Rules

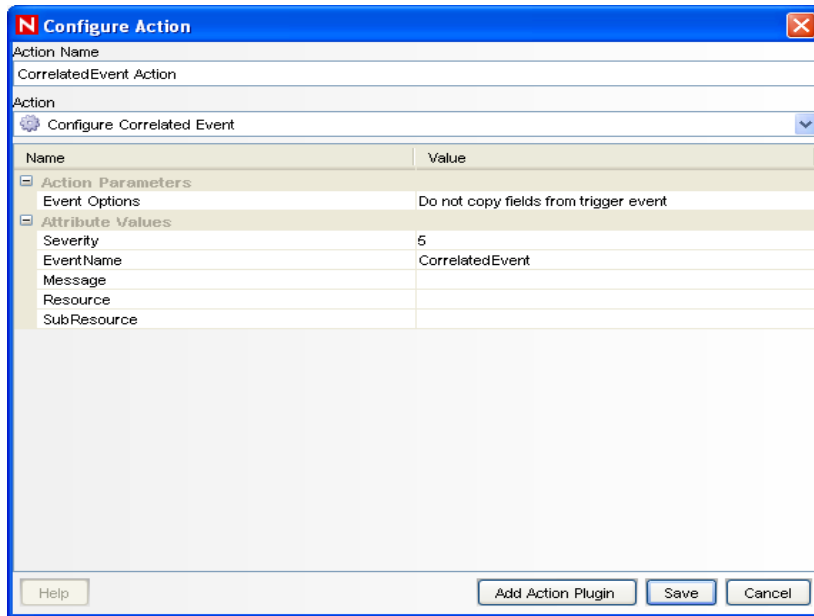
Description

This is a description of the rule.

< Back Next Cancel

- 31 Name the rule as *TestRule1*, provide a description, then 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 75](#).

The Configure Action window is displayed.



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

- ◆ Specify the action name, such as CorrelatedEvent Action.
- ◆ Select *Configure Correlated Event* from the *Action* drop-down list.
- ◆ Set the *Event Options*.
- ◆ Set the *Severity* to 5.
- ◆ Specify the *EventName*, such as CorrelatedEvent.
- ◆ Specify a message, if necessary.

For more information on creating an action, see “[Creating Actions](#)” in the *Sentinel Rapid Deployment User Guide*.

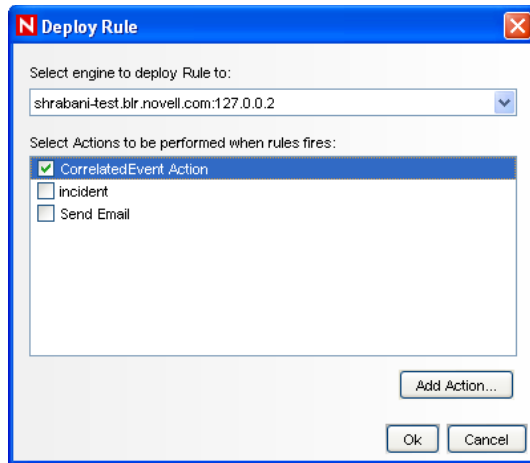
33c Click *Save*.

34 Open the Correlation Rule Manager window.

35 Select a rule, then click the *Deploy Rules* link. The Deploy Rule window is displayed.

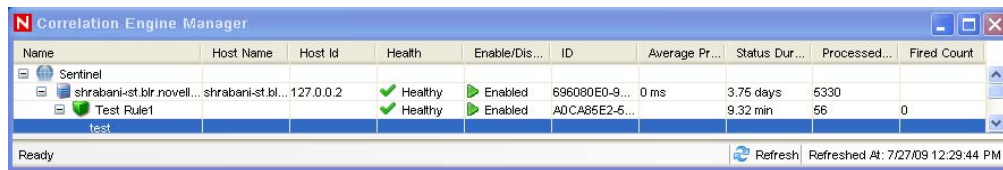
36 In the Deploy Rule window, select the Engine to deploy the rule.

37 Select the action you created in [Step 33 on page 74](#) to associate with the rule, then 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, then specify wrong user credentials to generate such an event.

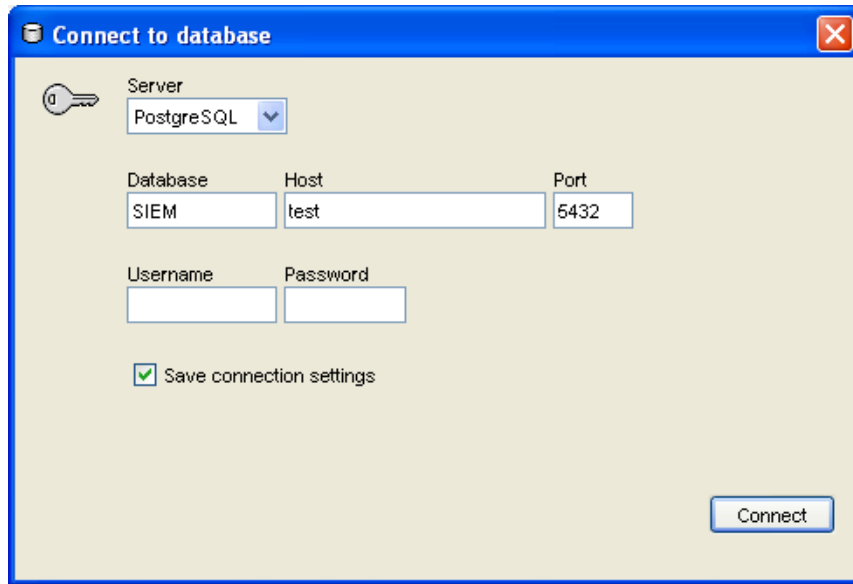
40 Click the *Active Views* tab, then verify if the Correlated Event is generated.

Severity	Event Time	Event Name	Message	X:DASTaxonomyName
4	8/17/09 11:43:34 AM	Authentication-Failed	User dd has failed Authentication to Sentinel/Wizard; reqId(A9A0B9A0-6D21-102...	
4	8/17/09 11:43:34 AM	AuthenticationFailed-Failed	Authentication of user dd with OS name BLR-PRADHIKA\pradhi from 169.254....	
4	8/17/09 11:43:34 AM	CorrelatedEvent		
4	8/17/09 11:43:34 AM	CorrelatedEvent		

41 Close the Sentinel Control Center.

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

43 Log in to 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.

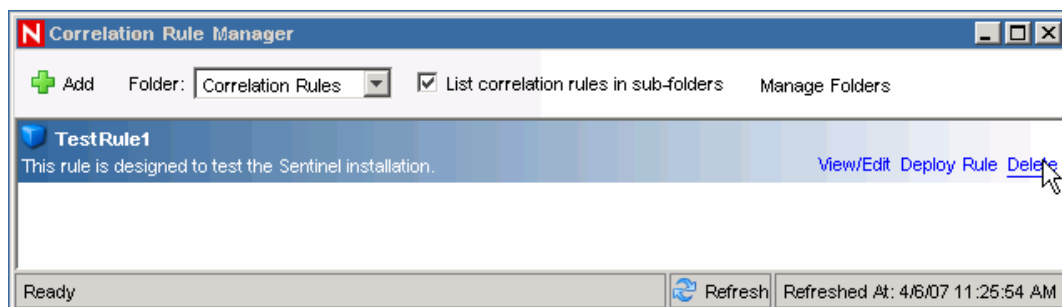
45 Close Sentinel Data Manager.

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

6.2 Cleaning Up after Testing

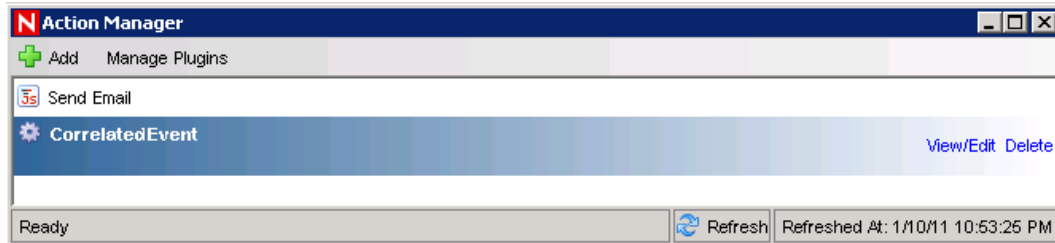
After completing the system verification, you should remove the objects created for the tests.

- 1 Log in to the system by 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, then select *Undeploy*.
- 5 Open the Correlation Rule Manager.
- 6 Select *TestRule1*, then click *Delete*.



7 Select *Tools > Action Manager* to display the Action Manager window.

8 Select the *CorrelatedEvent* action, click *Delete*, then click *Yes* to confirm the deletion.



- 9 Select the *Event Source Management* menu, then select *Live View*.
- 10 In the Graphical event source hierarchy, right-click *General Collector*, then select *Stop*.
- 11 Close the Event Source Management window.
- 12 Click the *Incidents* tab.
- 13 Open the Incident View Manager.
- 14 Select *TestIncident1*, right-click, then select *Delete*.

6.3 Using Real Data

To get started with real data, you 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 the *Sentinel Rapid Deployment User Guide*. Sentinel Solution Packs can help you get started quickly. See the [Sentinel Content Page \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html) for more details.

Uninstalling Sentinel Rapid Deployment

7

- ♦ [Section 7.1, “Uninstalling the Sentinel Rapid Deployment Server,” on page 79](#)
- ♦ [Section 7.2, “Uninstalling the Remote Collector Manager and Sentinel Client Applications,” on page 79](#)

7.1 Uninstalling the Sentinel Rapid Deployment Server

- 1 Log in as the `root` user.
- 2 Change to the `setup` directory.

```
cd <install_directory>/setup
```
- 3 Run the `uninstall.sh` script to uninstall the Sentinel Rapid Deployment server:

```
./uninstall.sh
```

The script prompts you with a message that indicates Sentinel Rapid Deployment will be completely removed.
- 4 Specify if you want to keep or remove the user while uninstalling the Sentinel Rapid Deployment server. Press `y` to remove the user or `n` to keep the user.
- 5 Specify if you want to keep or remove the group while uninstalling the Sentinel Rapid Deployment server. Press `y` to remove the group or `n` to keep the group.
- 6 Enter `y` to uninstall or `n` to exit the uninstallation.

7.2 Uninstalling the Remote Collector Manager and Sentinel Client Applications

- ♦ [Section 7.2.1, “Linux,” on page 79](#)
- ♦ [Section 7.2.2, “Windows,” on page 80](#)
- ♦ [Section 7.2.3, “Post-Uninstallation Procedures,” on page 80](#)

7.2.1 Linux

- 1 Log in as `root`.
- 2 (Conditional) If you are uninstalling the Collector Manager, stop the Sentinel Rapid Deployment services:

```
<install_directory>/bin/sentinel.sh stop
```
- 3 Go to the following location:

```
<install_directory>/_uninst
```
- 4 Perform any of the following:

Mode	Command
GUI	./uninstall.bin Continue with Step 5 on page 80 .
Console	./uninstall.bin -console Continue with the on-screen instructions.

- 5 Select a language and click *OK*.
- 6 In the Sentinel UninstallShield Wizard, click *Next*.
- 7 Select the components you want to uninstall and click *Next*.
- 8 Ensure that any running Sentinel applications are stopped and click *Next*.
A summary of the features selected for uninstall is displayed.
- 9 Click *Uninstall*.
- 10 Click *Finish*.

7.2.2 Windows

- 1 Log in as an Administrator user.
- 2 (Conditional) If you are uninstalling the Collector Manager, stop the Sentinel Rapid Deployment services:

```
<install_directory>\bin\sentinel.bat stop
```
- 3 Do either of the following:
 - ♦ Select *Start > All Programs > Sentinel > Uninstall Sentinel*.
 - ♦ Select *Start > Run*, enter `<install_directory>_uninst`, then double-click `uninstall.exe`.
- 4 Select a language and click *OK*.
The Sentinel Rapid Deployment UninstallShield Wizard is displayed.
- 5 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 uninstalling is displayed.
- 8 Click *Uninstall*.
- 9 Select to reboot the system and click *Finish*.

7.2.3 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 81](#)
- ♦ [“Windows” on page 81](#)

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\Universal` 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 Rapid Deployment Hostname

A

- ◆ [Section A.1, “Server,” on page 83](#)
- ◆ [Section A.2, “Client Applications,” on page 83](#)

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_directory>/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_directory>/config/configuration.xml`.

The Sentinel Control Center and the Solution Designer use this information.

- ◆ The help URL given in the `<install_directory>/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 Rapid Deployment installation issues.

- ♦ [Section B.1, “Database Authentication Fails on Entering Invalid Credentials,” on page 85](#)
- ♦ [Section B.2, “Sentinel Web Interface Fails to Start Up,” on page 85](#)
- ♦ [Section B.3, “Remote Collector Manager Throws Exception on Windows 2008 When UAC is Enabled,” on page 86](#)
- ♦ [Section B.4, “UUID Does Not Get Created for Imaged Collector Managers,” on page 87](#)

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 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 Rapid Deployment on a machine where an Identity Audit process is either running, or its uninstall is incomplete.

Action: Sentinel Rapid Deployment and Novell Identity Audit cannot be installed on a same machine. Before you install Sentinel 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 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 \(http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/\)](http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/).

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

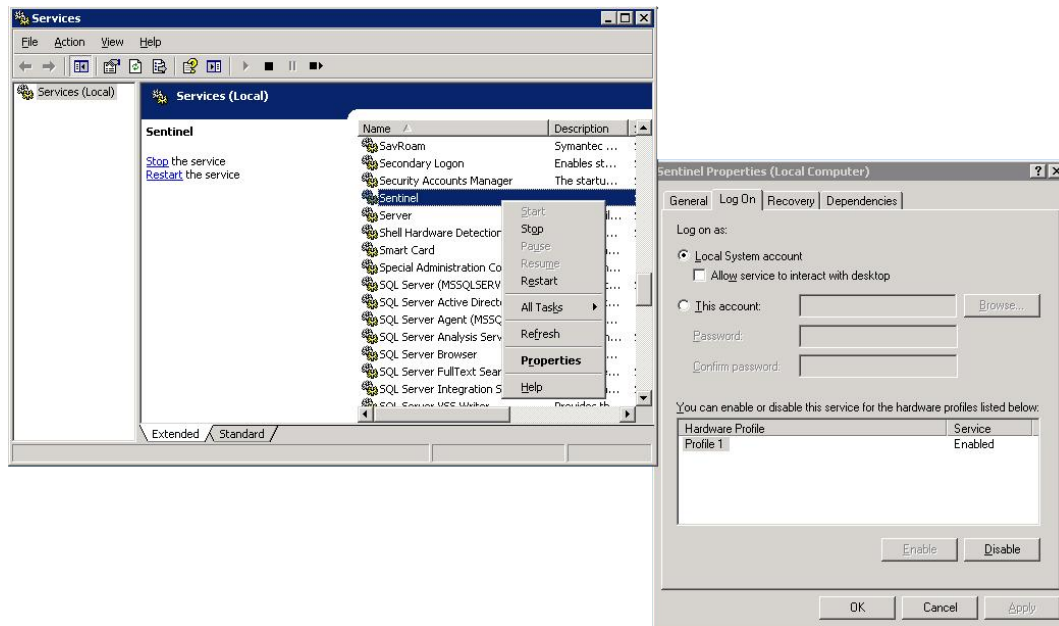
Problem: Log in as any user who belongs to the Administrator group. Execute the `setup.bat` command in a terminal prompt to install the Collector Manager. Restart the system or start the Collector Manager services manually, then log in with the same user credentials. Exceptions are logged in the `collector_manager0.0.log`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

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

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

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

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



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

B.4 UUID Does Not Get Created for Imaged Collector Managers

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

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

- 1** Delete the `host.id` or `sentinel.id` file that is located in the `<install_directory>/data` folder.
- 2** Restart the Collector Manager.

The Collector Manager automatically generates the UUID.

Best Practices for Maintaining PostgreSQL Database

C

You can fine-tune the database to improve the performance of the database server. The limits mentioned in this section are approximate recommendations. They are not hard limits. However, in highly dynamic systems, it is a good practice to build in buffers and allow room for growth.

- ♦ [Section C.1, “Modifying the Memory Configuration Parameters,” on page 89](#)
- ♦ [Section C.2, “Reducing the I/O Impact of Vacuum/Analyze,” on page 90](#)

C.1 Modifying the Memory Configuration Parameters

To fine-tune the PostgreSQL database server, modify the following memory configuration parameters in the `<install_dir>/3rd party/postgresql/data/postgresql.conf` file:

- ♦ **shared_buffers:** Determines how much memory is dedicated to PostgreSQL for caching data. For better performance, you can set this parameter value to one-fourth of the available RAM.
- ♦ **effective_cache_size:** Determines how much memory is available for disk caching by the operating system and within the database. You can estimate the size of this parameter by taking into account what is used by the operating system and other applications. You can allocate half of the total available system memory to this parameter.
- ♦ **work_mem:** Determines the amount of memory used by internal sort operations and hash tables before switching to temporary disk files. The value is specified in kilobytes. The default value is 1024 kilobytes (1 MB).

For a complex query, several sort or hash operations might be running in parallel. Each operation uses as much memory as the value specified for `work_mem` before it starts to put data into temporary disk files. If you are scheduling more reports on your Sentinel Rapid Deployment system, set this value between 500MB and 1GB.

- ♦ **maintenance_work_mem:** Determines the maximum amount of memory to be used in maintenance operations of the database, such as `VACUUM`, `CREATE INDEX`, and `ALTER TABLE ADD FOREIGN KEY`. The value is specified in kilobytes. The default value is 16384 kilobytes (16 MB).

Larger settings might improve the performance for vacuuming and for restoring database dumps. Keep this parameter unchanged because, the default value is sufficient for the Sentinel Rapid Deployment operations.

C.2 Reducing the I/O Impact of Vacuum/Analyze

You can improve the performance of the PostgreSQL database in several ways.

- ♦ The following two parameters take control of automatic vacuum operations and by default, these parameters are commented while installing the Sentinel Rapid Deployment server and you have to remove the comment and set the values.
 - ♦ **vacuum_cost_delay:** Determines the length of time that the process will sleep when the cost limit has been exceeded. For example, you can set this value to 100.
 - ♦ **vacuum_cost_limit:** Determines the accumulated cost that will cause the vacuuming process to sleep. For example, you can set this value to 10000.
If you set the value of these parameter to a non zero value, it will reduce the I/O impact of vacuum and analyze command on the normal database activity. They might be negligible performance impact while running the reports, since the vacuum takes more time than earlier.
- ♦ By default, the autovacuum process is set to true and runs periodically to recover the disk space and update the planner statistics. When the database size increases, autovacuum is not able to maintain all the database objects. In such cases, if the performance is slow, run the `AnalyzePartitions.sh` script as a cron job. This cron job should be set by the user who owns the Sentinel Rapid Deployment processes.

For example:

```
30 11 * * * $ESEC_HOME/bin/AnalyzePartitions.sh
```

Where:

- ♦ 30 is the time in minutes.
- ♦ 11 is the time in hours.
- ♦ `ESEC_HOME` is the absolute path of the database.

In this example, the script runs daily at 11:30.

- ♦ Avoid scheduling archiving to occur during reporting. If you schedule both processes together, reporting enters a waiting state because of PostgreSQL bugs and starts processing the data after the archive job is complete. This change impacts the performance of the database.