Installationshandbuch

Novell®
Sentinel 6.1 Rapid Deployment

SP2

April 2011

www.novell.com

Rechtliche Hinweise

Novell, Inc. leistet keinerlei Gewähr bezüglich des Inhalts oder Gebrauchs dieser Dokumentation. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Novell, Inc. behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt Novell, Inc. für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für ausstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Webseite Novell International Trade Services (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
USA.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite (http://www.novell.com/documentation) von Novell.

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch

Dieses Handbuch gibt eine Einführung in Novell Sentinel 6.1 Rapid Deployment Service Pack 2 und beschreibt die Installationsprozeduren.

Zielgruppe

Diese Dokumentation ist für Mitarbeiter des Bereichs Informationssicherheit konzipiert.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Funktion „Benutzerkommentare“ unten auf den einzelnen Seiten der Onlinedokumentation, um Ihre Kommentare einzugeben.

Zusätzliche Dokumentation

Die technische Dokumentation von Sentinel umfasst mehrere Bände. Dazu gehören:

- *Novell Sentinel Rapid Deployment-Installationshandbuch* (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-Benutzerhandbuch)
- *Novell Sentinel Rapid Deployment Reference Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/bookinfo.html) (Novell Sentinel Rapid Deployment-Referenzhandbuch)
- *Novell Sentinel -Installationshandbuch* (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 6.1-Benutzerhandbuch)

- *Novell Sentinel -Referenzhandbuch* (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)

  Auf der Sentinel SDK-Website finden Sie Details zur Entwicklung von Collectors (proprietär oder JavaScript) und JavaScript-Korrelationsaktionen.

Anfragen an Novell

- *Novell-Website* (http://www.novell.com)
- *Technischer Support von Novell* (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- *Novell-Self-Support* (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- *Patch Download Site* (http://download.novell.com/index.jsp)
- *Novell 24x7-Support* (http://www.novell.com/company/contact.html)
- *Sentinel TIDS* (http://support.novell.com/products/sentinel)
- Sentinel Community Support Forum (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sentinel Plugin-Website (http://support.novell.com/products/sentinel/secure/sentinelplugins.html)
- Benachrichtigungs-Mailingliste: Sie können sich über die Sentinel Plugin-Website in die Mailingliste eintragen.

Produktübersicht

1

Sentinel 6.1 Rapid Deployment ist eine vereinfachte Version von Novell Sentinel, die die Open Source-Komponenten PostgreSQL, activeMQ und JasperReports nutzt.

Die folgenden Abschnitte bieten Informationen zu den Hauptkomponenten des Sentinel 6.1 Rapid Deployment-Systems. Dieses Dokument, das *Sentinel Rapid Deployment-Installationshandbuch*, enthält detaillierte Informationen zu den Installations- und Konfigurationsprozeduren. Architektur und Betrieb der Software sowie administrative Vorgänge werden im *Sentinel Rapid Deployment User Guide* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) (Sentinel Rapid Deployment-Benutzerhandbuch) beschrieben.

1.1 Sentinel 6.1 Rapid Deployment – Überblick

Sentinel ist eine Lösung für die Verwaltung von Sicherheitsinformationen und Ereignissen, die Informationen von zahlreichen Quellen im gesamten Unternehmen empfängt, standardisiert und priorisiert. Diese aufbereiteten Informationen unterstützen die Entscheidungsfindung in Bezug auf Bedrohungen, Risiken und Richtlinien.

Sentinel protokolliert automatisch Erfassungs-, Analyse- und Berichtsprozesse, um zu gewährleisten, dass die Bedrohungserkennung und Audit-Anforderungen durch IT-Steuerelemente effektiv unterstützt werden. Mit Sentinel werden arbeitsaufwändige manuelle Prozesse durch die automatisierte Dauerüberwachung von Sicherheits- und Konformitätsereignissen sowie IT-Steuerelementen ersetzt.

Darüber hinaus sammelt Sentinel in der gesamten Netzwerkinfrastruktur des Unternehmens sowie von Drittanbieter-Systemen, -Geräten und -Anwendungen sicherheitsbezogene und nicht sicherheitsbezogene Informationen und korreliert sie. Sentinel zeigt die gesammelten Daten in einer grafischen Benutzeroberfläche (Graphical User Interface, GUI) an, identifiziert Sicherheits- bzw. Konformitätsprobleme und verfolgt die Behebungsmaßnahmen. Auf diese Weise werden ehemals fehleranfällige Prozesse optimiert und es entsteht ein strikteres und sichereres Verwaltungsprogramm.

Mithilfe der automatisierten Vorfallsreaktions-Verwaltung können Sie den Prozess der Verfolgung, Eskalation und Reaktion auf Vorfälle und Richtlinienverstöße dokumentieren und formalisieren. Außerdem wird die bidirektionale Integration in Problemberichtssysteme ermöglicht. Mit Sentinel können Sie prompt reagieren und Vorfälle auf effiziente Weise aus der Welt schaffen.

Mithilfe von Lösungspaketen können Sentinel-Korrelationsregeln, dynamische Listen, Zuordnungen, Berichte sowie iTRAC-Workflows mühelos verteilt und in Steuerelemente importiert werden. Diese Steuerelemente können für die Einhaltung spezifischer behördlicher Bestimmungen

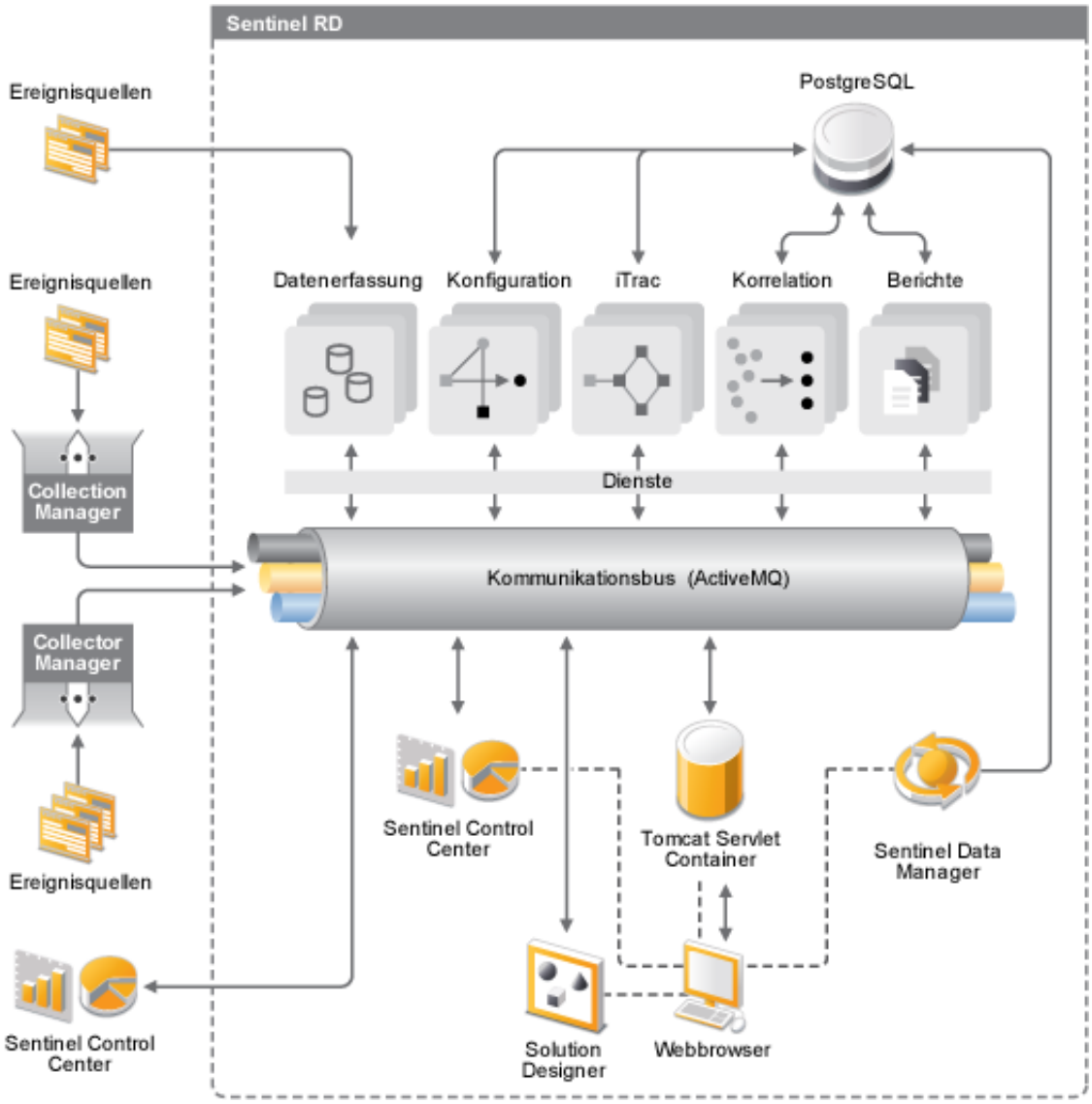
wie z. B. dem PCI-Standard (Payment Card Industry Data Security Standard) konfiguriert oder mit einer spezifischen Datenquelle, beispielsweise den Benutzerauthentifizierungsereignissen für eine Datenbank, verknüpft werden.

Mit Sentinel Rapid Deployment erhalten Sie:

- Integrierte automatisierte Sicherheitsverwaltung und Konformitätsüberwachung in Echtzeit in allen Systemen und Netzwerken.
- Ein Rahmenwerk mit Geschäftsrichtlinien zur Verbesserung der IT-Richtlinien und -Initiativen.
- Automatische Dokumentation und Berichterstellung in Bezug auf Sicherheits-, System- und Zugriffsereignisse im gesamten Unternehmen.
- Integrierte Verwaltung und Auflösung von Vorfällen.
- Nachweis und Überwachung der Einhaltung von internen Richtlinien und gesetzlichen Auflagen, darunter Sarbanes-Oxley, HIPAA, GLBA, FISMA und andere. Die für die Implementierung dieser Steuerelemente erforderlichen Inhalte werden mithilfe von Lösungspaketen verteilt und implementiert.

Im Folgenden finden Sie die Darstellung der konzeptuellen Architektur von Sentinel Rapid Deployment, die Aufschluss über die an der Sicherheits- und Konformitätsverwaltung beteiligten Komponenten gibt.

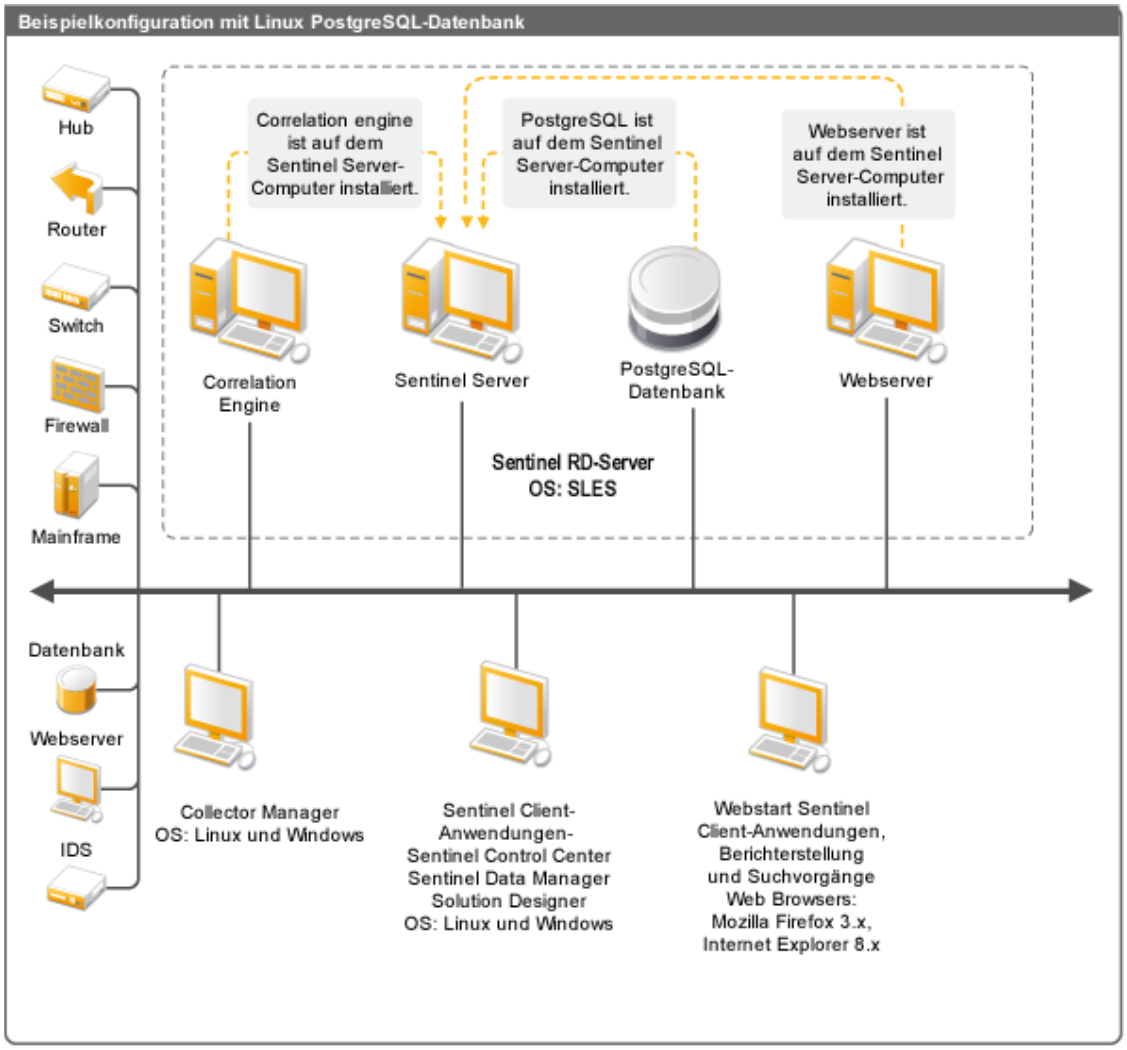
Abbildung 1-1 *Konzeptuelle Architektur von Sentinel*



1.2 Konfiguration von Sentinel 6.1 Rapid Deployment

Die folgende Grafik zeigt die Konfiguration von Sentinel 6.1 Rapid Deployment.

Abbildung 1-2 *Konfiguration von Sentinel 6.1 Rapid Deployment*



1.3 Benutzeroberflächen von Sentinel Rapid Deployment

Sentinel enthält folgende einfach bedienbare Benutzeroberflächen:

- Weboberfläche von Sentinel 6.1 Rapid Deployment
- Sentinel Control Center
- Sentinel Data Manager
- Sentinel Solution Designer
- Sentinel Plugin SDK

1.3.1 Weboberfläche von Sentinel 6.1 Rapid Deployment

Über die Weboberfläche von Novell Sentinel 6.1 Rapid Development können Sie Berichte verwalten sowie Sentinel Control Center (SCC), Sentinel Data Manager und Solution Designer starten. Außerdem können Sie über die Seite *Anwendungen* der Sentinel Rapid 6.1 Deployment-Weboberfläche die Installationsprogramme für den Collector-Manager und den Client herunterladen.

Weitere Informationen finden Sie unter „Verwalten von Managing Sentinel Rapid Deployment über die Weboberfläche“ im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.3.2 Sentinel Control Center

Das SCC bietet eine integrierte Sicherheitsverwaltungskonsole, mit der Analysten schnell neue Trends oder Angriffe erkennen, grafische Informationen in Echtzeit bearbeiten, damit interagieren sowie auf Vorfälle reagieren können.

Sie können das SCC entweder als Client-Anwendung oder über Java Webstart starten.

Zu den wichtigsten Funktionen von SCC gehören:

- **Active Views:** Analysefunktionen und Visualisierung in Echtzeit
- **Analyse:** Ausführen und Speichern von Offline-Abfragen
- **Vorfälle:** Erstellung und Verwaltung von Vorfällen
- **Korrelation:** Definition und Verwaltung von Korrelationsregeln
- **iTRAC:** Prozessverwaltung für die Dokumentation, Erzwingung und Verfolgung von Prozessen zur Vorfallsauflösung
- **Berichterstellung:** Verlaufsberichte und Metriken
- **Ereignisquellenverwaltung** Überwachung und Bereitstellung von Collectors
- **Solution Manager:** Installiert, implementiert und testet die Inhalte von Lösungspaketen

Weitere Informationen finden Sie unter „Sentinel Control Center“ im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.3.3 Sentinel Data Manager

Mit dem Sentinel Data Manager können Sie die Sentinel-Datenbank verwalten. Folgende Vorgänge können im Sentinel Data Manager ausgeführt werden:

- Nutzung des Datenbankspeichers überwachen.
- Datenbankpartitionen anzeigen und verwalten.
- Datenbankarchive verwalten.
- Archivierte Daten zurück in die Datenbank importieren.

Weitere Informationen finden Sie unter „Sentinel Data Manager“ im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.3.4 Sentinel Solution Designer

Der Sentinel Solution Designer dient der Erstellung und Modifizierung von Lösungspaketen. Hierbei handelt es sich um Pakete mit Sentinel-Inhalten, beispielsweise Korrelationsregeln, Aktionen, iTRAC-Workflows und Berichte.

Sentinel-Inhalte erweitern die Funktionalität des Sentinel-Systems. Zu diesen Inhalten gehören Aktionen, Integratoren und Plugins, beispielsweise Collectors, Connectors und Lösungspakete, die ihrerseits mehrere andere Arten von Plugins enthalten können. Diese modularen Komponenten ermöglichen die Integration von Drittanbieter-Systemen, die Installation einer vollständig steuerungsbasierten Sicherheitslösung sowie die automatisierte Beseitigung erkannter Vorfälle.

Weitere Informationen finden Sie unter „Solution Packs“ (Lösungspakete) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.3.5 Sentinel Plugin SDK

Das Sentinel Plugin SDK enthält von Novell Engineering entwickelte Bibliotheken und Code. Außerdem beinhaltet es die Schablone und Beispielcode, die Sie für die Entwicklung Ihrer eigenen Projekte verwenden können. Weitere Informationen finden Sie auf der Webseite zu Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html).

1.4 Sentinel-Serverkomponenten

Sentinel besteht aus den folgenden Komponenten:

- Abschnitt 1.4.1, „Data Access Service“, auf Seite 14
- Abschnitt 1.4.2, „Nachrichtenbus“, auf Seite 15
- Abschnitt 1.4.3, „Sentinel-Datenbank“, auf Seite 15
- Abschnitt 1.4.4, „Sentinel Collector-Manager“, auf Seite 15
- Abschnitt 1.4.5, „Correlation Engine“, auf Seite 15
- Abschnitt 1.4.6, „iTRAC“, auf Seite 15
- Abschnitt 1.4.7, „Sentinel Advisor und Schwachstellenerkennung“, auf Seite 16
- Abschnitt 1.4.8, „Webserver“, auf Seite 16

1.4.1 Data Access Service

Der Sentinel Data Access Service ist die Hauptkomponente für die Kommunikation mit der Sentinel-Datenbank. Der Data Access Server sorgt gemeinsam mit anderen Server-Komponenten dafür, dass von den Collector-Managern übermittelte Ereignisse in der Datenbank gespeichert, Daten gefiltert, Active View-Anzeigen verarbeitet, Datenbankabfragen durchgeführt, Ergebnisse verarbeitet und administrative Aufgaben wie z. B. die Benutzerauthentifizierung und -autorisierung durchgeführt werden. Weitere Informationen finden Sie unter „Data Access Service“ im *Sentinel Rapid Deployment Reference Guide* (Sentinel Rapid Deployment Referenzhandbuch).

1.4.2 Nachrichtenbus

Sentinel Rapid 6.1 Deployment verwendet den Open-Source-Message-Broker Apache Active MQ. Der Nachrichtenbus kann in einer einzigen Sekunde Tausende Nachrichtenpakete zwischen den Komponenten von Sentinel übertragen. Die Apache Active MQ-Architektur orientiert sich an der Java Message Oriented Middleware (JMOM), die asynchrone Aufrufe zwischen den Client- und Server-Anwendungen unterstützt. Nachrichtenwarteschlangen ermöglichen die temporäre Speicherung, wenn das Zielprogramm beschäftigt ist oder keine Verbindung hergestellt werden kann. Weitere Informationen finden Sie unter „Communication Server“ (Kommunikationsserver) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.4.3 Sentinel-Datenbank

Das Produkt Sentinel wurde um eine Backend-Datenbank herum erstellt, in der Sicherheitsereignisse sowie sämtliche Sentinel-Metadaten gespeichert sind. Sentinel 6.1 Rapid Deployment unterstützt PostgreSQL. Die Ereignisse werden in normalisierter Form gespeichert, zusammen mit Bestands- und Anfälligkeitsdaten, Identitätsdaten, Vorfall- und Workflow-Status sowie zahlreichen anderen Datentypen. Weitere Informationen finden Sie unter „Sentinel Data Manager“ im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.4.4 Sentinel Collector-Manager

Der Sentinel Collector-Manager verwaltet die Datenerfassung, überwacht Meldungen zum Systemstatus und führt bei Bedarf eine Ereignisfilterung durch. Zu den Hauptfunktionen des Collector-Managers zählen das Umwandeln von Ereignissen, das Hinzufügen unternehmensrelevanter Kontextinformationen zu Ereignissen über die Taxonomie, das globale Filtern von Ereignissen, das Routing von Ereignissen sowie das Senden von Zustandsmeldungen an den Sentinel-Server. Der Sentinel Collector-Manager stellt eine direkte Verbindung mit dem Nachrichtenbus her. Weitere Informationen finden Sie unter „Collector Manager“ (Collector-Manager) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.4.5 Correlation Engine

Die Correlation Engine automatisiert die Analyse des eingehenden Ereignisdatenstroms zur Identifikation relevanter Muster und verbessert auf diese Weise die Handhabung von Sicherheitsereignissen. Die Korrelation ermöglicht Ihnen das Definieren von Regeln, die kritische Bedrohungen und komplexe Angriffsmuster identifizieren, sodass Sie Ereignissen Priorität verleihen und eine effektive Vorfallsverwaltung und -reaktion initialisieren können. Weitere Informationen finden Sie unter „Correlation Tab“ (Registerkarte Correlation) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.4.6 iTRAC

Sentinel stellt ein iTRAC-Workflow-Verwaltungssystem bereit, mit dem Prozesse für die Vorfallsreaktion definiert und automatisiert werden können. Vorfälle, die in Sentinel entweder durch eine Korrelationsregel oder manuell identifiziert werden, können mit einem iTRAC-Workflow

verknüpft werden. Weitere Informationen finden Sie unter „iTRAC Workflows“ (iTRAC-Workflows) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.4.7 Sentinel Advisor und Schwachstellenerkennung

Sentinel Advisor ist ein optionaler Datenabonnement-Service mit Informationen zu bekannten Angriffen, Anfälligkeiten und Gegenmaßnahmen. Diese Daten ermöglichen in Kombination mit Informationen zu bekannten Schwachstellen sowie Echtzeit-Informationen zu Intrusion Detection (Erkennung von Eindringversuchen) und den entsprechenden Gegenmaßnahmen aus Ihrer Systemumgebung eine proaktive Schwachstellenerkennung. Außerdem kann im Falle eines Angriffs eines anfälligen Systems sofort reagiert werden.

Bei der Installation von Sentinel 6.1 Rapid Deployment wird standardmäßig ein Advisor-Daten-Snapshot installiert. Sie benötigen eine Advisor-Lizenz, um die fortlaufenden Aktualisierungen der Advisor-Daten zu abonnieren. Weitere Informationen finden Sie unter „Advisor Usage and Maintenance“ (Verwendung und Wartung von Advisor) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.4.8 Webserver

Für eine sichere Verbindung zur Weboberfläche von Sentinel Rapid Deployment wird Apache Tomcat als Webserver verwendet.

1.5 Sentinel-Plugins

Sentinel unterstützt eine Reihe von Plugins zur Erweiterung und Optimierung der Systemfunktionalität. Einige dieser Plugins sind bereits vorinstalliert. Von der Sentinel 6.1 Plugins-Website (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) können weitere Plugins (und Updates) heruntergeladen werden.

Für das Herunterladen einiger Plugins (z. B. für Remedy Integrator, IBM Mainframe Connector und den Connector für SAP XAL) ist eine zusätzliche Lizenz erforderlich.

1.5.1 Collectors

Sentinel sammelt Daten von Quellgeräten und stellt einen umfassenderen Ereignisdatenstrom bereit, indem Taxonomie, Schwachstellenerkennung sowie Geschäftsrelevanz in den Datenstrom integriert werden, bevor Ereignisse korreliert, analysiert und an die Datenbank gesendet werden. Ein umfangreicherer Ereignisstrom bedeutet, dass die Daten mit dem erforderlichen Geschäftskontext korreliert werden, um interne bzw. externe Bedrohungen und Richtlinienverletzungen erkennen und beheben zu können.

Sentinel-Collectors können unter anderem Daten von folgenden Gerätetypen analysieren:

- Intrusion Detection-Systeme (Host)
- Intrusion Detection-Systeme (Netzwerk)
- Firewalls
- Betriebssysteme
- Richtlinienüberwachung
- Authentifizierung
- Router und Switches
- VPNs
- Virenschutzsysteme
- Webserver
- Datenbanken
- Mainframe
- System zur Anfälligkeitsbewertung
- Directory Services
- Netzwerkverwaltungssysteme
- Proprietäre Systeme

JavaScript-Collectors können mit standardmäßigen JavaScript-Entwicklungswerkzeugen und dem Collector-SDK geschrieben werden.

1.5.2 Connectors und Integratoren

Connectors stellen die Verbindung zwischen dem Collector-Manager und Ereignisquellen über Standardprotokolle wie JDBC (Java Database Connectivity) und Syslog her. Ereignisse werden zu Analysezwecken vom Connector an den Collector übertragen.

Integratoren ermöglichen die Durchführung von Gegenmaßnahmen auf Systemen außerhalb von Sentinel. So kann beispielsweise eine Korrelationsaktion den Simple Object Access Protocol-(SOAP-)Integrator zur Initiierung eines Novell Identity Manager-Workflows nutzen.

Mit dem optionalen Remedy AR-Integrator kann ein Remedy-Bericht anhand von Sentinel-Ereignissen oder -Vorfällen erstellt werden. Weitere Informationen finden Sie unter „Action Manager and Integrator“ (Aktionsmanager und Integrator) im *Sentinel Rapid Deployment User Guide* (Sentinel 6.1 Rapid Deployment-Benutzerhandbuch).

1.5.3 Korrelationsregeln und -aktionen

Anhand von Korrelationsregeln werden wichtige Muster im Ereignis-Stream identifiziert. Wenn eine Korrelationsregel ausgelöst wird, initiiert sie Korrelationsaktionen, zu denen das Senden von Email-Benachrichtigungen, das Initiieren eines iTRAC-Workflows oder das Ausführen einer Aktion mithilfe eines Integrators gehören können. Weitere Informationen finden Sie unter „Correlation Tab“ (Registerkarte Correlation) im *Sentinel Rapid Deployment User Guide (Sentinel Rapid Deployment-Benutzerhandbuch)*.

1.5.4 Berichte

Mithilfe von Jasper Reports können Sie über die Weboberfläche von Sentinel Rapid Deployment eine Vielzahl von Dashboard- und operativen Berichten ausführen. Die Berichte werden üblicherweise über Lösungspakete verteilt.

1.5.5 iTRAC-Workflows

iTRAC-Workflows sorgen für konsistente, wiederholbare Prozesse beim Verwalten von Vorfällen. Die Workflow-Schablonen werden üblicherweise über Lösungspakete verteilt. iTRAC umfasst eine Gruppe von Standardschablonen, die Sie an Ihre spezifischen Anforderungen anpassen können. Weitere Informationen finden Sie unter „iTRAC Workflows“ (iTRAC-Workflows) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.5.6 Lösungspakete

Lösungspakete enthalten verwandte Sentinel-Inhalte wie z. B. Korrelationsregeln, Aktionen, iTRAC-Workflows und Berichte. Novell stellt Lösungspakete bereit, die auf spezifische Anforderungen im Geschäftsleben ausgerichtet sind. So liegt beim PCI-DSS-Lösungspaket der Schwerpunkt beispielsweise auf der Konformität mit dem Payment Card Industry Data Security Standard. Novell erstellt zudem Collector-Pakete, die hauptsächlich Inhalte einer bestimmten Ereignisquelle enthalten, beispielsweise Windows Active Directory. Weitere Informationen finden Sie unter „Solution Packs“ (Lösungspakete) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

1.6 Sprachunterstützung

Die Sentinel-Komponenten stehen in folgenden Sprachen zur Verfügung:

- Tschechisch
- Englisch
- Französisch
- Deutsch
- Italienisch
- Japanisch
- Niederländisch
- Polnisch
- Portugiesisch
- Chinesisch (Vereinfacht)
- Spanisch
- Chinesisch (Traditionell)

Systemanforderungen

2

Damit die Sentinel Rapid Deployment-Komponenten optimal und zuverlässig funktionieren, müssen sie auf der in diesem Abschnitt aufgeführten geprüften Soft- und Hardware installiert werden. Die im Folgenden genannten Anforderungen wurden qualitätsgeprüft und zertifiziert.

2.1 Unterstützte Plattformen

In Tabelle 2-1 werden Software-Betriebssystem-Kombinationen aufgeführt, die von Novell zertifiziert sind bzw. unterstützt werden. Die zertifizierten Kombinationen wurden mithilfe der vollständigen Testsuite von Novell Engineering getestet. Unterstützte Kombinationen verfügen über vollen Funktionsumfang.

2.1.1 Unterstützte Betriebssysteme

Novell unterstützt die Ausführung von Sentinel Rapid Deployment auf den in diesem Abschnitt beschriebenen Betriebssystemversionen. Novell unterstützt auch die Ausführung auf Betriebssystemen, wenn diese kleinere Aktualisierungen erhalten haben, z. B. Sicherheitspatches oder Hotfixes. Das Ausführen von Sentinel Rapid Deployment auf Systemen mit großen oder kleinen Aktualisierungen dieser Plattformen wird jedoch erst unterstützt, wenn Novell diese Aktualisierungen geprüft und zertifiziert hat.

Zu den Serverkomponenten von Sentinel Rapid Deployment gehören der Communication Server, die Correlation Engine, der Data Access Service (DAS), der Webserver sowie der Datenabonnement-Service Advisor.

Die Client-Anwendungen von Sentinel sind Sentinel Control Center (SCC), Sentinel Data Manager (SDM) und Sentinel Solution Designer (SSD).

Für den Collector-Manager gelten besondere Plattformanforderungen.

Tabelle 2-1 *Unterstützte und zertifizierte Betriebssysteme*

Plattformen	Serverkomponenten	Client-Anwendungen von Sentinel	Collector-Manager
SUSE Linux Enterprise Server (SLES) 11 SP1 (64-Bit)	Zertifiziert	Zertifiziert	Zertifiziert

Plattformen	Serverkomponenten	Client-Anwendungen von Sentinel	Collector-Manager
SUSE Linux Enterprise Server (SLES) 11 SP1 (32-Bit)	Nicht unterstützt	Unterstützt	Unterstützt
SUSE Linux Enterprise Server (SLES) 10 SP3 (64-Bit)	Zertifiziert	Unterstützt	Unterstützt
SUSE Linux Enterprise Server (SLES) 10 SP3 (32-Bit)	Unterstützt	Unterstützt	Unterstützt
Windows Server 2008 R2 (64 Bit)	Nicht unterstützt	Zertifiziert	Zertifiziert
Windows Server 2003 R2 (64 Bit)	Nicht unterstützt	Unterstützt	Unterstützt
Windows Server 2003 R2 (32 Bit)	Nicht unterstützt	Unterstützt	Unterstützt
Windows XP SP3 (32 Bit)	Nicht unterstützt	Unterstützt	Nicht unterstützt
Windows Vista SP2 (32 Bit)	Nicht unterstützt	Unterstützt	Nicht unterstützt
Windows 7	Nicht unterstützt	Zertifiziert	Nicht unterstützt

Beachten Sie folgende Richtlinien zur Gewährleistung optimaler Leistung, Stabilität und Zuverlässigkeit:

- Wird SLES verwendet, müssen auf dem Computer mit dem Sentinel Rapid Deployment-Server mindestens die Komponenten Base Server und X Window von SLES installiert sein.
- Verwenden Sie für den Sentinel Rapid Deployment-Server das EXT3-Dateisystem. Weitere Informationen zu Dateisystemen finden Sie unter Overview of File Systems in Linux (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html) (Überblick über Dateisysteme in Linux) im *Storage Administration Guide* (Handbuch zur Speicherungsverwaltung).

Hinweis:

- Sentinel Rapid Deployment wird auf Open Enterprise Server-Installationen von SLES nicht unterstützt.
- Die 32-Bit-Demoversion des Sentinel 6.1 Rapid Deployment-Servers wurde für Demonstrations- und Testumgebungen mit begrenztem Umfang konzipiert, in denen 32-Bit-Hardware und -Betriebssysteme eingesetzt werden. Kunden oder Partner mit einem Support-Vertrag für Sentinel 6.1 Rapid Deployment können vom Technischen Support von Novell auch für diese Plattform Unterstützung erhalten, jedoch nur für solche Probleme, die sich auf einer 64-Bit-Produktionsplattform reproduzieren lassen. Wegen der bekannten Einschränkungen der 32-Bit-Hardware behebt der Technische Support von Novell bei der 32-Bit-Demoversion keine die Leistung oder Skalierbarkeit betreffenden Probleme. In einer Produktionsumgebung werden 32-Bit-Demoversionen nicht unterstützt.

2.2 Hardwareanforderungen

Die Sentinel Rapid Deployment-Serverkomponenten laufen mit einigen betriebssystemabhängigen Ausnahmen auf x86-64-Hardware (64 Bit), wie in Abschnitt 2.1.1, „Unterstützte Betriebssysteme“, auf Seite 19 beschrieben. Sentinel ist für AMD Optero- und Intel Xeon-Hardware zertifiziert. Itanium-Server werden nicht unterstützt.

In diesem Abschnitt finden Sie einige allgemeine Hardware-Empfehlungen für den Entwurf des Sentinel-Systems. Den Empfehlungen für das Design liegen Ereignisratenbereiche zugrunde. Diese Empfehlungen basieren jedoch auf folgenden Annahmen:

- Die Ereignisrate liegt am oberen Ende des Bereichs „Ereignisse pro Sekunde“ (EPS).
- Die durchschnittliche Ereignisgröße beträgt 1 KB.
- Alle Ereignisse werden in der Datenbank gespeichert (es gibt also keine Filter zum Verwerfen von Ereignissen).
- Daten werden 90 Tagen lang online in der Datenbank gespeichert.
- Der Speicherplatz für Advisor-Daten ist in den Spezifikationen in Tabelle 2-2 auf Seite 22 und Tabelle 2-3 auf Seite 22 nicht enthalten.
- Auf dem Sentinel-Server stehen standardmäßig 5 GB Speicherplatz für das vorübergehende Caching von Ereignisdaten zur Verfügung, die nicht sofort in die Datenbank eingefügt werden können.
- Auf dem Sentinel-Server stehen außerdem standardmäßig 5 GB Speicherplatz für Ereignisse zur Verfügung, die nicht sofort in die Ereigniserstellungsdateien eingefügt werden können.
- Für das optionale Advisor-Abonnement sind zusätzlich 1 GB Speicherplatz auf dem Server erforderlich.

Die Hardwareempfehlungen für eine Sentinel-Implementierung können im Einzelnen unterschiedlich ausfallen. Es empfiehlt sich daher, vor der Fertigstellung der Sentinel-Architektur die Novell Consulting Services oder einen der Novell Sentinel Partner zu Rate zu ziehen. Die nachfolgenden Empfehlungen dienen als Leitfaden.

In der SLES-Version ist die Datenbank in den Sentinel Rapid Deployment-Server eingebettet und wird auf demselben Computer wie der Server installiert.

Hinweis: Wegen des hohen Ereignisaufkommens und des umfangreichen lokalen Cachings muss der Sentinel-Server über ein lokales oder freigegebenes Disk-Array mit Striping-Funktionalität (RAID) und mindestens vier Datenträgerspindeln verfügen.

Tabelle 2-2 *Konfiguration mit einem Computer (bis zu 2000 EPS)*

Komponenten	RAM	Leerzeichen	Prozessor
Computer 1: Sentinel Rapid Deployment Server ◆ Eingebettete PostgreSQL-Datenbank (3 GB) ◆ Collector-Manager (1228 MB) ◆ DAS_Core (1579 MB) ◆ DAS_Binary (1404 MB) ◆ Correlation Engine (1073 MB) ◆ 4 Collectors (Generic, Cisco, Snort und IBM, die jeweils 500 EPS generieren) ◆ 10 Korrelationsregeln bereitgestellt ◆ 10 eindeutige Active Views ◆ 3 gleichzeitige Benutzer ◆ 2 Zuordnungen bereitgestellt	16 GB	1 TB, SAS-Festplatte(n) (15K U/min) Hardware RAID 10	Dell PowerEdge 2900, 2 x Quad-Core Intel Xeon E5310 (1,6 GHz) mit Gigabit Ethernet NIC

Tabelle 2-3 *Konfiguration mit drei Computern (bis zu 5000 EPS)*

Komponenten	RAM	Leerzeichen	Prozessor
Computer 1: Sentinel Rapid Deployment Server ◆ Eingebettete PostgreSQL-Datenbank (3 GB) ◆ Collector-Manager (1228 MB) ◆ DAS_Core (1579 MB) ◆ DAS_Binary (1404 MB) ◆ Correlation Engine (1073 MB) ◆ 4 Collectors (die jeweils 500 EPS generieren, 1500 EPS vom Remote-Collector Manager 1 und 1500 EPS vom Remote-Collector Manager 2.	16 GB	1 TB, SAS-Festplatte(n) (15K U/min) Hardware RAID 10	Dell PowerEdge 2900, 2 x Quad-Core Intel Xeon E5310 (1,6 GHz) mit Gigabit Ethernet NIC
Computer 2: Collector-Manager ◆ Collector-Manager/Collectors ◆ 3 Collectors (die jeweils 500 EPS generieren)	4 GB	300 GB, SATA-Festplatte (3 GBit/s)	Intel Core 2 Duo E6750 (2,66 GHz) mit Gigabit Ethernet NIC
Computer 3: Collector-Manager ◆ Collector Manager / Collectors ◆ 3 Collectors (die jeweils 500 EPS generieren)	4 GB	300 GB, SATA-Festplatte (3 GBit/s)	Intel Core 2 Duo E6750 (2,66 GHz) mit Gigabit Ethernet NIC

2.3 Unterstützte Webbrowser

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

2.4 Virtuelle Umgebung

Sentinel Rapid Deployment wurde intensiv auf VMWare ESX Server getestet. Novell unterstützt Sentinel Rapid Deployment uneingeschränkt in dieser Umgebung. Um auf ESX oder in anderen virtuellen Umgebungen Ergebnisse zu erzielen, die mit den Testergebnissen auf physischen Computern vergleichbar sind, sollte die virtuelle Umgebung dieselben Anforderungen an Arbeitsspeicher, CPU, Plattenplatz und E/A erfüllen, die auch für physische Computer gelten.

Empfehlungen zu einem physischen Computer für ein SLES-System finden Sie unter Abschnitt 2.2, „Hardwareanforderungen“, auf Seite 21

2.5 Empfohlene Begrenzungen

Die in diesem Abschnitt genannten Begrenzungsempfehlungen basieren auf bei Novell oder bei Kunden durchgeführten Leistungsmessungen. Es handelt sich nicht um „harte“ Begrenzungen, sondern um Näherungswerte. In sehr dynamischen Systemen hat es sich bewährt, Puffer zu bilden und Wachstum zu ermöglichen.

2.5.1 Begrenzungen für den Collector-Manager

Wenn nicht anders angegeben, wird für die Collector-Manager-Begrenzungen angenommen, dass die Software auf einem Computer mit vier 2,2-GHz-Prozessoren und 4 GB RAM unter dem Betriebssystem SLES 11 läuft.

Tabelle 2-4 *Leistungserhaltende Collector-Manager-Begrenzungen*

Attribut	Begrenzung	Kommentar
Maximale Anzahl der Collector-Manager-Instanzen	20	Für diesen Wert wird vorausgesetzt, dass jeder Collector-Manager mit wenigen EPS (z. B. weniger als 100 EPS) läuft. Der Wert verringert sich mit zunehmender Anzahl von Ereignissen pro Sekunde.
Maximale Anzahl von Connectors (voll ausgelastet) auf einem einzelnen Collector-Manager	1 pro CPU-Kern, wobei mindestens 1 CPU-Kern für das Betriebssystem und andere Prozesse reserviert ist	Ein voll ausgelasteter Connector läuft mit der für diesen Connector-Typ höchsten EPS.

Attribut	Begrenzung	Kommentar
Maximale Anzahl von Collectors (voll ausgelastet) auf einem einzelnen Collector-Manager	1 pro CPU-Kern, wobei mindestens 1 CPU-Kern für das Betriebssystem und andere Prozesse reserviert ist	Ein voll ausgelasteter Collector läuft mit der für diesen Collector-Typ höchsten EPS.
Maximale Anzahl an Geräten auf einem einzelnen Collector-Manager	2000	Die Begrenzung auf dem Sentinel Rapid Deployment Server beträgt ebenfalls 2000. Daher wird die Begrenzung der Geräte für das Gesamtsystem bereits auf einem einzelnen Collector-Manager erreicht, wenn auf diesem 2000 Geräte vorhanden sind.
Die maximale Anzahl an Geräten auf dem Sentinel Rapid Deployment-Server	2000	Die Begrenzung der Geräte auf dem Sentinel Rapid Deployment-Server beträgt 2000

2.5.2 Begrenzungen für Berichte

Tabelle 2-5 *Leistungserhaltende Begrenzungen für Berichte*

Attribut	Begrenzung	Kommentar
Höchstanzahl gespeicherter Berichte	200	Diese Begrenzung kann sich erhöhen oder reduzieren. Dies hängt von der Größe der Berichte und dem verfügbaren Speicherplatz auf dem Server ab, der nicht vom Rest des Systems verwendet wird.
Maximale Anzahl gleichzeitig ausgeführter Berichte	3	Für diesen Wert wird vorausgesetzt, dass der Server noch nicht stark mit Datenerfassungs- oder anderen Aufgaben ausgelastet ist.

2.6 Testergebnisse

Die Konfiguration von Sentinel Rapid Deployment kann an die Ansprüche Ihrer Umgebung angepasst werden. Die folgenden auf Leistungsmessungen beruhenden Informationen sind das Ergebnis von Untersuchungen, die Novell mit den in den folgenden Tabellen aufgeführten spezifischen Konfigurationen durchgeführt hat.

Die Hardwareempfehlungen für eine Sentinel-Implementierung können im Einzelnen unterschiedlich ausfallen. Es empfiehlt sich daher, vor der Fertigstellung der Sentinel-Architektur die Novell Consulting Services oder einen der Novell Sentinel Partner zu Rate zu ziehen. Die nachstehenden Testinformationen können als Leitfaden dienen.

Linux Die Linux-Tests wurden mit dem maximalen EPS-Wert und einer unterschiedlichen Anzahl von Geräten sowie mit der maximalen Geräteanzahl für einen bestimmten EPS-Wert durchgeführt. Es wurde folgende Hardware-Konfiguration verwendet:

- **Anzahl der CPU-Kerne:** 4
- **CPU-Modell:** Intel Xeon CPU X5770 bei 2,93 GHz

- **RAM:** 16 GB
- **Festplattengröße (+ RAID-Typ und Anzahl der Festplatten im RAID):** 1,7 TB (RAID 5, 6 Festplatten)

Hinweis: Alle Tests wurden mit Syslog-basierten Ereignisquellen durchgeführt. Andere Connectors bieten möglicherweise eine andere Leistung.

Die folgende Tabelle zeigt die maximalen EPS, die Sie mit einer unterschiedlichen Anzahl an Geräten auf einem SLES-System skalieren können:

Tabelle 2-6 *Maximale EPS auf einem SLES-System*

Systemeinrichtung	Geräte	Maximaler EPS-Wert
4 Collector-Manager (ein lokaler und drei remote) mit 10 Collectors, die jeweils 500 EPS generieren	25	5,000
4 Collector-Manager (ein lokaler und drei remote) mit 10 Collectors, die jeweils 500 EPS generieren	100	5,000
4 Collector-Manager (ein lokaler und drei remote) mit 10 Collectors, die jeweils 500 EPS generieren	1,000	5,000

Die folgende Tabelle zeigt die maximalen Geräte, die Sie mit unterschiedlichen EPS-Raten auf einem SLES-System skalieren können:

Tabelle 2-7 *Maximale Geräte auf einem SLES-System*

Systemeinrichtung	EPS	Maximale Geräteanzahl
1 Collector-Manager mit 1 Collector, der 500 EPS generiert	500	2.000
1 Collector-Manager mit 2 Collectors, die jeweils 500 EPS generieren	1,000	2.000
1 Collector-Manager mit 3 Collectors, die jeweils 500 EPS generieren	1,500	2.000

Hinweis:

- Wenn Sie mehr EPS oder Geräte skalieren möchten, installieren Sie zusätzliche Collector-Manager.
- Die maximalen Anzahlen an Geräten sind keine unveränderbaren Begrenzungen, sondern Empfehlungen, die auf Leistungsmessungen von Novell basieren. Sie gehen von einer geringen durchschnittlichen EPS-Rate pro Gerät aus (weniger als 3 EPS). Höhere EPS-Raten führen zu einem niedrigeren dauerhaften Maximum an Geräten. Mit der folgenden Gleichung können Sie die ungefähren Grenzen für Ihre spezifische durchschnittliche EPS-Rate oder die Anzahl der Geräte ermitteln, sofern die maximale Anzahl der Geräte die oben angegebene Grenze nicht überschreitet: (maximale Geräte) x (durchschnittliche EPS pro Gerät) = maximale Ereignisrate.

Installation

3

Dieser Abschnitt enthält Informationen zur Installation von Sentinel Rapid Deployment und der Client-Komponenten.

3.1 Überblick

Zum Installationspaket von Sentinel gehört ein vereinfachtes Installationsprogramm für einen Einzelcomputer-Server, mit dem Sie alles installieren können, was für die Ausführung von Sentinel Rapid Deployment benötigt wird. Das Installationsprogramm von Sentinel Rapid Deployment-Server installiert folgende Komponenten:

3.1.1 Serverkomponenten

Tabelle 3-1 *Komponenten und Anwendungen des Sentinel-Servers*

Komponente	Beschreibung
	In der Sentinel-Datenbank werden Konfigurations- und Ereignisdaten gespeichert.
Nachrichtenbus	Ein auf JMS basierender Nachrichtenbus übernimmt die Kommunikation zwischen den Komponenten des Sentinel-Systems.
Correlation Engine	Die Correlation Engine führt eine Ereignisanalyse in Echtzeit durch.
Advisor	Advisor ermittelt die Echtzeit-Korrelation zwischen erkannten IDS-Angriffen und den Ergebnissen der Schwachstellenprüfung, um sofort auf ein erhöhtes Risiko hinweisen zu können.
Data Access Service	Enthält Komponenten zur Speicherung, Abfrage, Anzeige und Verarbeitung von Daten.

Komponente	Beschreibung
Webserver	Unterstützt die Weboberfläche für Sentinel Rapid Deployment.
Collector-Manager	Ein Dienst, der die Verbindung zu Ereignisquellen, Datenanalysen, Zuordnungen usw. handhabt. Sie können den Collector-Manager an andere Standorte, auf andere Computer und andere Betriebssysteme verteilen. Verwenden Sie dazu das Collector-Manager-Installationsprogramm, das über die Weboberfläche von Sentinel Rapid Deployment erhältlich ist. Sie können beispielsweise einen zusätzlichen Collector-Manager auf einem Windows-Computer installieren, um Windows-Ereignisse zu sammeln.
iTRAC	Sentinel stellt ein iTRAC-Workflow-Verwaltungssystem bereit, mit dem Prozesse für die Vorfallsreaktion definiert und automatisiert werden können. Vorfälle, die in Sentinel entweder durch eine Korrelationsregel oder manuell identifiziert werden, können mit einem iTRAC-Workflow verknüpft werden.

3.1.2 Client-Anwendungen

Die Client-Anwendungen (Sentinel Control Center, Sentinel Data Manager und Solution Designer) werden standardmäßig auf dem Sentinel Rapid Deployment-Server installiert. Es gibt mehrere Methoden, die Client-Anwendungen zu starten:

- Über die Weboberfläche von Sentinel Rapid Deployment. Auf den Clientsystemen sollte Java 1.6.0_20 oder höher installiert und der JRE-Pfad sollte definiert sein, damit die Sentinel-Anwendungen mittels Webstart gestartet werden können.

  Legen Sie die Umgebungsvariable `JAVA_HOME` so fest, dass sie auf den `JRE 6`-Ordner verweist. Der Exportpfad sollte auf den Ordner `bin` unterhalb des JRE 6-Speicherorts verweisen.

- Durch Verwendung von `<Installationsverzeichnis>/bin` als der Benutzer, der Eigentümer der Sentinel Rapid Deployment-Installationsdateien ist. Beispiel:

  `./bin/<client_application>.sh`

Tabelle 3-2 *Client-Anwendungen von Sentinel*

Komponente	Beschreibung
Sentinel Control Center	Die Hauptkonsole für Sicherheits- oder Konformitätsanalysten
Sentinel Data Manager	Dienstprogramm zur Datenbankverwaltung.
Solution Designer	Anwendung zum Erstellen von Lösungspaketen
Sentinel Collector-Manager	Dienst, der die Verbindung zu Ereignisquellen, Datenanalysen, Zuordnungen usw. handhabt. Auf dem Sentinel-Server wird ein Collector-Manager installiert. Mithilfe eines per Download erhältlichen Installationsprogramms können jedoch auf Windows- oder Linux-Remote-Computern zusätzliche Collector-Manager installiert werden.

3.2 Installation auf SUSE Linux Enterprise Server

3.2.1 Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind, bevor Sie Sentinel Rapid Deployment installieren. Weitere Informationen zu diesen Voraussetzungen (einschließlich der Liste der zertifizierten Plattformen) finden Sie hier: Kapitel 2, „Systemanforderungen“, auf Seite 19.

Wichtig: Sentinel Rapid Deployment-Installationen, die das vollständige Installationsprogramm verwenden, sollten immer auf einem sauberen System durchgeführt werden. Falls auf den Computern bereits andere Versionen von Sentinel installiert wurden, beispielsweise Sentinel Classic oder Sentinel Log Manager, müssen diese zunächst deinstalliert werden. Informationen zur Deinstallation älterer Versionen von Sentinel finden Sie in den entsprechenden Installationshandbüchern:

- Informationen zur Deinstallation von Sentinel Classic finden Sie im Kapitel „Uninstalling Sentinel“ (Deinstallation von Sentinel) im Sentinel Installation Guide (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html) (Sentinel 6.1 Installationshandbuch).
- Informationen zur Deinstallation von Sentinel Log Manager finden Sie im Kapitel „Uninstalling Sentinel Log Manager“ (Deinstallation von Sentinel Log Manager) im 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) (Sentinel Log Manager 1.1 Installationshandbuch).

Server

- Stellen Sie sicher, dass jeder Server-Computer die minimalen Systemanforderungen erfüllt. Weitere Informationen zu den Systemanforderungen finden Sie unter Kapitel 2, „Systemanforderungen“, auf Seite 19.
- Konfigurieren Sie das Betriebssystem so, dass der Befehl `hostname-f` einen gültigen Hostnamen zurückgibt.
- Installieren und konfigurieren Sie einen SMTP-(Simple Mail Transfer Protocol-)Server, wenn Sie Email-Benachrichtigungen über das Sentinel-System senden möchten.

Client

- Stellen Sie sicher, dass jeder Client-Computer die minimalen Systemanforderungen erfüllt. Weitere Informationen zu diesen Voraussetzungen finden Sie in Kapitel 2, „Systemanforderungen“, auf Seite 19.
- Erstellen Sie ein Verzeichnis, dessen Name ausschließlich ASCII-Zeichen (und keine Sonderzeichen) enthält, von dem aus Sie das Installationsprogramm starten können.

- Wenn Sie den Collector-Manager oder Client-Anwendungen remote auf Linux-Rechnern installieren, müssen Sie sicherstellen, dass der Admin-Benutzer uneingeschränkten Zugriff auf den Ordner `/tmp` hat.
- Vergewissern Sie sich, dass der Domänenbenutzer für den Collector-Manager unter Windows über Hauptbenutzerrechte verfügt, da normale Benutzerrechte für die Installation des Collector-Managers nicht ausreichen.
- Wenn Sie den Collector-Manager auf einem 64-Bit-Computer installieren, vergewissern Sie sich, dass die 32-Bit-Bibliotheken verfügbar sind. Die 32-Bit-Bibliotheken sind erforderlich, wenn ein Collector ausgeführt wird, der in der proprietären Collector-Sprache geschrieben wurde (dies trifft auf nahezu alle vor Juni 2008 geschriebenen Collectors zu), bzw. wenn bestimmte Connectors ausgeführt werden (etwa der LEA-Connector). Auf JavaScript basierende Collectors sowie der Rest von Sentinel sind 64-Bit-fähig. Das Sicherstellen der Verfügbarkeit dieser Bibliotheken ist besonders auf Linux-Plattformen wichtig, die sie möglicherweise nicht standardmäßig enthalten.

Advisor

Falls Sie den Advisor installieren möchten, müssen Sie das Daten-Abonnement für Sentinel Advisor und Schwachstellenerkennung erwerben. Verwenden Sie nach dem Erwerb des Abonnements Novell eLogin, um die Advisor-Daten herunterzuladen und zu aktualisieren. Weitere Informationen finden Sie im Kapitel „Advisor Usage and Maintenance“ (Verwendung und Wartung von Advisor) im *Sentinel Rapid Deployment User Guide* (Sentinel 6.1. Rapid Deployment-Benutzerhandbuch).

3.2.2 Installation von Sentinel Rapid Deployment

Für die Installation des Sentinel Rapid Deployment-Servers stehen folgende Möglichkeiten zur Verfügung:

- „Einzelskriptinstallation mit „root“-Rechten“ auf Seite 30
- „Nicht-root-Installation“ auf Seite 33

Während der Installation bietet das Installationsskript für den Sentinel Rapid Deployment-Server folgende Optionen an:

- **-all:** Diese Option können Sie nur als `root`-Benutzer verwenden. Es werden ein Benutzer (Standard: `novell`) und eine Benutzergruppe (Standard: `novell`) erstellt. Anschließend wird der Sentinel Rapid Deployment-Server installiert. Die Option sorgt dafür, dass die Sentinel Rapid Deployment-Dienste beim Systemstart automatisch gestartet werden.
- **-install:** Diese Option installiert den Sentinel Rapid Deployment-Server.
- **-createuser:** Diese Option können Sie nur als `root`-Benutzer verwenden. Es werden nur der Benutzer (Standard: `novell`) und die Benutzergruppe (Standard: `novell`) erstellt.
- **-createservice:** Diese Option können Sie nur als `root`-Benutzer verwenden. Diese Option sogt dafür, dass die Sentinel Rapid Deployment-Dienste beim Systemstart automatisch ausgeführt werden.
- **-help:** Diese Option zeigt die Hilfe für die Installationsoptionen an.

Einzelskriptinstallation mit „root“-Rechten

1. Melden Sie sich als `root`-Benutzer an.

Der Benutzer, der die Installation durchführt, benötigt Schreibzugriff auf das temporäre Verzeichnis, in das die Installationsdateien heruntergeladen werden.

2. Laden Sie das Installationsprogramm `sentinel6_rd_linux_x86-64.tar.gz` von der Website Novell Downloads (http://download.novell.com/) in ein temporäres Verzeichnis herunter.
3. Extrahieren Sie das Installationsprogramm:

   ```
   tar zxvf sentinel6_rd_linux_x86-64.tar.gz
   ```
4. Wechseln Sie in das Verzeichnis, in das Sie das Installationsprogramm extrahiert haben:

   ```
   cd sentinel6_rd_linux_x86-64
   ```
5. Führen Sie das Skript `install.sh` mit der Option `-all` aus:

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

   Das Installationsskript prüft zunächst, ob genügend Arbeitsspeicher und Plattenspeicherplatz zur Verfügung stehen. Bei weniger als 1 GB verfügbarem Arbeitsspeicher beendet das Skript die Installation automatisch. Bei mehr als 1 GB, doch weniger als 4 GB Arbeitsspeicher meldet das Skript, dass weniger Arbeitsspeicher als empfohlen zur Verfügung steht. Sie können angeben, ob Sie mit der Installation fortfahren möchten. Geben Sie `y` ein, wenn die Installation fortgesetzt werden soll, und `n`, wenn Sie nicht fortfahren möchten.
6. Geben Sie den Benutzernamen ein oder drücken Sie die Eingabetaste, um den Standardbenutzernamen zu verwenden. Der Standardbenutzername ist `novell`.

   Wenn der angegebene Benutzer bereits vorhanden ist, informiert Sie das Installationsprogramm und listet die Gruppe der Benutzer auf. Fahren Sie mit Schritt 8 fort.

   Wenn der angegebene Benutzername nicht vorhanden ist, erstellt das Installationsprogramm den Benutzer. Fahren Sie mit Schritt 7 fort.
7. Geben Sie den Gruppennamen ein oder drücken Sie die Eingabetaste, um den Standardgruppennamen zu verwenden. Der Standardgruppenname ist `novell`.

   Wenn der angegebene Gruppenname vorhanden ist, fährt das Installationsprogramm mit der Installation fort. Anderenfalls erstellt das Installationsprogramm die Gruppe und meldet, dass der angegebene Benutzername in der angegebenen Gruppe erstellt wird.

   Der angegebene Benutzer und die angegebene Gruppe sind Eigentümer der Installation und der Ausführungsvorgänge von Sentinel.
8. Geben Sie den Installationspfad ein oder drücken Sie die Eingabetaste, um den standardmäßigen Installationspfad zu verwenden. Der Standardpfad ist `/opt/novell`.

   Der angegebene Installationspfad sollte kein Leerzeichen enthalten. Kommen Leerzeichen darin vor, fordert das Installationsskript Sie auf, einen Installationspfad ohne Leerzeichen anzugeben.
9. Wählen Sie eine der folgenden Sprachen aus, indem Sie die entsprechende Zahl eingeben:

Seriennummer	Sprache
1	Tschechisch
2	Englisch
3	Französisch
4	Deutsch

Seriennummer	Sprache
5	Italienisch
6	Japanisch
7	Niederländisch
8	Polnisch
9	Portugiesisch
10	Chinesisch (Vereinfacht)
11	Spanisch
12	Chinesisch (Traditionell)

Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.

10 Lesen Sie die Endbenutzer-Lizenzvereinbarung und geben Sie `1` ein, wenn Sie der Vereinbarung zustimmen und mit der Installation fortfahren möchten. Geben Sie `2` ein, wenn Sie die Installation beenden möchten.

Das Installationsprogramm beginnt, die Dateien zu extrahieren, und fragt nach Ihrer Lizenz.

11 Geben Sie `1` ein, wenn Sie einen Lizenzschlüssel für eine 90-Tage-Testversion verwenden möchten. Geben Sie `2` ein, wenn Sie den gültigen Lizenzschlüssel verwenden möchten.

Wenn Sie `2` eingeben, fordert das Installationsprogramm Sie auf, den gültigen Sentinel RD-Lizenzschlüssel einzugeben. Geben Sie einen ungültigen Lizenzschlüssel ein, fordert Sie das Installationsprogramm erneut dazu auf, den gültigen Lizenzschlüssel einzugeben. Ist auch der zweite angegebene Lizenzschlüssel ungültig, wird automatisch ein Lizenzschlüssel für eine 90-Tage-Testversion verwendet. Sie können den gültigen Lizenzschlüssel später eingeben.

Anschließend lädt das Skript die gültige Lizenz bzw. die Testlizenz.

12 Geben Sie ein Passwort für den Benutzer `dbauser` ein und bestätigen Sie es durch erneutes Eingeben.

Die `dbauser`-Berechtigung wird zur Erstellung von Tabellen und Partitionen in der PostgreSQL-Datenbank verwendet.

13 Geben Sie ein Passwort für den Benutzer `admin` ein und bestätigen Sie es durch erneutes Eingeben.

Verwenden Sie in den Passwörtern für die Benutzer `admin` und `dbauser` keinen umgekehrten Schrägstrich (\) und kein Apostroph (‘), da diese Zeichen in PostgreSQL-Datenbanken nicht zulässig sind.

Das Installationsskript installiert die PostgreSQL-Datenbank, erstellt Tabellen und Partitionen und installiert anschließend den Sentinel Rapid Deployment-Server.

Nach der Installation haben Sie folgende Möglichkeiten:

- Starten Sie die Sentinel Rapid Deployment-Weboberfläche über die URL `https://<SERVER_IP>:8443/sentinel`. <*SERVER_IP*> ist die IP-Adresse des Computers, auf dem Sentinel Rapid Deployment installiert ist.
- Starten Sie das Sentinel Control Center, indem Sie das Skript `<Installationsverzeichnis>/bin/control_center.sh` als der oben in Schritt 6 erstellte Benutzer ausführen.

Nicht-root-Installation

Falls Richtlinien Ihrer Organisation die Ausführung des gesamten Installationsvorgangs als `root` verbieten, kann die Installation auch in zwei Schritten durchgeführt werden. Für die Durchführung des ersten Teils des Installationsvorgangs sind `root`-Rechte erforderlich. Der zweite Teil wird vom verwaltungsbefugten Benutzer (der im ersten Schritt erstellt wurde) durchgeführt.

1. Melden Sie sich bei dem Server an, auf dem Sie Sentinel Rapid Deployment installieren möchten.

   Der Benutzer, der die Installation durchführt, benötigt Schreibzugriff auf das temporäre Verzeichnis, in das die Installationsdateien heruntergeladen werden.

2. Laden Sie das Installationsprogramm `sentinel6_rd_linux_x86-64.tar.gz` von der Website Novell Downloads (http://download.novell.com/) in ein temporäres Verzeichnis herunter.

3. Extrahieren Sie das Installationsprogramm:

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

4. Melden Sie sich als `root`-Benutzer an.

5. Wechseln Sie in das Verzeichnis, in das Sie das Installationsprogramm extrahiert haben:

   ```
   cd sentinel6_rd_linux_x86-64
   ```

6. Führen Sie das Skript `install.sh` mit der Option `-createuser` aus:

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

7. Geben Sie den Benutzernamen ein oder drücken Sie die Eingabetaste, um den Standardbenutzernamen zu verwenden. Der Standardbenutzername ist `novell`.

   Wenn der angegebene Benutzer bereits vorhanden ist, informiert Sie das Installationsprogramm und listet die Gruppe der Benutzer auf. Fahren Sie mit Schritt 9 fort.

   Wenn der angegebene Benutzername nicht vorhanden ist, erstellt das Installationsprogramm den Benutzer. Fahren Sie mit Schritt 8 fort.

8. Geben Sie den Gruppennamen ein oder drücken Sie die Eingabetaste, um den Standardgruppennamen zu verwenden. Der Standardgruppenname ist `novell`.

   Wenn der angegebene Gruppenname vorhanden ist, fährt das Installationsprogramm mit der Installation fort. Anderenfalls erstellt das Installationsprogramm die Gruppe und meldet, dass der angegebene Benutzername in der angegebenen Gruppe erstellt wird.

   Der angegebene Benutzer und die angegebene Gruppe sind Eigentümer der Installation und der Ausführungsvorgänge von Sentinel.

9. Geben Sie den Installationspfad ein oder drücken Sie die Eingabetaste, um den standardmäßigen Installationspfad zu verwenden. Der Standardpfad ist `/opt/novell`.

   Der angegebene Installationspfad sollte kein Leerzeichen enthalten. Kommen Leerzeichen darin vor, fordert das Installationsskript Sie auf, einen Installationspfad ohne Leerzeichen anzugeben.

10. Melden Sie sich als der Nicht-root-Benutzer an. Beispiel.

    ```
    su - novell
    ```

11. Führen Sie das Installationsskript mit der Option `-install` aus:

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

Das Installationsskript prüft zunächst, ob genügend Arbeitsspeicher und Plattenspeicherplatz zur Verfügung stehen. Bei weniger als 1 GB verfügbarem Arbeitsspeicher beendet das Skript die Installation automatisch. Bei mehr als 1 GB, doch weniger als 4 GB Arbeitsspeicher meldet das Skript, dass weniger Arbeitsspeicher als empfohlen zur Verfügung steht. Sie können angeben, ob Sie mit der Installation fortfahren möchten. Geben Sie `y` ein, wenn die Installation fortgesetzt werden soll, und `n`, wenn Sie nicht fortfahren möchten.

12 Geben Sie den Installationspfad ein oder drücken Sie die Eingabetaste, um den standardmäßigen Installationspfad zu verwenden. Der Standardpfad ist `/opt/novell`.

Der angegebene Installationspfad sollte kein Leerzeichen enthalten. Kommen Leerzeichen darin vor, fordert das Installationsskript Sie auf, einen Installationspfad ohne Leerzeichen anzugeben.

13 Wählen Sie eine der folgenden Sprachen aus, indem Sie die entsprechende Zahl eingeben:

Seriennummer	Sprache
1	Tschechisch
2	Englisch
3	Französisch
4	Deutsch
5	Italienisch
6	Japanisch
7	Niederländisch
8	Polnisch
9	Portugiesisch
10	Chinesisch (Vereinfacht)
11	Spanisch
12	Chinesisch (Traditionell)

Die Endbenutzer-Lizenzvereinbarung wird in der ausgewählten Sprache angezeigt.

14 Lesen Sie die Endbenutzer-Lizenzvereinbarung und geben Sie `1` ein, wenn Sie der Vereinbarung zustimmen und mit der Installation fortfahren möchten. Geben Sie `2` ein, wenn Sie die Installation beenden möchten.

Das Installationsprogramm beginnt, die Dateien zu extrahieren, und fragt nach Ihrer Lizenz.

15 Geben Sie `1` ein, wenn Sie einen Lizenzschlüssel für eine 90-Tage-Testversion verwenden möchten. Geben Sie `2` ein, wenn Sie den gültigen Lizenzschlüssel verwenden möchten.

Wenn Sie `2` eingeben, fordert das Installationsprogramm Sie auf, den gültigen Sentinel RD-Lizenzschlüssel einzugeben. Geben Sie einen ungültigen Lizenzschlüssel ein, fordert Sie das Installationsprogramm erneut dazu auf, den gültigen Lizenzschlüssel einzugeben. Ist auch der zweite angegebene Lizenzschlüssel ungültig, wird automatisch ein Lizenzschlüssel für eine 90-Tage-Testversion verwendet. Sie können den gültigen Lizenzschlüssel später eingeben.

Anschließend lädt das Skript die gültige Lizenz bzw. die Testlizenz.

16 Geben Sie ein Passwort für den Benutzer `dbauser` ein und bestätigen Sie es durch erneutes Eingeben.

   Die `dbauser`-Berechtigung wird zur Erstellung von Tabellen und Partitionen in der PostgreSQL-Datenbank verwendet.

17 Geben Sie ein Passwort für den Benutzer `admin` ein und bestätigen Sie es durch erneutes Eingeben.

   Verwenden Sie in den Passwörtern für die Benutzer `admin` und `dbauser` keinen umgekehrten Schrägstrich (\) und kein Apostroph (‘), da diese Zeichen in PostgreSQL-Datenbanken nicht zulässig sind.

18 Wenn die Sentinel Rapid Deployment-Dienste automatisch beim Systemstart gestartet werden sollen, führen Sie im Anschluss an die Installation das Skript `install.sh` mit der Option `-createservice` als `root`-Benutzer aus:

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

Nach der Installation haben Sie folgende Möglichkeiten:

- Starten Sie die Sentinel Rapid Deployment-Weboberfläche über die URL `https://<SERVER_IP>:8443/sentinel`. <*SERVER_IP*> ist die IP-Adresse des Computers, auf dem Sentinel Rapid Deployment installiert ist.
- Starten Sie das Sentinel Control Center, indem Sie das Skript `<Installationsverzeichnis>/bin/control_center.sh` als der oben in Schritt 7 erstellte Benutzer ausführen.

3.3 Installieren des Collector-Managers und der Sentinel-Client-Anwendungen

Laden Sie mit der Novell Sentinel Rapid Deployment-Weboberfläche die Installationsprogramme für den Collector-Manager und den Client herunter.

- Abschnitt 3.3.1, „Herunterladen der Installationsprogramme“, auf Seite 35
- Abschnitt 3.3.2, „Portnummern für Sentinel Rapid Deployment Client-Komponenten“, auf Seite 36
- Abschnitt 3.3.3, „Installieren der Sentinel-Client-Anwendungen“, auf Seite 37
- Abschnitt 3.3.4, „Installieren des Sentinel Collector-Managers auf SLES oder Windows“, auf Seite 39

3.3.1 Herunterladen der Installationsprogramme

1 Öffnen Sie einen Webbrowser und rufen Sie folgende URL auf:

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

   Ersetzen Sie `<svrname.example.com>` durch den tatsächlichen DNS-Namen bzw. die tatsächliche IP-Adresse des Servers, unter dem Sentinel ausgeführt wird. Bei der URL wird zwischen Groß- und Kleinschreibung unterschieden.

2 Wenn Sie zur Überprüfung der Zertifikate aufgefordert werden, gehen Sie die Zertifikatsdaten durch und klicken Sie dann auf *Ja*, wenn sie gültig sind.

3 Geben Sie den Benutzernamen und das Passwort zum Zugriff auf das Sentinel-Konto ein.

4 Wählen Sie mit der Dropdown-Liste *Sprachen* die Sprache aus.

Normalerweise sollte diese Sprache dem Sprachcode entsprechen, der für den Sentinel Rapid Deployment-Server und den lokalen Computer verwendet wird. Stellen Sie sicher, dass die Spracheneinstellung Ihres Browsers für die Unterstützung der gewünschten Sprache konfiguriert ist.

5 Klicken Sie auf *Anmelden*.

6 Wählen Sie *Anwendungen* aus.

Sie können folgende Installationsprogramme herunterladen:

Optionen	Beschreibung	Aktion
Installationsprogramm für Collector-Manager	Das Collector-Manager-Installationsprogramm ermöglicht es Ihnen, den Sentinel Collector-Manager auf den unterstützten Windows- und Linux-Plattformen zu installieren.	Klicken Sie auf *Download Collector Manager Installer* (Installationsprogramm für Collector-Manager herunterladen) und befolgen Sie die Anweisungen auf dem Bildschirm.
Client-Installationsprogramm	Mit dem Client-Installationsprogramm können Sie Sentinel Control Center, Sentinel Solution Designer und Sentinel Data Manager auf den unterstützten Plattformen installieren.	Klicken Sie auf *Client-Installationsprogramme herunterladen* und befolgen Sie die Anweisungen auf dem Bildschirm.

Weitere Informationen zur Installation des Collector-Managers finden Sie in Abschnitt 3.3.4, „Installieren des Sentinel Collector-Managers auf SLES oder Windows“, auf Seite 39. Informationen zur Installation des Client-Installationsprogramms finden Sie in Abschnitt 3.3.3, „Installieren der Sentinel-Client-Anwendungen“, auf Seite 37.

3.3.2 Portnummern für Sentinel Rapid Deployment Client-Komponenten

Verwenden Sie bei der Konfiguration Ihrer Firewall-Einstellungen folgende Ports, um den gegenseitigen Zugriff zwischen dem Sentinel Rapid Deployment-Server und den Client-Komponenten zu ermöglichen.

Tabelle 3-3 *Kompatible Portnummern für Sentinel Rapid Deployment Client-Komponenten*

Portnummer	Beschreibung
61616	Die Remote-Collector-Manager verwenden diese Portnummer für die Verbindung zum Sentinel Rapid Deployment-Server über ActiveMQ.
10013	Das Sentinel Control Center verwendet diese Portnummer für die Verbindung zum Sentinel Rapid Deployment-Server über einen Proxy.
5432	Der Sentinel Data Manager verwendet diese Portnummer für die Verbindung zur PostgreSQL-Datenbank.
8443	Die Web-Clients verwenden diese Portnummer für die Verbindung zum Sentinel Rapid Deployment-Server.

3.3.3 Installieren der Sentinel-Client-Anwendungen

Sie können eine Sentinel Client-Anwendung auf einem Linux- oder einem Windows-System installieren. So installieren Sie Client-Anwendungen:

1. Wechseln Sie zu dem Ordner, in den Sie das Client-Installationsprogramm heruntergeladen haben.
2. Extrahieren Sie das Installationsskript aus folgender Datei:

Plattform	Aktion
Windows	Dekomprimieren Sie die Datei `client_installer.zip`. Die Dateien werden in ein Verzeichnis mit der Bezeichnung `disk1` dekomprimiert.
Linux	Führen Sie folgenden Befehl mit „root“-Rechten aus: `unzip client_installer.zip` Die Dateien werden in ein Verzeichnis mit der Bezeichnung `disk1` dekomprimiert.

3. Wechseln Sie in das Installationsverzeichnis und starten Sie die Installation:

Plattform	Aktion
Windows	Führen Sie `disk1\setup.bat` aus. **Hinweis:** Starten Sie auf einem Windows Vista-Computer die Befehlseingabeaufforderung, indem Sie die Option *Als Administrator ausführen* aus den Menüoptionen verwenden, die per Klick mit der rechten Maustaste aufgerufen werden können.
Linux	◆ **GUI-Modus:** `<Installationsverzeichnis>/disk1/setup.sh` ◆ **Konsolenmodus:** `<Installationsverzeichnis>/disk1/setup.sh –console`

Die folgenden Schritte gelten nur für den GUI-Modus.

4. Klicken Sie auf den Abwärtspfeil und wählen Sie eine der Sprachen aus.
5. Klicken Sie auf der ersten Seite auf *Weiter*.
6. Lesen Sie die Lizenzvereinbarung durch und erklären Sie Ihr Einverständnis. Klicken Sie auf *Weiter*.
7. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben. Klicken Sie auf *Weiter*.

Wichtig: Die Installation kann nicht in einem Verzeichnis erfolgen, dessen Name Sonderzeichen oder Nicht-ASCII-Zeichen enthält. Beispielsweise lautet der Standardpfad bei einer Installation von Sentinel Rapid Deployment unter Windows x86-64 `C:\\Programme (x86)`. Sie müssen diesen Standardpfad ändern, um Sonderzeichen wie die Klammern in „(x86)“ zu vermeiden, wenn Sie mit der Installation fortfahren möchten.

8 Wählen Sie die zu installierenden Sentinel-Anwendungen aus.

Folgende Optionen stehen zur Verfügung:

Komponente	Beschreibung
Sentinel Control Center	Die Hauptkonsole für Sicherheits- oder Konformitätsanalysten.
Sentinel Data Manager (SDM)	Wird für Aktivitäten zur Datenbankverwaltung verwendet.
Solution Designer	Hilft Ihnen beim Erstellen von Lösungspaketen.

9 Wenn Sie auswählen, dass Sentinel Control Center installiert werden soll, fordert Sie das Installationsprogramm auf, die maximale Menge an Arbeitsspeicher einzugeben, die Sentinel Control Center zugeordnet werden soll. Geben Sie die maximale JVM-Heap-Größe (MB) an, die ausschließlich von Sentinel Control Center verwendet werden soll.

Zulässig sind Werte im Bereich von 64 bis 1024 MB.

Diese Option ist nicht verfügbar, wenn bereits eine der Sentinel-Anwendungen installiert wurde.

10 Geben Sie den Benutzernamen ein oder drücken Sie die Eingabetaste, um den Standardbenutzernamen zu verwenden. Der Standardbenutzername ist `esecadm`.

Dies ist der Benutzername des Eigentümers des installierten Sentinel-Produkts. Wenn der Benutzer noch nicht existiert, wird er gemeinsam mit einem Basisverzeichnis im angegebenen Verzeichnis erstellt.

11 Geben Sie das Basisverzeichnis des Benutzers an oder drücken Sie die Eingabetaste, um das Standardverzeichnis zu verwenden. Das Standardverzeichnis ist `/export/home`.

Lautet der Benutzername `esecadm`, dann heißt das entsprechende Basisverzeichnis `/export/home/esecadm`.

12 Geben Sie das Passwort an, mit dem sich der Benutzer als `esecadm`-Benutzer anmelden kann, falls Sie in Schritt 10 den Standardbenutzernamen ausgewählt haben. Anderenfalls geben Sie das Passwort für den Benutzer an, den Sie in Schritt 10 erstellt haben.

13 Legen Sie die folgenden Werte fest:

- **Nachrichtenbus-Port:** Der Port, den der Kommunikationsserver überwacht. Die Komponenten, die eine direkte Verbindung mit dem Kommunikationsserver herstellen, verwenden diesen Port. Die Standard-Portnummer lautet 61616.
- **Sentinel Control Center-Proxy-Port:** Der Port, den der SSL-Proxyserver (DAS-Proxy) überwacht, um den Benutzernamen und das Passwort zu akzeptieren. Der SSL-Proxyserver akzeptiert den Berechtigungsnachweis auf Basis der authentifizierten Verbindungen. Sentinel Control Center verwendet diesen Port, um die Verbindung zum Sentinel-Server herzustellen. Die Standardportnummer ist `10013`.
- **Hostname des Kommunikationsservers:** Die IP-Adresse oder der Hostname des Computers, auf dem der Sentinel Rapid Deployment-Server installiert ist.

Stellen Sie sicher, dass die Portnummern denen in der Datei `<Installationsverzeichnis>/config/configuration.xml` auf dem Sentinel Rapid Deployment-Server entsprechen, damit die Kommunikation möglich ist. Notieren Sie sich diese Ports für spätere Installationen auf anderen Computern. Weitere Informationen zu Portnummern finden Sie in Abschnitt 3.3.2, „Portnummern für Sentinel Rapid Deployment Client-Komponenten“, auf Seite 36.

14 Klicken Sie auf *Weiter*.

Eine Zusammenfassung der Installation wird angezeigt.

15 Klicken Sie auf *Installieren*.

16 Schließen Sie die Installation mit *Fertig stellen* ab.

Hinweis: Verwenden Sie bei der erneuten Anmeldung den Benutzernamen, den Sie in Schritt 10 angegeben haben.

Sollten Sie den selbst festgelegten Benutzernamen vergessen haben, öffnen Sie eine Terminal-Konsole und geben Sie als `root`-Benutzer folgenden Befehl ein:

```
env | grep ESEC_USER
```

Mit diesem Befehl wird der Benutzername zurückgegeben, wenn der Benutzer bereits erstellt wurde und die Umgebungsvariablen bereits festgelegt worden sind.

3.3.4 Installieren des Sentinel Collector-Managers auf SLES oder Windows

Das Installationsprogramm für den Sentinel Collector-Manager kann auf der Seite „Anwendungen“ der Weboberfläche von Sentinel Rapid Deployment heruntergeladen werden. So installieren Sie den Collector-Manager:

1 Wechseln Sie zu dem Ordner, in den Sie das Installationsprogramm für den Collector-Manager heruntergeladen haben.

2 Extrahieren Sie das Installationsskript aus folgender Datei:

Plattform	Aktion
Windows	Dekomprimieren Sie die Datei `scm_installer.zip`. Die Dateien werden in ein Verzeichnis mit der Bezeichnung `disk1` dekomprimiert.
Linux	Führen Sie folgenden Befehl mit „root“-Rechten aus: `unzip scm_installer.zip` Die Dateien werden in ein Verzeichnis mit der Bezeichnung `disk1` dekomprimiert.

3 Wechseln Sie in das Verzeichnis `disk1` und starten Sie die Installation:

Plattform	Aktion
Windows	Führen Sie den folgenden Befehl aus: `disk1\setup.bat`
Linux	◆ **GUI-Modus:** `<`*`Installationsverzeichnis`*`>/disk1/setup.sh` ◆ **Konsolenmodus:** `<`*`Installationsverzeichnis`*`>/disk1/setup.sh -console`

4. Wählen Sie die Sprache aus, in der Sie die Installation fortsetzen möchten.
5. Lesen Sie die Informationen im Begrüßungsbildschirm und klicken Sie auf *Weiter*.
6. Lesen Sie die Lizenzvereinbarung durch und erklären Sie Ihr Einverständnis. Klicken Sie auf *Weiter*.
7. Übernehmen Sie das Standardinstallationsverzeichnis oder klicken Sie auf *Durchsuchen*, um den Speicherort für die Installation anzugeben, und klicken Sie dann auf *Weiter*.

   Wichtig: Die Installation kann nicht in einem Verzeichnis erfolgen, dessen Name Sonderzeichen oder Nicht-ASCII-Zeichen enthält. Beispielsweise lautet der Standardpfad bei einer Installation von Sentinel unter Windows x86-64 `C:\\Programme (x86)`. Sie müssen den Standardpfad ändern, um Sonderzeichen wie die Klammern in „(x86)“ zu vermeiden, wenn Sie mit der Installation fortfahren möchten.

   ---

8. Geben Sie den Sentinel-Administrator-Benutzernamen und den Pfad zum entsprechenden Basisverzeichnis an.

   Diese Option ist nicht verfügbar, wenn bereits irgendwelche Sentinel-Anwendungen installiert wurden.

   - **Benutzername des Betriebssystem-Sentinel-Administrators:** Die Standardeinstellung ist `esecadm`.

     Dies ist der Benutzername des Eigentümers des installierten Sentinel-Produkts. Wenn der Benutzer noch nicht existiert, wird er gemeinsam mit einem entsprechenden Basisverzeichnis im angegebenen Verzeichnis erstellt.
   - **Basisverzeichnis des Betriebssystem-Sentinel-Administrators:** Die Standardvorgabe lautet `/export/home`. Lautet der Benutzername `esecadm`, dann heißt das entsprechende Basisverzeichnis `/export/home/esecadm`.

   Um sich als Benutzer `esecadm` anmelden zu können, müssen Sie zunächst dessen Passwort festlegen.
9. Legen Sie die folgenden Werte fest:
   - **Nachrichtenbus-Port:** Der Port, den der Kommunikationsserver überwacht. Die Komponenten, die eine direkte Verbindung mit dem Kommunikationsserver herstellen, verwenden diesen Port. Die Standard-Portnummer lautet 61616.
   - **Kommunikationsserver-Hostname:** Die IP-Adresse oder der Hostname des Computers, auf dem der Sentinel Rapid Deployment-Server installiert ist.

   Stellen Sie sicher, dass die Portnummern bei allen Computern im Sentinel-System dieselben sind, damit die Kommunikation möglich ist. Notieren Sie sich diese Ports für spätere Installationen auf anderen Computern.
10. Klicken Sie auf *Weiter*.
11. Legen Sie die folgenden Werte fest:
    - **Automatische Konfiguration des Arbeitsspeichers:** Wählen Sie aus, wie viel Arbeitsspeicher dem Collector-Manager insgesamt zugewiesen werden soll. Das Installationsprogramm bestimmt automatisch die optimale Verteilung des Arbeitsspeichers unter den Komponenten und berücksichtigt dabei den geschätzten Betriebssystem- und Datenbank-Overhead.

Wichtig: Sie können den Xmx-Wert in der Datei `configuration.xml` modifizieren, um die RAM-Menge zu ändern, die dem Collector-Manager-Prozess zugewiesen wird. Die Datei `configuration.xml` wird unter Linux im Verzeichnis `<Installationsverzeichnis>/config` und unter Windows im Verzeichnis `<Installationsverzeichnis>\config` abgelegt.

- **Benutzerdefinierte Konfiguration des Arbeitsspeichers** Klicken Sie auf *Konfigurieren*, um eine Feinabstimmung der Arbeitsspeicherzuordnungen vorzunehmen. Diese Option ist nur verfügbar, wenn genügend Arbeitsspeicher auf dem Computer vorhanden ist.

12 Klicken Sie auf *Weiter*.

Eine Zusammenfassung aller zur Installation vorgesehenen Funktionen wird angezeigt.

13 Klicken Sie auf *Installieren*.

14 Nach der Installation werden Sie aufgefordert, den Benutzernamen und das Passwort einzugeben, die von der ActiveMQ-JMS-Strategie für die Herstellung einer Verbindung mit dem Broker verwendet werden.

Verwenden Sie den Benutzernamen `collectormanager` und das zugehörige Passwort, das in der Datei `<Installationsverzeichnis>/config/activemqusers.properties` auf dem Sentinel-Server zu finden ist.

Beispiel für die in der Datei `activemqusers.properties` verfügbaren Berechtigungsnachweise:

```
collectormanager=cefc76062c58e2835aa3d777778f9295
```

`collectormanager` ist der Benutzername und `cefc76062c58e2835aa3d777778f9295` ist das zugehörige Passwort.

Es wird empfohlen, für die Installation des Collector-Manager-Diensts den Benutzer collectormanager und das zugehörige Passwort zu benutzen. In diesem Fall verfügt der `collectormanager`-Benutzer nur über Zugriffsrechte auf die für den Collector-Manager-Betrieb erforderlichen Kommunikationskanäle.

Nach der Installation werden Sie aufgefordert, neu zu booten oder sich erneut anzumelden und die Sentinel-Dienste manuell zu starten.

15 Klicken Sie auf *Fertig stellen*, um das System neu zu booten.

16 Verwenden Sie bei der erneuten Anmeldung den Benutzernamen, den Sie in Schritt 8 angegeben haben.

Sollten Sie den Benutzernamen vergessen haben, öffnen Sie eine Terminal-Konsole und geben Sie als `root`-Benutzer folgenden Befehl ein:

```
env | grep ESEC_USER
```

Mit diesem Befehl wird der Benutzername zurückgegeben, wenn der Benutzer bereits erstellt wurde und die Umgebungsvariablen bereits festgelegt worden sind.

Hinweis: Bei der Installation des Collector-Managers auf der Windows 2008-Plattform und im Zusammenhang mit Collector-Manager-Images gibt es einige Probleme. Informationen zur Behebung dieser Probleme finden Sie in Anhang B, „Tipps zur Fehlersuche“, auf Seite 91.

3.4 Manuelles Starten und Anhalten der Sentinel-Dienste

Zum manuellen Starten der Sentinel-Dienste können Sie einen der folgenden Befehle verwenden:

Plattform	Befehl
Linux	`<Installationsverzeichnis>/bin/sentinel.sh start`
Windows	`<Installationsverzeichnis>/bin/sentinel.bat start`

Zum manuellen Beenden der Sentinel-Dienste können Sie einen der folgenden Befehle verwenden:

Plattform	Befehl
Linux	`<Installationsverzeichnis>/bin/sentinel.sh stop`
Windows	`<Installationsverzeichnis>/bin/sentinel.bat stop`

Sie können auch den folgenden Befehl für das Starten oder Beenden der Sentinel-Dienste verwenden.

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

3.5 Manuelle Aufrüstung von Java

Die Java-Version 1.6.0_24 ist im Installationsprogramm des Sentinel Rapid Deployment-Servers enthalten und wird während der Installation des Sentinel Rapid Deployment-Servers installiert. Wenn Sie Java auf dem Server jedoch auf die neueste Version aufrüsten, müssen Sie folgende Schritte durchführen, damit Sentinel Rapid Deployment die neueste Version verwendet:

1. Laden Sie die JRE-Bundles für das Betriebssystem herunter, auf dem der Sentinel Rapid Deployment-Server installiert ist.

   Der Benutzer, der die Aufrüstung durchführt, benötigt Schreibzugriff auf das Sentinel Rapid Deployment-Installationsverzeichnis sowie auf das Verzeichnis, in das die Aufrüstungsdateien heruntergeladen werden.

   - Wenn Sie Sentinel Rapid Deployment auf einem SUSE Linux Enterprise Server installiert haben, laden Sie sowohl 32-Bit- als auch 64-Bit-JRE-Bundles von der Java-Download-Seite (http://www.java.com/en/download/manual.jsp) herunter.

2. Benennen Sie die Ordner `jre` und `jre64` im Installationsverzeichnis von Sentinel Rapid Deployment in `jre_old` bzw. `jre64_old` um.

   ```
   cd <install_path>/sentinel_rd
   mv jre jre_old
   mv jre64 jre64_old
   ```

   Hinweis: Das Umbenennen ist erforderlich, um wieder die älteren Versionen verwenden zu können, falls die Java-Aufrüstung nicht ordnungsgemäß funktioniert. Sie können die umbenannten Ordner löschen, wenn Java nach der Aufrüstung korrekt funktioniert.

3. Extrahieren Sie die heruntergeladenen JRE-Bundles.
4. Benennen Sie den 32-Bit-Ordner in `jre` und den 64-Bit-Ordner in `jre64` um.

5 Kopieren Sie die umbenannten Ordner `jre` und `jre64` in das Installationsverzeichnis von Sentinel Rapid Deployment.

```
copy jre <install_path>/sentinel_rd/
copy jre64 <install_path>/sentinel_rd/
```

6 (Bedingt) Stellen Sie sicher, dass Sie die erforderliche Eigentümerschaft und die erforderlichen Berechtigungen der Ordner `jre` und `jre64` auf den Benutzer einstellen, der den Sentinel Rapid Deployment-Server ausführt.

7 Starten Sie den Sentinel Rapid Deployment-Server neu, starten Sie den Browser neu und prüfen Sie, ob Java korrekt installiert wurde.

3.6 Konfiguration im Anschluss an die Installation

In diesem Abschnitt erhalten Sie einen Einblick in die nach der Installation vorzunehmende Konfiguration für die Sentinel Rapid Deployment-Dienste.

3.6.1 Ändern der Datums- und Zeiteinstellungen

Das Standardformat für Datum und Uhrzeit im Sentinel Control Center kann geändert werden. Weitere Informationen zur Anpassung des Formats von Datums- und Zeitangaben auf Ihre lokale Zeitzone finden Sie auf der Java-Website (http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html).

1 Bearbeiten Sie die Datei `SentinelPreferences.properties`.

`<Installationsverzeichnis>/config/SentinelPreferences.properties`

2 Entfernen Sie den Kommentar aus der folgenden Zeile und ändern Sie das Format für die Datums- und Uhrzeitfelder von Sentinel Control Center-Ereignissen:

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

3.6.2 Konfigurieren des SMTP-Integrators für das Senden von Sentinel-Benachrichtigungen

In Sentinel Rapid Deployment arbeitet eine JavaScript SendEmail-Aktion mit einem SMTP-Integrator zusammen, um Mail-Nachrichten aus verschiedenen Kontexten innerhalb der Sentinel-Schnittstelle an die Mail-Empfänger zu senden. Der SMTP-Integrator muss mit gültigen Verbindungsinformationen konfiguriert werden, damit er ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter „Sending an E-mail“ (Senden einer Email) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

In jeder Sentinel-Installation wird automatisch eine Aktionsinstanz des Aktions-Plugins „SendEmail“ erstellt. Bis auf die Angabe der Empfänger und des Inhalts der Nachricht in den Aktionsparametern ist für die SendEmail-Aktion keine Konfiguration erforderlich.

Die SendEmail-Aktion wird intern von Sentinel ausgelöst, um in den folgenden Situationen Emails zu senden:

- Wenn eine Korrelationsregel generiert wird, wird eine SendEmail-Aktion ausgelöst. Bei der SendEmail-Aktion handelt es sich um die durch das Zahnrad symbolisierte Aktion, die nur für die Korrelation gültig ist (anders als die JavaScript-SendEmail-Aktion, zu der das JavaScript-Symbol „JS“ gehört).
- Wenn ein Workflow einen Email-Schritt oder eine Email-Aktivität enthält, der bzw. die für das Senden von Email konfiguriert ist.
- Wenn ein Benutzer einen Vorfall öffnet und eine Aktivität ausführt, die zum Senden von Email konfiguriert ist.
- Wenn ein Benutzer mit der rechten Maustaste auf ein Ereignis klickt und *Email* wählt.
- Wenn der Benutzer einen Vorfall öffnet und *Vorfall mailen* wählt.

3.6.3 Collector-Manager-Dienste

- „Installieren zusätzlicher Collector-Manager-Instanzen“ auf Seite 44
- „Arbeiten mit dem Generic Collector“ auf Seite 45

Installieren zusätzlicher Collector-Manager-Instanzen

Collector-Manager verwalten alle Datensammel- und -analyseprozesse. Manchmal ist es für den Lastausgleich zwischen Computern erforderlich, einen zusätzlichen Sentinel Collector-Manager-Knoten für eine Sentinel-Umgebung zu installieren. Remote-Collector-Manager bieten einige Vorteile:

- Sie ermöglichen eine verteilte Ereignisanalyse und -verarbeitung und tragen zur Verbesserung der Systemleistung bei.
- Sie ermöglichen die Filterung, Verschlüsselung und Datenkomprimierung auf den Quellsystemen über die Kollokation mit den Ereignisquellen. Dies reduziert die Anforderungen an die Netzwerkbandbreite und gewährleistet zusätzliche Datensicherheit.
- Sie ermöglichen die Installation auf weiteren Betriebssystemen. Beispielsweise die Installation eines Collector-Manager-Knotens auf Microsoft Windows, um die Datensammlung unter Verwendung des WMI-Protokolls zu ermöglichen.
- Sie ermöglichen das Datei-Caching, mit dessen Hilfe Remote-Collector-Manager große Datenmengen im Cache speichern können, wenn der Server vorübergehend durch das Archivieren oder Verarbeiten eines hohen Ereignisaufkommens belegt ist. Dies ist ein Vorteil bei Protokollen wie Syslog, die nicht von vornherein ein Ereignis-Caching unterstützen.

Außerdem kann für die Collector-Manager-Komponenten ein Lastausgleich durchgeführt werden, indem Instanzen dieser Komponenten auf zusätzlichen Computern installiert werden. Sie können weitere Collector-Manager installieren, indem Sie das Installationsprogramm auf einem neuen Computer ausführen. Weitere Informationen zur Installation von Collector-Managern finden Sie in Abschnitt 3.3.4, „Installieren des Sentinel Collector-Managers auf SLES oder Windows“, auf Seite 39.

Arbeiten mit dem Generic Collector

Während der Installation des Sentinel Rapid Deployment-Servers wird ein Collector mit der Bezeichnung „Generic Collector“ konfiguriert. Standardmäßig erstellt er 5 Ereignisse pro Sekunde (eps).

Weitere Collectors, die Sie für Ihr System benötigen, können Sie von der Novell Website (http://support.novell.com/products/sentinel/collectors.html) herunterladen.

3.6.4 Zeitverwaltung

Sie müssen den Sentinel-Server mit einem NTP-Server oder einen anderen Zeitserver verbinden. Wenn die Systemzeit nicht zwischen den einzelnen Computern synchronisiert ist, funktionieren Sentinel Correlation Engine und Active Views nicht ordnungsgemäß. Die Ereignisse von den Collector-Managern werden nicht als Echtzeitereignisse betrachtet und daher unter Umgehung der Sentinel Control Center und Correlation Engines nicht direkt an die Sentinel-Datenbank gesendet.

Standardmäßig liegt der Schwellwert für Echtzeit-Daten bei 120 Sekunden. Diese Vorgabe kann durch eine Änderung des Werts `esecurity.router.event.realtime.expiration` in der Datei `event-router.properties` geändert werden. Die Sentinel-Ereignisuhrzeit wird entsprechend der Uhrzeit des Trust Device oder des Collector-Managers ausgefüllt. Die Uhrzeit des Trust Device kann während der Konfiguration eines Collector ausgewählt werden. Die Uhrzeit des Trust Device ist der Zeitpunkt, an dem das Protokoll vom Gerät erstellt wurde. Die Collector-Manager-Uhrzeit ist die lokale Systemzeit des Collector-Manager-Systems.

3.7 LDAP-Authentifizierung

Sentinel Rapid Deployment unterstützt die LDAP-Authentifizierung neben der Datenbank-Authentifizierung. Sie können Benutzern erlauben, sich bei Sentinel Rapid Deployment unter Verwendung ihrer Novell eDirectory- oder Microsoft Active Directory-Berechtigung anzumelden, indem Sie einen Sentinel Rapid Deployment-Server für die LDAP-Authentifizierung konfigurieren.

- Abschnitt 3.7.1, „Überblick“, auf Seite 45
- Abschnitt 3.7.2, „Voraussetzungen“, auf Seite 46
- Abschnitt 3.7.3, „Konfigurieren des Sentinel-Servers für die LDAP-Authentifizierung“, auf Seite 47
- Abschnitt 3.7.4, „Konfigurieren mehrerer LDAP-Server zur Ausfallsicherheit“, auf Seite 50
- Abschnitt 3.7.5, „Konfigurieren der LDAP-Authentifizierung für mehrere Active Directory-Domänen“, auf Seite 52
- Abschnitt 3.7.6, „Anmeldung unter Verwendung von LDAP-Benutzerberechtigungsnachweisen“, auf Seite 53

3.7.1 Überblick

Sie können den Sentinel Rapid Deployment-Server für die LDAP-Authentifizierung über eine sichere SSL-Verbindung konfigurieren. Dabei kann die Verwendung anonymer Suchen im LDAP-Verzeichnis zugelassen oder nicht zugelassen werden.

Hinweis: Sollte die anonyme Suche im LDAP-Verzeichnis nicht möglich sein, dürfen Sie auch den Sentinel Rapid Deployment-Server nicht für die Verwendung der anonymen Suche konfigurieren.

- **Anonyme Suche:** Wenn Sie LDAP-Benutzerkonten für Sentinel Rapid Deployment erstellen, müssen Sie den Verzeichnisbenutzernamen angeben. Es ist nicht notwendig, den eindeutigen Benutzernamen (DN) anzugeben.

  Wenn sich der LDAP-Benutzer bei Sentinel Rapid Deployment anmeldet, führt der Sentinel Rapid Deployment-Server basierend auf dem angegebenen Benutzernamen eine anonyme Suche im LDAP-Verzeichnis durch, findet den zugehörigen DN und authentifiziert die Benutzeranmeldung im LDAP-Verzeichnis unter Verwendung des DN.

- **Nicht-anonyme Suche:** Wenn Sie LDAP-Benutzerkonten für Sentinel Rapid Deployment erstellen, müssen Sie den Verzeichnisbenutzernamen und den eindeutigen Benutzernamen (DN) angeben.

  Wenn sich der LDAP-Benutzer bei Sentinel Rapid Deployment anmeldet, authentifiziert der Sentinel Rapid Deployment-Server die Benutzeranmeldung im LDAP-Verzeichnis unter Verwendung des angegebenen Benutzer-DN und führt keine anonyme Suche im LDAP-Verzeichnis durch.

  Für Active Directory steht eine weitere Methode zur Verfügung. Weitere Informationen finden Sie unter Nicht-anonyme LDAP-Authentifizierung unter Verwendung des UserPrincipalName-Attributs in Active Directory.

3.7.2 Voraussetzungen

- „Exportieren des LDAP-Server-CA-Zertifikats“ auf Seite 46
- „Aktivieren der anonymen Suche im LDAP-Verzeichnis“ auf Seite 46

Exportieren des LDAP-Server-CA-Zertifikats

Die sichere SSL-Verbindung zum LDAP-Server erfordert das LDAP-Server-CA-Zertifikat, das Sie in eine Base64-kodierte Datei exportieren müssen.

- **eDirectory:** Weitere Informationen hierzu finden Sie unter Exporting an Organizational CA's Self-Signed Certificate (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html) (Exportieren eines von einer Zertifizierungsstelle der Organisation selbst signierten Zertifikats).

  Um ein eDirectory-CA-Zertifikat in iManager exportieren zu können, müssen die Novell Certificate Server-Plugins für iManager installiert sein.

- **Active Directory:** Weitere Informationen hierzu finden Sie unter Aktivieren von LDAP über SSL mit einer Fremdanbieter-Zertifizierungsstelle (http://support.microsoft.com/kb/321051).

Aktivieren der anonymen Suche im LDAP-Verzeichnis

Um die LDAP-Authentifizierung unter Verwendung der anonymen Suche durchführen zu können, muss diese im LDAP-Verzeichnis aktiviert werden. Standardmäßig ist die anonyme Suche in eDirectory aktiviert und in Active Directory deaktiviert.

Beachten Sie Folgendes, wenn Sie die anonyme Suche im LDAP-Verzeichnis aktiveren möchten:

- **eDirectory:** Lesen Sie die Informationen zu ldapBindRestrictions im Abschnitt Attributes on the LDAP Server Object (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html) (Attribute des LDAP-Serverobjekts).
- **Active Directory:** Das Benutzerobjekt „ANONYMOUS LOGON“ muss mit ausreichenden Berechtigungen für den Listen- und Lesezugriff auf die Attribute `sAMAccountName` und `objectclass` ausgestattet sein. Weitere Informationen finden Sie unter Konfigurieren von Active Directory, um anonyme Abfragen zu ermöglichen (http://support.microsoft.com/kb/320528).

  Für Windows Server 2003 ist zusätzlicher Konfigurationsaufwand erforderlich. Weitere Informationen finden Sie unter Configuring Active Directory on Windows Server 2003 (http://support.microsoft.com/kb/326690/en-us) (Konfigurieren von Active Directory auf Windows Server 2003).

3.7.3 Konfigurieren des Sentinel-Servers für die LDAP-Authentifizierung

1. Stellen Sie sicher, dass Sie die in Abschnitt 3.7.2, „Voraussetzungen“, auf Seite 46 aufgeführten Voraussetzungen erfüllen.
2. Melden Sie sich beim Sentinel Rapid Deployment-Server als `root`-Benutzer an.
3. Kopieren Sie die Datei mit dem exportierten LDAP-Server-CA-Zertifikat in das Verzeichnis `<Installationsverzeichnis>/config`.
4. Definieren Sie den Eigentümer der Zertifikatdatei und die Zugriffsrechte darauf:

   ```
   chown novell:novell <Installationsverzeichnis>/config/<cert-file>
   chmod 700 <Installationsverzeichnis>/config/<cert-file>
   ```
5. Wechseln Sie zum Benutzer `novell`:

   ```
   su - novell
   ```
6. Wechseln Sie in das Verzeichnis `<Installationsverzeichnis>/bin`.
7. Führen Sie das Skript für die Konfiguration der LDAP-Authentifizierung aus:

   ```
   ./ldap_auth_config.sh
   ```

   Das Skript sichert die Konfigurationsdateien `auth.login` und `configuration.xml` im Verzeichnis `config` als `auth.login.sav` und `configuration.xml.sav`, bevor sie für die LDAP-Authentifizierung geändert werden.
8. Legen Sie die folgenden Werte fest:

   Drücken Sie die Eingabetaste, um den Standardwert zu übernehmen, oder geben Sie einen neuen Wert ein, der den vorgegebenen Wert überschreibt.

   - **Sentinel install location (Sentinel-Installationsverzeichnis):** Das Installationsverzeichnis auf dem Sentinel-Server.
   - **LDAP server hostname or IP address (Hostname oder IP-Adresse des LDAP-Servers):** Der Hostname bzw. die IP-Adresse des Computers, auf dem der LDAP-Server installiert ist. Der Standardwert ist „localhost“. Der LDAP-Server sollte jedoch nicht auf demselben Computer wie der Sentinel Log Manager-Server installiert sein.
   - **LDAP server port (LDAP-Server-Port):** Die Portnummer für die sichere LDAP-Verbindung. Die Standard-Portnummer lautet 636.

- **Anonymous searches on LDAP directory (Anonyme Suchen im LDAP-Verzeichnis):**

  Geben Sie `y` ein, wenn anonyme Suchen möglich sein sollen. Anderenfalls geben Sie `n` ein. Der Standardwert ist `y`.

  Wenn Sie `n` angeben, führen Sie die LDAP-Konfiguration und die Schritte durch, die in Abschnitt „LDAP-Authentifizierung ohne anonyme Suchen“ auf Seite 49 beschrieben sind.

- **LDAP Directory used (Verwendetes LDAP-Verzeichnis):** Dieser Parameter wird nur dann angezeigt, wenn Sie anonyme Suchen zugelassen haben. Geben Sie „1“ für Novell eDirectory oder „2“ für Active Directory ein. Der Standardwert ist 1.

- **LDAP subtree to search for users (Nach Benutzern zu durchsuchender LDAP-Teilbaum):** Dieser Parameter wird nur dann angezeigt, wenn Sie anonyme Suchen zugelassen haben. Der Teilbaum im Verzeichnis, der die Benutzerobjekte enthält. Die folgenden Beispiele zeigen, wie Teilbäume in eDirectory und Active Directory angegeben werden:

  - eDirectory:

    ```
    ou=users,o=novell
    ```

    Hinweis: Wird in eDirectory kein Teilbaum angegeben, wird die Suche im gesamten Verzeichnis durchgeführt.

  - Active Directory:

    ```
    CN=users,DC=TESTAD,DC=provo, DC=novell,DC=com
    ```

    Hinweis: Bei Active Directory muss der Teilbaum angegeben werden.

- **Filename of the LDAP server certificate (Dateinamen des LDAP-Server-Zertifikats):** Der Dateiname des Zertifizierungsstellenzertifikats für eDirectory bzw. Active Directory CA, das Sie in Schritt 3 kopiert haben.

9 Geben Sie einen der folgenden Befehle ein:

- `y`, um die eingegebenen Werte zu übernehmen
- `n`, um neue Werte einzugeben
- `q`, um die Konfiguration abzubrechen

Bei erfolgreicher Konfiguration:

- Das LDAP-Server-Zertifikat wird dem Keystore `<Installationsverzeichnis>/config/ldap_server.keystore` hinzugefügt.
- Die Konfigurationsdateien `auth.login` und `configuration.xml` im Verzeichnis `<Installationsverzeichnis>/config` werden aktualisiert, um die LDAP-Authentifizierung zuzulassen.

10 Geben Sie `y` ein, um den Sentinel-Dienst erneut zu starten.

Wichtig: Sollten Fehler auftreten, machen Sie die Änderungen rückgängig, die Sie an den Konfigurationsdateien `auth.login` und `configuration.xml` im Verzeichnis `config` vorgenommen haben:

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

11 (Bedingt) Wenn Sie `n` für Anonymous searches on LDAP directory (Anonyme Suchen im LDAP-Verzeichnis): angegeben haben, fahren Sie mit „LDAP-Authentifizierung ohne anonyme Suchen“ auf Seite 49 fort.

LDAP-Authentifizierung ohne anonyme Suchen

Wenn Sie bei der Konfiguration von Sentinel Rapid Deployment für die LDAP-Authentifizierung festgelegt haben, dass anonymen Suchen im LDAP-Verzeichnis nicht zulässig sind, führt die LDAP-Authentifizierung keine anonymen Suchen durch.

Wenn Sie das LDAP-Benutzerkonto über das Sentinel Control Center erstellen, müssen Sie für die nicht-anonyme LDAP-Authentifizierung die *LDAP-Benutzer-DN* angeben. Sie können diesen Ansatz sowohl für eDirectory als auch für Active Directory verwenden.

Weitere Informationen finden Sie unter „Creating an LDAP User Account for Sentinel“ (Erstellen eines LDAP-Benutzerkontos) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

Darüber hinaus gibt es für Active Directory einen alternativen Ansatz zur Durchführung der LDAP-Authentifizierung ohne anonyme Suchvorgänge. Weitere Informationen finden Sie in Nicht-anonyme LDAP-Authentifizierung unter Verwendung des UserPrincipalName-Attributs in Active Directory.

Nicht-anonyme LDAP-Authentifizierung unter Verwendung des UserPrincipalName-Attributs in Active Directory

In Active Directory können Sie LDAP-Authentifizierung ohne anonyme Suchen auch mithilfe des Attributs „userPrinicipalName“ durchführen:

1 Stellen Sie sicher, dass das userPrinicipalName-Attribut für den Active Directory-Benutzer mit <*sAMAccountName@domain*> definiert ist.

   Weitere Informationen finden Sie unter User-Principal-Name Attribute (http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx).

2 Stellen Sie sicher, dass Sie die Schritte Schritt 1 auf Seite 47 bis Schritt 10 auf Seite 48 durchgeführt und bei der Eingabeaufforderung „Anonymous searches on LDAP directory (Anonyme Suchen im LDAP-Verzeichnis):“ auf Seite 48 ein `n` eingegeben haben.

3 Bearbeiten Sie auf dem Sentinel-Server den Abschnitt `LdapLogin` in der Datei `<Installationsverzeichnis>/config/auth.login`:

```
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;
 };
```

   Beispiel:

```
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 Starten Sie den Sentinel-Dienst neu:

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

3.7.4 Konfigurieren mehrerer LDAP-Server zur Ausfallsicherheit

So konfigurieren Sie einen oder mehrere LDAP-Server als Failover-Server für die LDAP-Authentifizierung:

1 Stellen Sie sicher, dass die Schritte Schritt 2 auf Seite 47 bis Schritt 10 auf Seite 48 zur Konfiguration des Sentinel-Servers für die LDAP-Authentifizierung über den primären LDAP-Server durchgeführt wurden.

2 Melden Sie sich beim Sentinel-Server als der Benutzer `novell` an.

3 Beenden Sie den Sentinel-Dienst.

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

4 Wechseln Sie in das Verzeichnis `<Installationsverzeichnis>/config`.

```
cd <Installationsverzeichnis>/config
```

5 Öffnen Sie die Datei `auth.login` zum Bearbeiten.

```
vi auth.login
```

6 Aktualisieren Sie den Parameter `userProvider` im Abschnitt „LdapLogin“ und geben Sie mehrere LDAP-URLs an. Trennen Sie die URLs durch ein Leerzeichen.

Beispiel:

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

Bei Active Directory darf der Teilbaum in der LDAP-URL nicht leer sein.

Weitere Informationen zur Angabe mehrerer LDAP-URLs finden Sie in der Beschreibung der Option `userProvider` unter Class LdapLoginModule (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

7 Speichern Sie die Änderungen.

8 Exportieren Sie das Zertifikat für jeden Failover-LDAP-Server und kopieren Sie die Zertifikatdatei in das Verzeichnis `<Installationsverzeichnis>/config` auf dem Sentinel-Server.

Weitere Informationen finden Sie unter „Exportieren des LDAP-Server-CA-Zertifikats“ auf Seite 46.

9 Stellen Sie sicher, dass die Zertifikatdatei für jeden Failover-LDAP-Server mit den notwendigen Einstellungen für Eigentümerschaft und Berechtigungen versehen ist.

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

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

10 Fügen Sie jedes Failover-LDAP-Server-Zertifikat dem Keystore `ldap_server.keystore` zu, der in Schritt 8 im Abschnitt „Konfigurieren des Sentinel-Servers für die LDAP-Authentifizierung“ auf Seite 47 erstellt wird.

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

Ersetzen Sie `<certificate-file>` durch den Namen der Datei mit dem LDAP-Zertifikat im Base64-verschlüsselten Format und `<alias_name>` durch den Aliasnamen für das zu importierende Zertifikat.

Wichtig: Die Angabe des Aliasnamens ist erforderlich. Wird kein Aliasname angegeben, verwendet das Keytool standardmäßig `mykey` als Aliasnamen. Wenn Sie mehrere Zertifikate in den Keystore importieren, ohne einen Aliasnamen anzugeben, meldet das Keytool als Fehler, dass der Aliasname bereits vorhanden ist.

---

11 Starten Sie den Sentinel-Dienst.

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

Der Dienst stellt möglicherweise keine Verbindung zu dem Failover-LDAP-Server her, wenn auf dem Sentinel-Server eine Zeitüberschreitung stattfindet, bevor er feststellt, dass der primäre LDAP-Server nicht zur Verfügung steht. So stellen Sie sicher, dass der Sentinel-Server ohne Zeitüberschreitung eine Verbindung zu dem Failover-LDAP-Server herstellt:

1 Melden Sie sich beim Sentinel-Server als `root`-Benutzer an.

2 Öffnen Sie die Datei `sysct1.conf` zum Bearbeiten:

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

3 Stellen Sie sicher, dass der `net.ipv4.tcp_syn_retries` den Wert „3“ hat. Wenn der Eintrag nicht vorhanden ist, fügen Sie ihn hinzu. Speichern Sie die Datei:

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

4 Führen Sie die Befehle aus, damit die Änderungen wirksam werden:

```
/sbin/sysctl -p
```

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

5 Definieren Sie den Zeitüberschreitungswert für den Sentinel-Server, indem Sie in den Dateien `control_center.sh` und `solution_designer.sh` im Verzeichnis `<Installationsverzeichnis>/bin` den Parameter `-Desecurity.remote.timeout=60` hinzufügen:

control_center.sh:

```
"<Installationsverzeichnis>/jre/bin/java" $MEMORY -
Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
Desecurity.cache.directory="<Installationsverzeichnis>/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="<Installationsverzeichnis>/config/
control_center_log.prop" -
Djava.security.auth.login.config="<Installationsverzeichnis>/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:

```
"<Installationsverzeichnis>/jre/bin/java" -classpath $LOCAL_CLASSPATH
$MEMORY -Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
Dsentinel.installer.jar.location="<Installationsverzeichnis>/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="<Installationsverzeichnis>/config/
solution_designer_log.prop" -
Djava.security.auth.login.config="<Installationsverzeichnis>/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
```

3.7.5 Konfigurieren der LDAP-Authentifizierung für mehrere Active Directory-Domänen

Wenn sich die zu authentifizierenden LDAP-Benutzer in mehreren Active Directory-Domänen befinden, können Sie den Sentinel Rapid Deployment-Server wie folgt für die LDAP-Authentifizierung konfigurieren:

1. Stellen Sie sicher, dass Sie Schritt 2 auf Seite 47 bis Schritt 10 auf Seite 48 durchgeführt haben, um den Sentinel-Server für die LDAP-Authentifizierung anhand des Active Directory-Domänencontrollers der ersten Domäne zu konfigurieren. Stellen Sie außerdem sicher, dass Sie `n` für „Anonymous searches on LDAP directory (Anonyme Suchen im LDAP-Verzeichnis):“ auf Seite 48 angegeben haben.
2. Melden Sie sich beim Sentinel-Server als der Benutzer `novell` an.
3. Beenden Sie den Sentinel-Dienst.

   ```
   /etc/init.d/sentinel stop
   ```
4. Wechseln Sie in das Verzeichnis `<Installationsverzeichnis>/config`.

   ```
   cd <Installationsverzeichnis>/config
   ```
5. Öffnen Sie die Datei `auth.login` zum Bearbeiten.

   ```
   vi auth.login
   ```
6. Geben Sie im Abschnitt `LdapLogin` mehrere LDAP-URL-Adressen, jeweils durch ein Leerzeichen getrennt, ein.

   Beispiel:

   ```
   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;
   };
   ```

   Weitere Informationen zur Angabe mehrerer LDAP-URLs finden Sie in der Beschreibung der Option `userProvider` unter Class LdapLoginModule (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).
7. Speichern Sie die Änderungen.

8 Exportieren Sie das Zertifikat des Domänencontrollers jeder Domäne und kopieren Sie die Zertifikatsdateien in das Verzeichnis `<Installationsverzeichnis>/config` auf dem Sentinel-Server.

   Weitere Informationen finden Sie in „Exportieren des LDAP-Server-CA-Zertifikats“ auf Seite 46.

9 Achten Sie darauf, die erforderliche Eigentümerschaft und die erforderlichen Berechtigungen der Zertifikatsdateien festzulegen.

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

10 Fügen Sie jedes Zertifikat dem Keystore `ldap_server.keystore` zu, der in Schritt 8 im Abschnitt „Konfigurieren des Sentinel-Servers für die LDAP-Authentifizierung“ auf Seite 47 erstellt wird.

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

   Ersetzen Sie `<certificate-file>` durch den Namen der Datei mit dem LDAP-Zertifikat im Base64-verschlüsselten Format und `<alias_name>` durch den Aliasnamen für das zu importierende Zertifikat.

Wichtig: Die Angabe des Aliasnamens ist erforderlich. Wird kein Aliasname angegeben, verwendet das Keytool standardmäßig `mykey` als Aliasnamen. Wenn Sie mehrere Zertifikate in den Keystore importieren, ohne einen Aliasnamen anzugeben, meldet das Keytool als Fehler, dass der Aliasname bereits vorhanden ist.

---

11 Starten Sie den Sentinel-Dienst.

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

3.7.6 Anmeldung unter Verwendung von LDAP-Benutzerberechtigungsnachweisen

Nachdem Sie den Sentinel-Server für die LDAP-Authentifizierung konfiguriert haben, können Sie im Sentinel Control Center LDAP-Benutzerkonten erstellen. Weitere Informationen finden Sie unter „Creating an LDAP User Account for Sentinel“ (Erstellen eines LDAP-Benutzerkontos) im *Sentinel Rapid Deployment User Guide (Sentinel Rapid Deployment-Benutzerhandbuch).*

Wurde das LDAP-Benutzerkonto erstellt, können Sie sich bei der Weboberfläche von Sentinel Rapid Deployment, beim Sentinel Control Center und beim Sentinel Solution Designer mit Ihrem LDAP-Benutzernamen und -Passwort anmelden.

Hinweis: Soll die vorhandene LDAP-Konfiguration geändert werden, können Sie das Skript `ldap_auth_config` erneut ausführen und andere Parameterwerte angeben.

3.8 Aktualisieren des Lizenzschlüssels von einem Evaluierungsschlüssel zu einem Produktionsschlüssel

Wenn Sie dieses Produkt nach der Evaluation erwerben, sollten Sie den Lizenzschlüssel im System mit dem unten angegebenen Verfahren aktualisieren, damit keine erneute Installation erforderlich ist:

1. Melden Sie sich bei dem Computer, auf dem Sentinel Rapid Deployment installiert ist, als der Betriebssystembenutzer für den Sentinel Administrator an (der Standardbenutzername ist `novell`).
2. Wechseln Sie an der Eingabeaufforderung in das Verzeichnis `<Installationsverzeichnis>/bin`.
3. Geben Sie den folgenden Befehl ein:

   ```
   ./softwarekey.sh
   ```
4. Geben Sie 1 an, um den Primärschlüssel zu definieren. Drücken Sie die Eingabetaste.
5. Geben Sie den neuen gültigen Lizenzschlüssel an und befolgen Sie die Anweisungen auf dem Bildschirm, um den Vorgang nach der Aktualisierung des Lizenzschlüssels zu beenden.

Aktualisierung von Sentinel Rapid Deployment

4

Dieser Abschnitt enthält Informationen zur Aktualisierung einer vorhandenen Version von Sentinel Rapid Deployment mit dem neuesten Patch.

Hinweis: Dieser Patch steht nur für eine 64-Bit-Installation von Sentinel Rapid Deployment zur Verfügung. Die Anwendung dieses Patches auf einem 32-Bit-Demosystem führt zu einer nicht funktionsfähigen Installation.

4.1 Voraussetzungen

- Stellen Sie sicher, dass auf dem System, das Sie aktualisieren, bereits Sentinel 6.1 Rapid Deployment SP1 installiert ist.
- Stellen Sie sicher, dass Sentinel Data Manager-Aufträge aktiviert sind, damit die Partition „Aktuelle Elemente online“ nie den Wert „P_MAX“ erreicht. Falls der P_MAX-Wert erreicht wird und Sie manuell Partitionen hinzufügen, startet Sentinel Control Center nicht.

4.2 Installation des Patches auf dem Server

1 Melden Sie sich bei dem Server, auf dem Sie den Patch installieren möchten, als `novell`-Benutzer an.

Sichern Sie vor der Installation des Patches mittels folgender Befehle die Sentinel-Datenbank, den Konfigurations- und den Datenordner:

Sentinel-Datenbank:

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

Konfigurationsordner:

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

Datenordner:

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

Weitere Informationen zu diesen Befehlen finden Sie unter File system level back up (http://www.postgresql.org/docs/8.1/static/backup-file.html) (Sicherung auf Dateisystemebene) auf der PostgreSQL-Website.

2 Sichern Sie die ESM-Konfiguration und erstellen Sie einen ESM-Export.

Weitere Informationen finden Sie unter „Exporting a Configuration“ (Exportieren einer Konfiguration) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

3. Laden Sie das Patch-Installationsprogramm für Sentinel Rapid Deployment von der Webseite Novell Patch Finder (http://download.novell.com/patch/finder/) herunter.
4. Kopieren Sie das heruntergeladene Installationspaket in ein temporäres Verzeichnis.
5. Beenden Sie die Sentinel-Dienste:

   ```
   sentinel.sh stop
   ```
6. Geben Sie den folgenden Befehl ein, um die Dateien im Installationspaket zu extrahieren:

   ```
   unzip <install_filename>
   ```

   Ersetzen Sie <*install_filename*> durch den tatsächlichen Namen der Installationsdatei.
7. Wechseln Sie in das Verzeichnis, in das Sie die Dateien des Installationsprogramms extrahiert haben:

   ```
   cd <directory_name>
   ```

   Ersetzen Sie <*directory_name*> durch den Namen des Verzeichnisses, in das Sie die Dateien extrahiert haben.
8. Geben Sie den folgenden Befehl zur Installation des Patches auf dem Server an und befolgen Sie anschließend die Bildschirmanweisungen:

   ```
   ./service_pack.sh
   ```

   Nach der Installation starten die Sentinel-Dienste automatisch.
9. Wenden Sie den Patch auf allen Computern an, auf denen Collector-Manager und/oder Client-Anwendungen laufen.

4.3 Aktualisieren des Collector-Managers und der Client-Anwendungen

4.3.1 Aktualisieren des Collector-Managers

Linux

1. Melden Sie sich bei dem Computer mit dem Sentinel Rapid Deployment Collector-Manager als `root`-Benutzer an.
2. Laden Sie das Patch-Installationsprogramm für Sentinel Rapid Deployment von der Webseite Novell Patch Finder (http://download.novell.com/patch/finder/) herunter.
3. Kopieren Sie die heruntergeladene Datei in ein temporäres Verzeichnis.
4. Geben Sie den folgenden Befehl ein, um die Dateien im Installationspaket zu extrahieren:

   ```
   unzip <install_filename>
   ```

   Ersetzen Sie <*install_filename*> durch den tatsächlichen Namen der Installationsdatei.

5 Wechseln Sie in das Verzeichnis, in das Sie die Dateien des Installationsprogramms extrahiert haben:

```
cd <directory_name>
```

Ersetzen Sie <*directory_name*> durch den Namen des Verzeichnisses, in das Sie die Dateien des Installationsprogramms extrahiert haben.

6 Beenden Sie die Collector-Manager-Dienste.

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

7 Führen Sie das Installationsprogramm für das Service Pack aus und befolgen Sie die Anweisungen auf dem Bildschirm:

```
./service_pack.sh
```

Nach der Installation starten die Collector-Manager-Dienste automatisch.

Windows

1 Melden Sie sich bei dem Computer mit dem Sentinel Rapid Deployment Collector-Manager als ein Admin-Benutzer an.

2 Laden Sie das Patch-Installationsprogramm für Sentinel Rapid Deployment von der Webseite Novell Patch Finder (http://download.novell.com/patch/finder/) herunter.

3 Kopieren Sie die Installationsprogrammdatei in ein temporäres Verzeichnis.

4 Extrahieren Sie die Dateien in dem Installationspaket.

5 Beenden Sie die Collector-Manager-Dienste.

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

6 Navigieren Sie zu dem Verzeichnis, in das Sie die Dateien des Installationsprogramms extrahiert haben.

7 Wählen Sie eine der folgenden Vorgehensweisen, um das Installationsprogramm zu starten:

- Doppelklicken Sie auf die Datei `service_pack.bat` und befolgen Sie die Anweisungen auf dem Bildschirm.
- Starten Sie die Datei `service_pack.bat` von einer Eingabeaufforderung aus und befolgen Sie die Anweisungen auf dem Bildschirm.

Nach der Installation starten die Collector-Manager-Dienste automatisch.

4.3.2 Aktualisieren der Client-Anwendungen

- „Linux“ auf Seite 57
- „Windows“ auf Seite 58

Linux

1 Melden Sie sich bei dem Computer, auf dem die Client-Anwendungen von Novell Sentinel Rapid Deployment laufen, als `root`-Benutzer an.

2 Laden Sie das Patch-Installationsprogramm für Sentinel Rapid Deployment von der Webseite Novell Patch Finder (http://download.novell.com/patch/finder/) herunter.

3 Kopieren Sie das heruntergeladene Installationspaket in ein temporäres Verzeichnis.

4 Geben Sie den folgenden Befehl ein, um die Dateien im Installationspaket zu extrahieren:

```
unzip <install_filename>
```

Ersetzen Sie <*install_filename*> durch den tatsächlichen Namen der Installationsdatei.

5 Wechseln Sie in das Verzeichnis, in das Sie die Dateien des Installationsprogramms extrahiert haben:

```
cd <directory_name>
```

Ersetzen Sie <*directory_name*> durch den Namen des Verzeichnisses, in das Sie die Dateien extrahiert haben.

6 Führen Sie das Installationsprogramm aus und befolgen Sie die Anweisungen auf dem Bildschirm:

```
./service_pack.sh
```

Windows

1 Melden Sie sich bei dem Computer, auf dem die Client-Anwendungen von Novell Sentinel Rapid Deployment laufen, als Administrator an.

2 Laden Sie das Patch-Installationsprogramm für Sentinel Rapid Deployment von der Webseite Novell Patch Finder (http://download.novell.com/patch/finder/) herunter.

3 Kopieren Sie die heruntergeladene Datei in ein temporäres Verzeichnis.

4 Extrahieren Sie die Dateien in dem Installationspaket.

5 Navigieren Sie zu dem Verzeichnis, in das Sie die Dateien des Installationsprogramms extrahiert haben.

6 Wählen Sie eine der folgenden Vorgehensweisen, um das Installationsprogramm zu starten:

- Doppelklicken Sie auf die Datei `service_pack.bat` und befolgen Sie die Anweisungen auf dem Bildschirm.
- Starten Sie die Datei `service_pack.bat` von einer Eingabeaufforderung aus und befolgen Sie die Anweisungen auf dem Bildschirm.

Sicherheitsüberlegungen für Sentinel Rapid Deployment

5

Dieser Abschnitt enthält spezielle Anweisungen für die sichere Installation, Konfiguration und Wartung von Novell Sentinel Rapid Deployment.

5.1 Erhöhen der Systemsicherheit

5.1.1 Schließen von Sicherheitslücken

- Alle nicht benötigten Ports werden ausgeschaltet.
- Wenn möglich, überwacht ein Dienste-Port nur lokale Verbindungen und lässt keine Remote-Verbindungen zu.
- Dateien werden mit den geringstmöglichen Zugriffsrechten installiert, sodass nur eine kleine Zahl von Benutzern diese Dateien lesen kann.
- Standardpasswörter sind nicht erlaubt.
- Datenbankberichte werden unter einem Benutzer ausgeführt, der nur bestimmte Zugriffsrechte für die Datenbank besitzt.
- Alle Webschnittstellen erfordern HTTPS.
- Es werden eine Schwachstellenprüfung auf die Anwendung ausgeführt und alle potenziellen Sicherheitsprobleme bearbeitet.
- Jede Kommunikation über das Netzwerk verwendet standardmäßig SSL und ist für die Authentifizierung konfiguriert.
- Passwörter für Benutzerkonten werden standardmäßig verschlüsselt, wenn sie im Dateisystem oder in der Datenbank gespeichert werden.

5.1.2 Sichern der Sentinel Rapid Deployment-Daten

Aufgrund des hochsensiblen Charakters der Daten in Sentinel Rapid Deployment muss der Computer physisch geschützt und in einem sicheren Bereich des Netzwerks betrieben werden.Verwenden Sie einen remoten Collector-Manager, um Daten von Ereignisquellen außerhalb des sicheren Netzwerks zu sammeln. Weitere Informationen zu remote betriebenen Collector-Managern finden Sie in „Abschnitt 3.3, „Installieren des Collector-Managers und der Sentinel-Client-Anwendungen“, auf Seite 35“.

5.2 Sichern der Kommunikation im gesamten Netzwerk

Die Kommunikation zwischen den verschiedenen Komponenten von Sentinel Rapid Deployment erfolgt über das Netzwerk, und im gesamten Netzwerk werden verschiedene Arten von Kommunikationsprotokollen verwendet.

5.2.1 Kommunikation zwischen Sentinel-Serverprozessen

Zu den Sentinel-Serverprozessen zählen DAS Core, DAS Binary, Correlation Engine, Collector-Manager und der Webserver. Sie kommunizieren untereinander über ActiveMQ.

Die Kommunikation zwischen diesen Serverprozessen erfolgt standardmäßig per SSL über den ActiveMQ-Nachrichtenbus. Für die Konfiguration von SSL geben Sie in der Datei `<Installationsverzeichnis>/configuration.xml` folgende Informationen an:

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

Weitere Informationen zum Einrichten benutzerdefinierter Server- und Client-Zertifikate finden Sie unter „Processes“ (Prozesse) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

5.2.2 Kommunikation zwischen dem Sentinel-Server und den Sentinel-Client-Anwendungen

Die Sentinel-Client-Anwendungen wie das Sentinel Control Center (SCC), der Sentinel Data Manager (SDM) und der Solution Designer nutzen standardmäßig die SSL-Kommunikation über den SSL-Proxyserver.

Geben Sie zur Aktivierung der Kommunikation zwischen dem Sentinel-Server und SCC, dem SDM und dem Solution Designer, wenn diese auf dem Server alle als Client-Anwendungen ausgeführt werden, in der Datei `<Installationsverzeichnis>/configuration.xml` folgende Informationen an:

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

Zur Aktivierung der Kommunikation zwischen dem Sentinel-Server, dem SCC, dem SDM und dem Solution Designer, die über Web Start ausgeführt werden, wird die Kommunikationsstrategie auf dem Server in der Datei `<Installationsverzeichnis>/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml` folgendermaßen festgelegt:

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

Weitere Informationen zum Einrichten benutzerdefinierter Server- und Client-Zertifikate finden Sie unter „Processes“ (Prozesse) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

5.2.3 Kommunikation zwischen Server und Datenbank

Das für die Kommunikation zwischen dem Server und der Datenbank verwendete Protokoll wird vom JDBC-Treiber definiert. Einige Treiber sind in der Lage, die Kommunikation mit der Datenbank zu verschlüsseln.

Sentinel Rapid Deployment verwendet für die Verbindung mit der PostgreSQL-Datenbank, einer Java-Implementierung (Typ 4), den PostgreSQL-Treiber (`postgresql-<Version>.jdbc3.jar`), der auf der PostgreSQL-Download-Webseite (http://jdbc.postgresql.org/download.html) verfügbar ist. Dieser Treiber unterstützt die Verschlüsselung der Datenkommunikation. Informationen zur Verschlüsselung der Datenkommunikation finden Sie unter PostgreSQL-Verschlüsselungsoptionen (http://www.postgresql.org/docs/8.1/static/encryption-options.html).

Hinweis: Das Aktivieren der Verschlüsselung wirkt sich auf die Systemleistung aus. Daher erfolgt die Kommunikation mit der Datenbank standardmäßig unverschlüsselt. Dies ist jedoch kein Sicherheitsproblem, da die Kommunikation zwischen der Datenbank und dem Server über die Loopback-Netzwerkschnittstelle stattfindet und deshalb nicht mit dem offenen Netzwerk in Berührung kommt.

5.2.4 Kommunikation zwischen den Collector-Managern und den Ereignisquellen

Sie können Sentinel Rapid Deployment für die sichere Sammlung von Daten aus verschiedenen Ereignisquellen konfigurieren. Jedoch wird die Sicherung der Datensammlung durch die spezifischen, von der Ereignisquelle unterstützten Protokolle bestimmt. So können beispielsweise Check Point LEA, Syslog und Audit Connectors für die Verschlüsselung der Kommunikation mit den Ereignisquellen konfiguriert werden.

Weitere Informationen zu den möglichen Sicherheitsfunktionen, die aktiviert werden können, finden Sie in der Dokumentation zu Connectors und Ereignisquellen auf der Novell Sentinel Plugins-Website (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

5.2.5 Kommunikation mit Webbrowsern

Der Webserver ist standardmäßig zur Kommunikation über HTTPS konfiguriert. Weitere Informationen finden Sie in der Tomcat-Dokumentation (http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html).

5.2.6 Kommunikation zwischen der Datenbank und anderen Clients

Sie können die PostgreSQL-SIEM-Datenbank so konfigurieren, dass Verbindungen von allen Client-Computern zugelassen werden. Dazu verwenden Sie den Sentinel Data Manager oder eine Drittanbieteranwendung, z. B. Pgadmin.

Um dem Sentinel Data Manager die Verbindung von jedem Client-Computer aus zu erlauben, fügen Sie in die Datei `<Installationsverzeichnis>/3rdparty/postgresql/data/pg_hba.conf` folgende Zeile ein:

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

Wenn Sie die Client-Verbindungen einschränken möchten, die durchgeführt werden dürfen und über den SDM mit der Datenbank Verbindung aufnehmen können, dann ersetzen Sie die oben angegebene Zeile durch die IP-Adresse des Hosts. Die folgende Zeile in der Datei `pg_hba.conf` weist PostgreSQL an, nur Verbindungen vom lokalen Computer zu akzeptieren, sodass der SDM nur auf dem Server ausgeführt werden darf.

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

Um die Verbindungen von anderen Client-Computern einzuschränken, können Sie zusätzliche `host`-Einträge hinzufügen.

5.3 Sichern von Benutzern und Passwörtern

- Abschnitt 5.3.1, „Betriebssystembenutzer“, auf Seite 63
- Abschnitt 5.3.2, „Sentinel-Anwendungs- und Datenbankbenutzer“, auf Seite 63
- Abschnitt 5.3.3, „Erzwingen der Einhaltung einer Passwortrichtlinie für Benutzer“, auf Seite 64

5.3.1 Betriebssystembenutzer

- „Server-Installation“ auf Seite 63
- „Installation von Collector-Manager“ auf Seite 63

Server-Installation

Bei der Server-Installation von Sentinel Rapid Deployment werden der Systembenutzer und eine Gruppe erstellt, die Eigentümer der installierten Dateien im *<Installationsverzeichnis>* sind. Wenn der Benutzer nicht vorhanden ist, dann wird er erstellt und sein Basisverzeichnis wird auf *<Installationsverzeichnis>* festgelegt. Wenn ein neuer Benutzer erstellt wird, wird das Passwort aus Sicherheitsgründen nicht standardmäßig festgelegt. Wenn Sie sich bei dem System als der Benutzer anmelden möchten, der während der Installation erstellt wurde, müssen Sie dem Benutzer im Anschluss an die Installation ein Passwort zuweisen.

Installation von Collector-Manager

Abhängig von dem Betriebssystem, auf dem der Collector-Manager installiert ist, können die Sicherheitsstufen der Systembenutzer variieren.

Linux: Das Installationsprogramm fordert Sie auf, den Namen des Systembenutzers anzugeben, der Eigentümer der installierten Dateien sein soll. Außerdem fragt es nach dem Speicherort, an dem das Basisverzeichnis für diesen Benutzer erstellt werden soll. Standardmäßig ist der Systembenutzer `esecadm`. Sie können jedoch den Namen dieses Systembenutzers ändern. Wenn der Benutzer nicht vorhanden ist, wird er zusammen mit seinem Basisverzeichnis erstellt. Wenn ein neuer Benutzer erstellt wird, wird das Passwort während der Installation aus Sicherheitsgründen nicht festgelegt. Wenn Sie sich bei dem System als dieser Benutzer anmelden möchten, müssen Sie dem Benutzer im Anschluss an die Installation ein Passwort zuweisen. Die Standardgruppe ist `esec`.

Wenn der Benutzer während der Client-Installation bereits vorhanden ist, dann werden Sie vom Installationsprogramm nicht erneut nach dem Benutzer gefragt. Dieses Verhalten ähnelt dem Verhalten beim Deinstallieren oder erneuten Installieren von Software. Sie können jedoch dafür sorgen, dass das Installationsprogramm erneut nach dem Benutzer fragt:

1. Löschen Sie den Benutzer und die Gruppe, die bei der ersten Installation erstellt wurden.
2. Löschen Sie die ESEC_USER-Umgebungsvariablen aus `/etc/profile`.

Windows: Es werden keine Benutzer erstellt.

Die Passwortrichtlinien für Systembenutzer werden durch das verwendete Betriebssystem bestimmt.

5.3.2 Sentinel-Anwendungs- und Datenbankbenutzer

Alle Anwendungsbenutzer von Sentinel Rapid Deployment sind native Datenbankbenutzer, und ihre Passwörter sind durch Verfahren geschützt, die sich nach der nativen Datenbankplattform richten. Diese Benutzer haben lediglich Lesezugriff auf bestimmte Tabellen in der Datenbank, sodass sie Abfragen der Datenbank durchführen können.

Das Installationsprogramm erstellt und konfiguriert eine PostgreSQL-Datenbank mit folgenden Benutzern:

- **admin:** Bei dem Benutzer „admin“ handelt es sich um den Administrator-Benutzer, der sich bei allen Sentinel-Anwendungen anmelden kann.

- **dbauser:** Der Benutzer „dbauser“ wird als Superuser erstellt, der die Datenbank verwalten kann. Das Passwort für den Benutzer „dbauser“ wird während der Installation des Sentinel Rapid Deployment-Servers festgelegt. Dieses Passwort ist in `<user home directory>/.pgpass` gespeichert. Das System befolgt die Passwortrichtlinien für PostgreSQL-Datenbanken. Weitere Informationen finden Sie unter Abschnitt 5.3.3, „Erzwingen der Einhaltung einer Passwortrichtlinie für Benutzer“, auf Seite 64.
- **appuser:** Bei dem Benutzer „appuser“ handelt es sich um einen Nicht-Superuser, der von den Sentinel-Anwendungen für die Verbindungen zur Datenbank verwendet wird. Standardmäßig verwendet der Benutzer „appuser“ ein Passwort, das während der Installation per Zufallsgenerator erstellt und verschlüsselt in den XML-Dateien (`das_core.xml`, `das_binary.xml` und `advisor_client.xml`) gespeichert wird, die sich im Verzeichnis „<*Installationsverzeichnis*>/config“ befinden. Zum Ändern des Passworts für den appuser können Sie das Dienstprogramm `<Installationsverzeichnis>/bin/dbconfig` verwenden. Weitere Informationen finden Sie unter „Data Container Files“ (Datencontainerdateien) im *Sentinel Rapid Deployment Reference Guide* (Sentinel Rapid Deployment Referenzhandbuch).

Hinweis: Es gibt auch einen PostgreSQL-Datenbankbenutzer, der Eigentümer der gesamten Datenbank einschließlich der Systemdatenbanktabellen ist. Standardmäßig ist der PostgreSQL-Datenbankbenutzer auf NOLOGIN gesetzt, sodass sich keiner als der PostgreSQL-Benutzer anmelden kann.

5.3.3 Erzwingen der Einhaltung einer Passwortrichtlinie für Benutzer

Sentinel Rapid Deployment verwendet auf Standards basierende Mechanismen, um die Durchsetzung der Passwortrichtlinieneinhaltung zu erleichtern.

Das Installationsprogramm erstellt und konfiguriert eine PostgreSQL-Datenbank mit folgenden Benutzern:

dbauser: Der Eigentümer der Datenbank (Datenbankadministrator-Benutzer). Das Passwort wird bei der Installation festgelegt.

appuser: Dies ist der Anwendungsbenutzer, der für die Anmeldung bei der Datenbank von Sentinel Rapid Deployment verwendet wird. Das Passwort wird bei der Installation zufällig generiert und ist nur für interne Benutzer gedacht.

admin: Der Berechtigungsnachweis für den Administrator kann für die Anmeldung bei der Weboberfläche von Sentinel Rapid Deployment verwendet werden. Das Passwort wird bei der Installation festgelegt.

Standardmäßig werden Benutzerpasswörter innerhalb der in Sentinel Rapid Deployment eingebetteten PostgreSQL-Datenbank gespeichert. PostgreSQL bietet die Möglichkeit, verschiedene standardbasierte Authentifizierungsmechanismen einzusetzen, wie im Abschnitt Client Authentication (http://www.postgresql.org/docs/8.3/static/client-authentication.html) (Client-Authentifizierung) der PostgreSQL-Dokumentation beschrieben.

Die Verwendung dieser Mechanismen betrifft alle Benutzerkonten in Sentinel Rapid Deployment, d. h. die Benutzer der Webanwendung sowie Konten, die ausschließlich von Backend-Diensten verwendet werden, z. B. `dbauser` und `appuser`.

Einfacher ist es, Webanwendungsbenutzer mittels eines LDAP-Verzeichnisses zu authentifizieren. Informationen dazu, wie dies auf einem Sentinel Rapid Deployment-Server ermöglicht wird, finden Sie in Abschnitt 3.7, „LDAP-Authentifizierung“, auf Seite 45. Diese Option wirkt sich nicht auf von Backend-Diensten verwendete Konten aus, die, solange Sie nicht die Konfigurationseinstellungen für PostgreSQL ändern, weiterhin über PostgreSQL authentifiziert werden.

Sie können die Einhaltung von Sentinel Rapid Deployment-Passwortrichtlinien zuverlässig erzwingen, wenn Sie diese standardbasierten Mechanismen und die in Ihrer Umgebung vorhandenen Mittel, beispielsweise Ihr LDAP-Verzeichnis, nutzen.

5.4 Sichern der Sentinel-Daten

Wichtig: Aufgrund des hochsensiblen Charakters der Daten auf dem Sentinel-Server sollten Sie den Computer physisch schützen und in einem sicheren Bereich des Netzwerks betreiben.Verwenden Sie einen remoten Collector-Manager, um Daten von Ereignisquellen außerhalb des sicheren Netzwerks zu sammeln.

Für bestimmte Komponenten müssen Passwörter gespeichert werden, sodass sie verfügbar sind, wenn das System eine Verbindung zu einer Ressource herstellen muss, z. B. zur Datenbank oder zu einer Ereignisquelle. In diesem Fall wird das Passwort beim Speichern zunächst verschlüsselt, um den unerlaubten Zugriff auf das unverschlüsselte Passwort zu verhindern.

Auch wenn Passwörter verschlüsselt werden, müssen Sie dafür sorgen, dass der Zugriff auf die gespeicherten Passwortdaten geschützt ist, um eine Passwortoffenlegung zu verhindern. Beispielsweise können Sie sicherstellen, dass die Berechtigungen für die Dateien mit vertraulichen Daten nicht von unbefugten Benutzern gelesen werden können.

DATEIEN

`advisor_client.xml`

Datenbank-Berechtigungsnachweise

Der Datenbank-Berechtigungsnachweis wird in der Datei `<Installationsverzeichnis>/config/server.xml` gespeichert:

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

Advisor-Berechtigungsnachweis

```
<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.Ac
tiveMQStrategyFactory" 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>
```

In einigen Datenbanktabellen werden Passwörter und Zertifikate gespeichert. Diese vertraulichen Daten sind verschlüsselt und werden in den unten aufgeführten Tabellen gespeichert. Sie müssen den Zugriff auf diese Tabellen einschränken.

- **evt_src:** evt_src_config-Spaltendaten
- **evt_src_collector:** Spalten: evt_src_collector_props
- **evt_src_grp (ungewiss):** Spalten: evt_src_default_config
- **md_config:** Spalte : data
- **integrator_config:** Spalte : integrator_properties
- **md_view_config:** Spalte : view_data
- **esec_content:** Spalte: content_context, content_hash
- **esec_content_grp_content:** Spalten: content_hash
- **sentinel_plugin:** Spalten: content_pkg, file_hash

Sentinel Rapid Deployment speichert sowohl Konfigurationsdaten als auch Ereignisdaten. Diese Daten werden an folgenden Speicherorten gespeichert:

Komponenten	Speicherort für Konfigurationsdaten	Speicherort für Ereignisdaten
Sentinel Rapid Deployment-Server	Datenbanktabellen und das Dateisystem (<*Installationsverzeichnis*>/config) Diese Konfigurationsdaten enthalten die verschlüsselte Datenbank, die Ereignisquelle, die Integratoren und die Passwörter.	Datenbank (Tabellen „EVENTS“, „CORRELATED_EVENTS“, „EVT_SMRY_“ und „AUDIT_RECORD“) sowie das Dateisystem unter <*Installationsverzeichnis*>/data/eventdata und <*Installationsverzeichnis*>/data/raw data Die Ereignisdaten können im Rahmen der Partitionsverwaltung in das Dateisystem archiviert werden.
Correlation Engine	Dateisystem (<*Installationsverzeichnis*>/config). Die einzigen sensitiven Konfigurationsdaten sind das Client-Schlüsselpaar, das zur Verbindung mit dem Nachrichtenbus verwendet wird.	correlation_engine.cache
DAS Core	<*Installationsverzeichnis*>/config	das_core.cache
DAS Binary	<*Installationsverzeichnis*>/config	Die Ereignisdaten können im Cache zwischengespeichert werden, wenn die Datenbank außer Betrieb ist. das_binary.cache
Collector-Manager	Dateisystem (<*Installationsverzeichnis*>/config). Die einzigen vertraulichen Konfigurationsdaten sind das Collector-Manager-Benutzerpasswort, das zur Verbindung mit dem Nachrichtenbus verwendet wird.	In Störungssituationen können die Ereignisdaten im Dateisystem zwischengespeichert werden, z. B. wenn der Nachrichtenbus außer Betrieb ist oder ein Ereignisüberlauf vorliegt. Diese Ereignisdaten werden im Verzeichnis <*Installationsverzeichnis*>/data/collector_mgr.cache gespeichert.

Komponenten	Speicherort für Konfigurationsdaten	Speicherort für Ereignisdaten
Client-Anwendungen	Dateisystem (*`Installationsverzeichnis`*`/config`). Die Client-Anwendungen speichern keine vertraulichen Daten in ihren Konfigurationsdateien. Beispielsweise können Client-Anwendungen die ESM-Daten in ein lokales Dateisystem exportieren. Die exportierten Dateien enthalten verschlüsselte Passwörter, wenn sie in der Konfiguration der Ereignisquellen vorhanden sind, die exportiert wurden. Obwohl die Passwörter verschlüsselt sind, sollte die Erlaubnis zum ESM-Export nur Benutzern erteilt werden, denen dieses Privileg wirklich anvertraut werden kann.	Keine

5.5 Sicherung von Informationen

- Sie müssen die Ereignisse regelmäßig sichern. Die Sicherungsmedien sollten in einer sicheren Offsite-Einrichtung aufbewahrt werden.
- Sichern Sie die Systemdaten. Weitere Informationen finden Sie unter „Backup and Restore Utility“ (Backup- und Wiederherstellungs-Dienstprogramm) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).
- Verwenden Sie bei vertraulichen Daten eine der folgenden Methoden zum Verschlüsselung der Datensicherung:
  - Verschlüsseln Sie die eigentlichen Daten, wenn die Anwendung, mit der die Daten erzeugt werden, eine Verschlüsselung unterstützt. So unterstützen beispielsweise Datenbankprodukte und Drittanbieter-Tools die Datenverschlüsselung. Verwenden Sie Sicherungssoftware, die in der Lage ist, die Daten während des Sicherungsvorgangs zu verschlüsseln. Diese Methode ist mit Leistungs- und Verwaltungsanforderungen verknüpft, insbesondere beim Verwalten von Verschlüsselungsschlüsseln.
  - Verwenden Sie eine Verschlüsselungs-Appliance, die während der Datensicherung die Sicherungsmedien verschlüsselt.
- Wenn Sie die Medien transportieren und an einem anderen Ort aufbewahren möchten, sollten Sie damit ein Unternehmen beauftragen, das auf den Transport und die Aufbewahrung von Speichermedien spezialisiert ist. Stellen Sie sicher, dass Ihre Bänder mit Barcodes verfolgt werden können, unter umweltfreundlichen Bedingungen aufbewahrt werden und durch ein Unternehmen gehandhabt werden, dessen Ruf auf seiner Fähigkeit zum richtigen Umgang mit Speichermedien beruht.
- Laden von Wiederherstellungszertifikaten. Der Novell Sentinel-Dienst ist standardmäßig nicht für den Wiederherstellungsagenten konfiguriert. Während der Serverkonfiguration über YaST müssen Sie sicherstellen, dass der Pfad des Wiederherstellungsagenten konfiguriert ist. Dieser Pfad sollte die Liste der Zertifikate enthalten, die der Dienst laden kann, damit die Benutzer eine Auswahl treffen können.

Weitere Informationen finden Sie unter „Certificate Management for Sentinel 6.1 Rapid Deployment Server“ (Zertifikatsverwaltung für Sentinel 6.1 Rapid Deployment Server) im *Sentinel Rapid Deployment Reference Guide* (Sentinel Rapid Deployment Referenzhandbuch).

YaST enthält Module für die Basisverwaltung von X.509-Zertifikaten, die vor allem das Erstellen von CAs, Sub-CAs und deren Zertifikaten umfasst. Weitere Informationen zum Verwalten und Aktualisieren von Zertifikaten finden Sie unter Verwalten der X.509-Zertifizierung (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html) im *SUSE Linux Enterprise Server 10 Installations- und Administrationshandbuch* (http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html).

5.6 Sichern des Betriebssystems

- Sentinel Rapid Deployment wird auf SUSE Linux Enterprise Server (SLES) 10 SP3 oder höher unterstützt. Weitere Information zum Sichern des SLES-Computers finden Sie in der SuSE Linux Enterprise Server 10 Dokumentation (http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html).
- Sichern Sie den Zugriff auf den Sentinel Rapid Deployment-Server mit einer Firewall. Wenn der Zugriff auf den Sentinel-Server von außerhalb des Unternehmensnetzwerks möglich ist, sollte eine Firewall eingesetzt werden, um den direkten Zugriff durch einen Eindringling zu verhindern.

  Aktivieren Sie folgende Ports in der Firewall:

Komponenten	Port
ActiveMQ	61616
PostgreSQL	5432
Tomcat	8443
Sentinel Control Center-Proxy-Client-Port	10013
Vertrauenswürdiger Proxy-Client	10014
internal_gateway_server und internal_gateway (verwendet zwischen Engine und Manager)	5556
internal_router_server und internal_router_client Wird zwischen Ereignis-Router-Client und -Server verwendet	5558
Ereignis-Listener-Port in `config/collector_mgr.properties` als „`esecurity.agentmanager.event.port`“ konfiguriert	35000

Hinweis: Mit einem Sternchen markierte Ports können anders definiert sein, falls sie zum Zeitpunkt der Installation bereits in Verwendung waren. Wenn sie zum Zeitpunkt der Installation bereits Verwendung waren, sind sie durch die Portnummern zu ersetzen, die zum Zeitpunkt der Installation abgefragt wurden.

Weitere Informationen zum Aktivieren einer Firewall auf SLES 10 finden Sie unter Konfigurieren von Firewalls mit YaST (http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html) im *SLES 10 Administrationshandbuch*.

5.7 Anzeigen von Sentinel Audit-Ereignissen

Für viele von Benutzern durchgeführte Aktionen und für solche, die intern für Systemaktivitäten durchgeführt werden, generiert Sentinel Rapid Deployment Audit-Ereignisse. Diese Ereignisse können in den Active Views angezeigt oder durch eine Suche oder einen Bericht abgefragt werden. Sie benötigen jedoch die entsprechenden Berechtigungen, um die Systemereignisse anzeigen zu können.

Weitere Informationen finden Sie unter „System Events for Sentinel“ (Systemereignisse für Sentinel) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

5.8 Verwenden eines CA-Zertifikats

Sie können das eigensignierte Zertifikat durch ein Zertifikat ersetzen, das durch eine bekannte Zertifizierungsstelle wie VeriSign, Thawte oder Entrust signiert ist. Außerdem können Sie das eigensignierte Zertifikat durch ein Zertifikat ersetzen, das durch eine weniger bekannte Zertifizierungsstelle signiert ist – beispielsweise durch eine Zertifizierungsstelle in Ihrem Unternehmen oder Ihrer Organisation.

Weitere Informationen finden Sie unter „Certificate Management for Sentinel 6.1 Rapid Deployment Server“ (Zertifikatsverwaltung für Sentinel 6.1 Rapid Deployment Server) im *Sentinel Rapid Deployment Reference Guide* (Sentinel Rapid Deployment Referenzhandbuch).

Testen der Funktionalität von Sentinel Rapid Deployment

6

Sentinel wird mit einem Generic Collector installiert, mit dem viele der Grundfunktionen des Systems getestet werden können. Sie können diesen Collector verwenden, um Active Views, erstellte Vorfälle, Korrelationsregeln und Berichte zu testen.

6.1 Testen der Installation von Rapid Deployment

Nachfolgend werden die Schritte erläutert, mit denen sich das Sentinel Rapid Deployment-System und die erwarteten Ergebnisse testen lassen. Möglicherweise werden bei Ihnen nicht dieselben Ereignisse angezeigt, Ihre Ergebnisse sollten jedoch in etwa mit den unten angezeigten übereinstimmen.

Auf der untersten Ebene können Sie mit diesen Tests überprüfen, ob Folgendes zutrifft:

- Die Sentinel-Dienste sind aktiv und werden ausgeführt.
- Die Kommunikation über den Nachrichtenbus funktioniert.
- Interne Audit-Ereignisse werden gesendet.
- Ereignisse können über einen Collection-Manager gesendet werden.
- Ereignisse werden in die Datenbank eingefügt und können mithilfe eines Berichts abgerufen werden.
- Vorfälle können erstellt und angezeigt werden.
- Die Correlation Engine bewertet Regeln und löst korrelierte Ereignisse aus.
- Der Sentinel Data Manager wird mit der Datenbank verbunden und kann die Partitionsinformationen lesen.

Wenn einer dieser Tests nicht erfolgreich ist, lesen Sie im Installationsprotokoll und den anderen Protokolldateien nach und nehmen Sie ggf. Kontakt mit Novell Technical Support (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) auf.

So testen Sie die Installation:

1. Melden Sie sich bei einer Weboberfläche von Sentinel Rapid Deployment an.

   Weitere Informationen finden Sie in „Accessing the Novell Sentinel Web Interface“ (Zugriff auf die Weboberfläche von Novell Sentinel) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).
2. Wählen Sie die Seite „Suche“ aus und suchen Sie nach einem internen Ereignis. Ein oder mehrere Ereignisse sollten zurückgegeben werden.

Wenn Sie beispielsweise nach internen Ereignissen mit dem Schweregradbereich 3 bis 5 suchen möchten, wählen Sie *Systemereignisse einbeziehen* aus und geben Sie anschließend im Feld *Suchen > sev:[3 TO 5]* ein.

Weitere Informationen zur Suche finden Sie unter „Running an Event Search“ (Ausführen einer Ereignissuche) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

Die Suchfunktion ist in SP2 nicht standardmäßig aktiviert. Wenn Sie diese Funktion aktivieren möchten, lesen Sie „Enabling the Search Option in Web User Interface“ (Aktivieren der Suchoption in der Weboberfläche) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

3. Wählen Sie die Seite „Berichte“ aus, geben Sie die Parameter an und führen Sie anschließend einen Bericht aus.

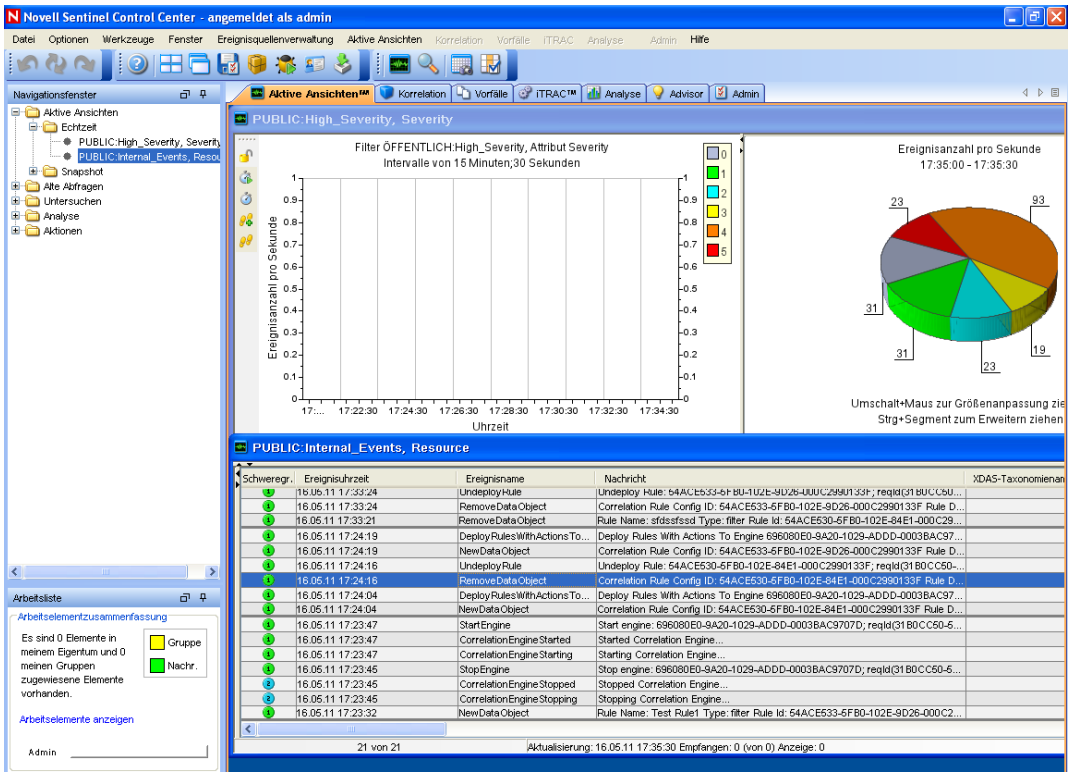
   Klicken Sie beispielsweise auf die Schaltfläche *Ausführen* neben „Sentinel Core Event Configuration“, geben Sie die gewünschten Parameter an und klicken Sie anschließend auf *Ausführen*.

   Weitere Informationen finden Sie unter „Running Reports“ (Ausführen von Berichten) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

4. Klicken Sie auf der Seite „Anwendungen“ auf *Control Center starten*.

5. Melden Sie sich als der verwaltungsbefugte Sentinel-Benutzer beim System an, der während der Installation angegeben wurde (Standard: „admin“).

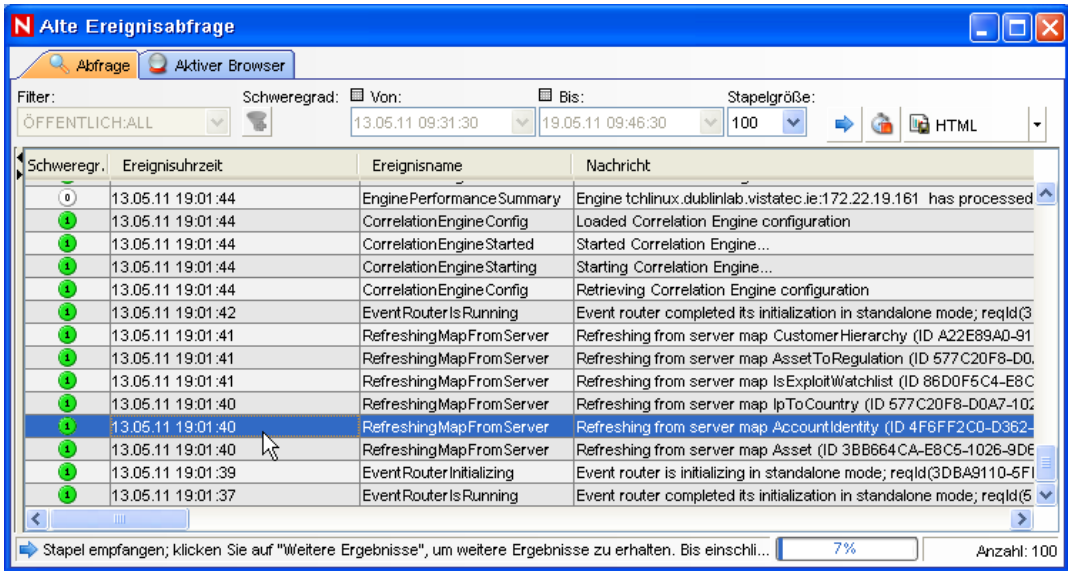
   Das Sentinel Control Center wird geöffnet und die Registerkarte *Active Views* wird mit Ereignissen angezeigt, die mit den öffentlichen Filtern *Internal_Events* und *High_Severity* gefiltert wurden.



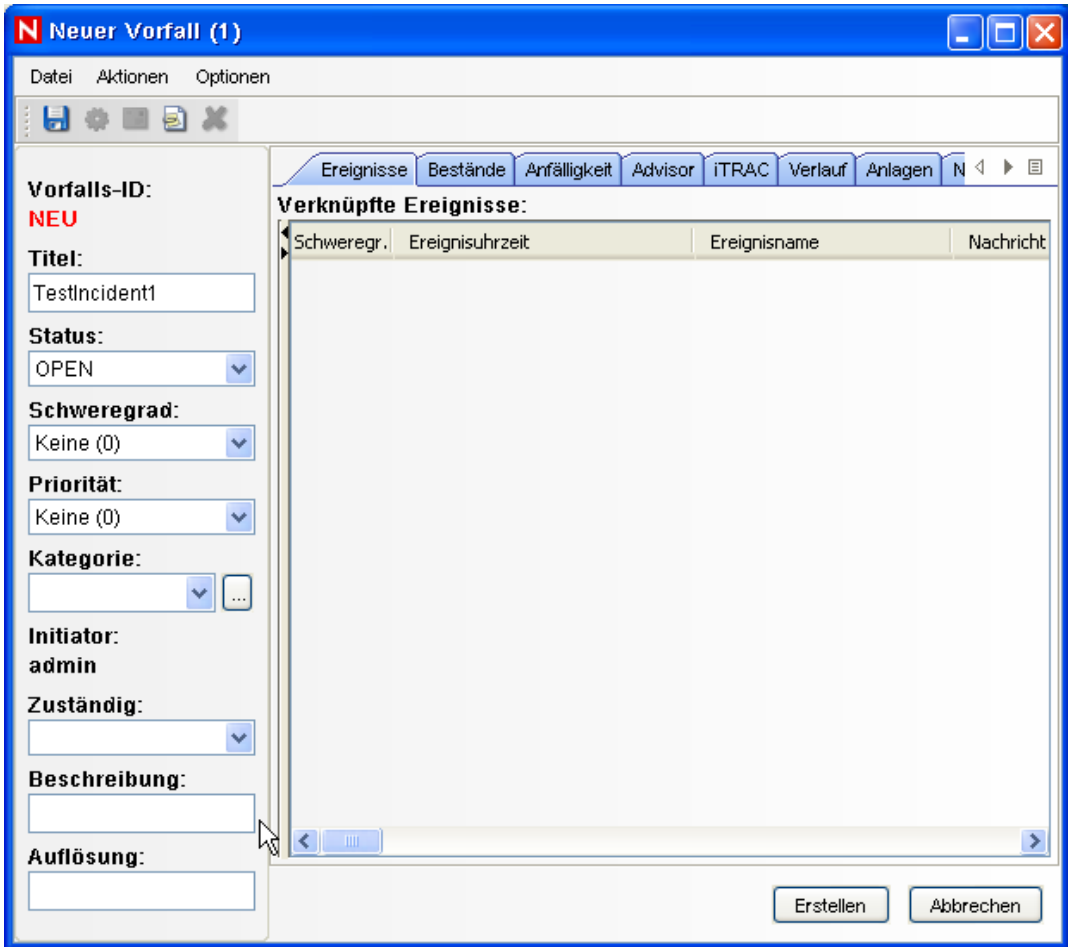
6. Rufen Sie das Menü *Ereignisquellenverwaltung* auf und wählen Sie die Option *Live-Ansicht.*

7. Klicken Sie in der grafischen Ansicht mit der rechten Maustaste auf *Ereignisquelle mit 5 EPS* und wählen Sie die Option *Starten*.
8. Schließen Sie das Fenster „Ereignisquellenverwaltung [Live-Ansicht]“.
9. Klicken Sie auf die Registerkarte *Active Views*.

   Sie können das aktive Fenster mit dem Titel „PUBLIC: High_Severity, Severity“ anzeigen. Es kann einige Zeit dauern, bis der Collector gestartet wird und die Daten in diesem Fenster angezeigt werden.
10. Klicken Sie in der Symbolleiste auf die Schaltfläche *Ereignisabfrage*. Das Fenster „Alte Ereignisabfrage“ wird angezeigt.
11. Klicken Sie im Fenster „Alte Ereignisabfrage“ auf den Abwärtspfeil neben *Filter*, um den Filter auszuwählen. Wählen Sie den Filter *Öffentlich: Alle* aus.
12. Wählen Sie einen Zeitraum aus, der die Zeit abdeckt, in der der Collector aktiv war. Wählen Sie mithilfe der Dropdown-Listen *Von* und *Bis* den Datumsbereich aus.
13. Wählen Sie die Stapelgröße aus.
14. Klicken Sie auf die Lupe, um die Abfrage auszuführen.



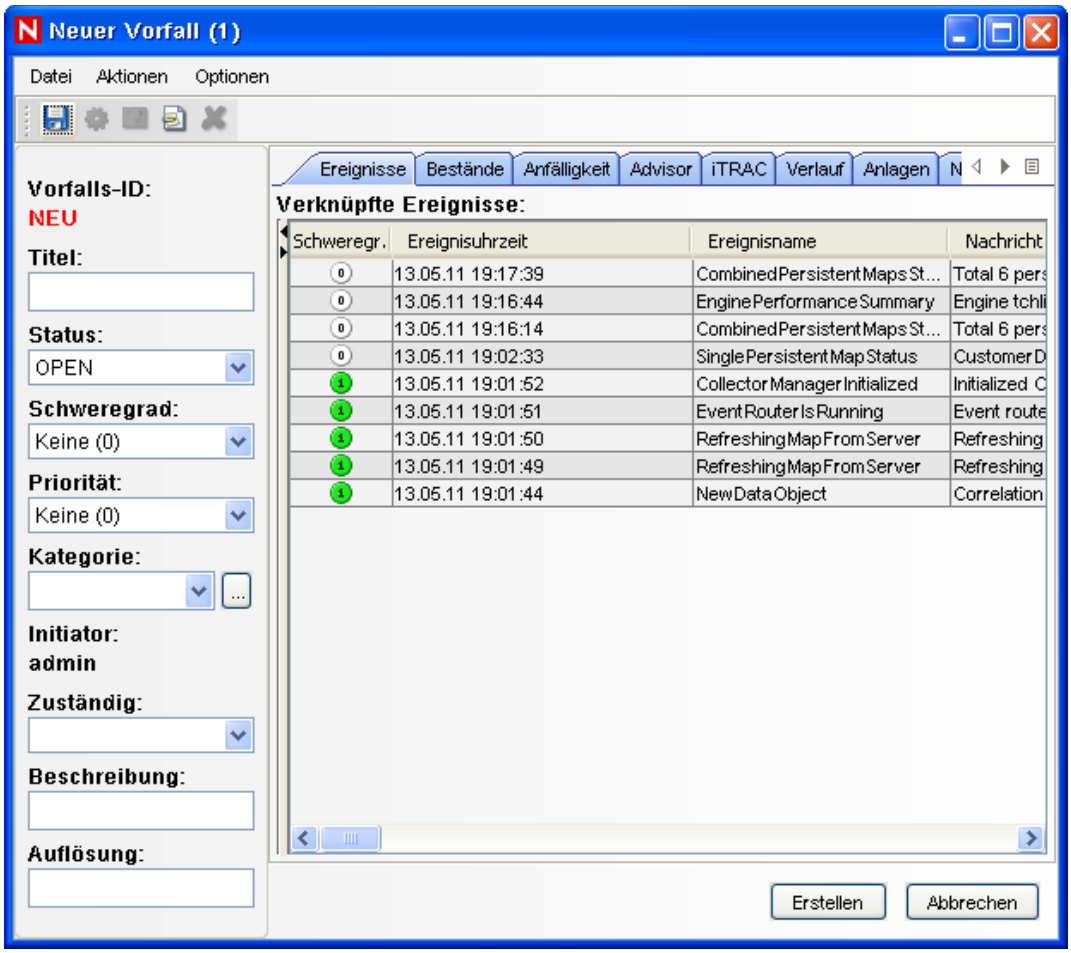
15. Wählen Sie bei gedrückter Strg- oder Umschalttaste im Fenster „Alte Ereignisabfrage“ mehrere Ereignisse aus.
16. Klicken Sie mit der rechten Maustaste in das Fenster und wählen Sie anschließend *Vorfall erstellen* aus, um das Fenster „Neuer Vorfall“ anzuzeigen.



17 Nennen Sie den Vorfall „Testvorfall1“ und klicken Sie auf *Erstellen*. Wenn die Erfolgsmeldung angezeigt wird, klicken Sie auf *Speichern*.

18 Klicken Sie auf die Registerkarte *Vorfall*, um den gerade erstellten Vorfall im Vorfallansichts-Manager zu sehen.

19 Doppelklicken Sie auf den Vorfall, um die Ereignisse anzuzeigen.



20 Schließen Sie das Fenster „Vorfall“.

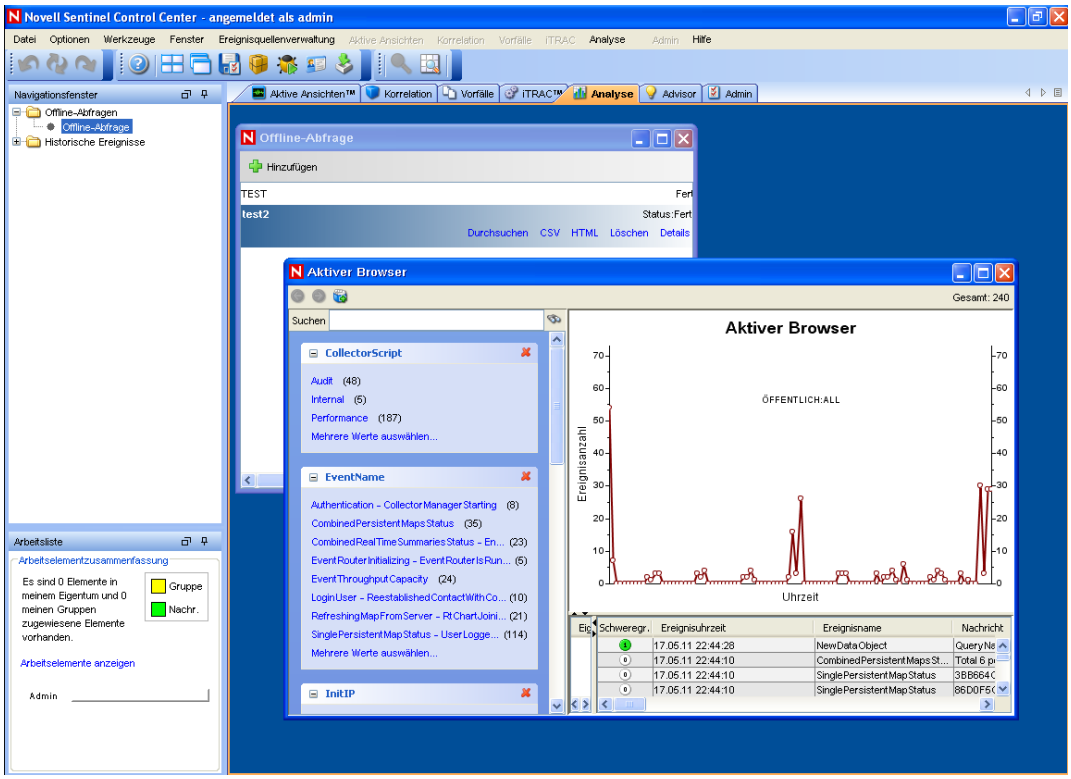
21 Klicken Sie auf die Registerkarte *Analyse*.

22 Klicken Sie vom Menü *Analyse* oder vom Navigator aus auf *Offline-Abfragen*.

23 Klicken Sie im Fenster „Offline-Abfrage“ auf *Hinzufügen*.

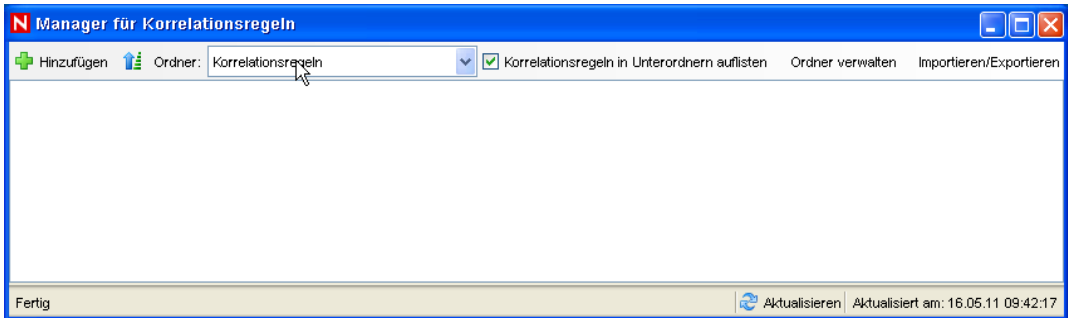
24 Geben Sie einen Namen an, wählen Sie einen Filter aus, wählen Sie eine Zeitspanne aus und klicken Sie anschließend auf *OK*.

25 Klicken Sie auf *Durchsuchen*, um die Liste der Ereignisse und der zugeordneten Details im Fenster „Aktiver Browser“ anzuzeigen.

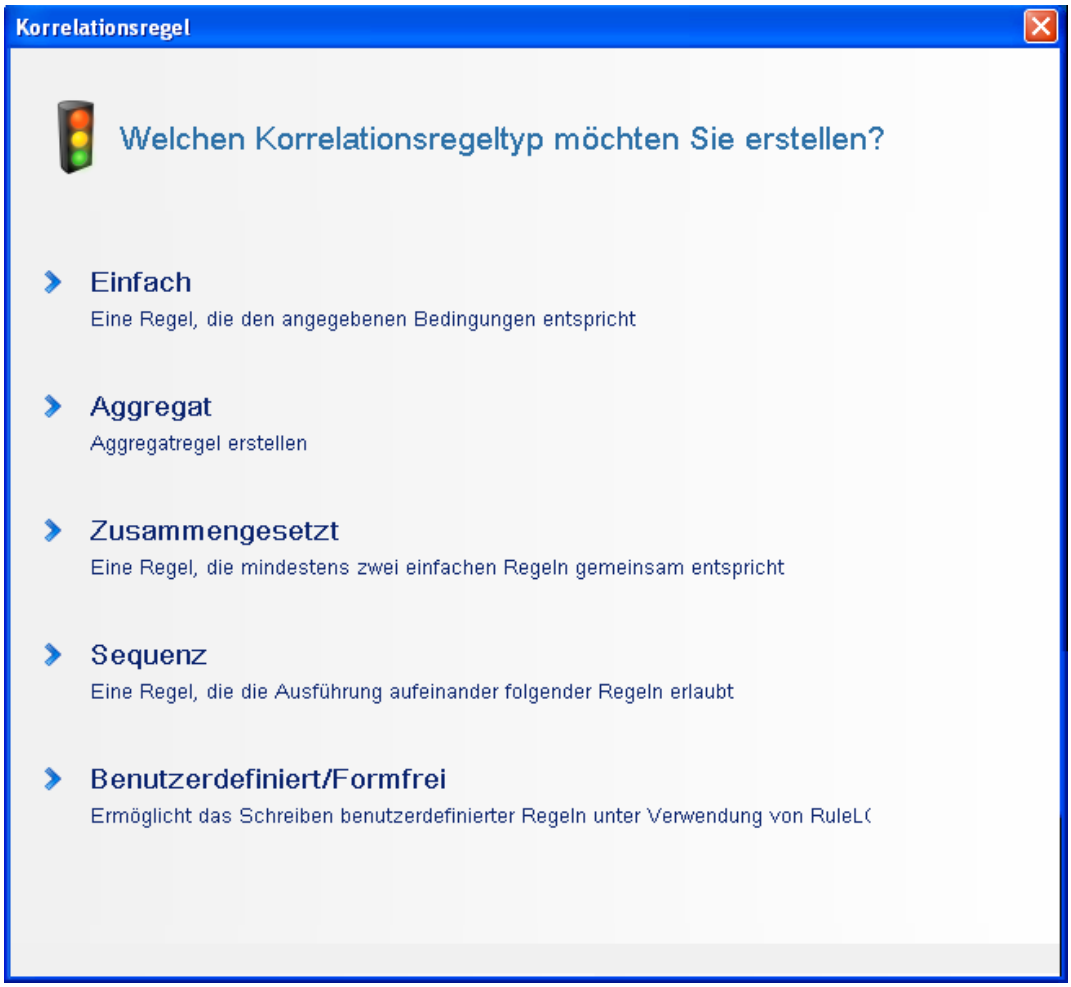


Sie können Details wie „Collector“, „TargetIP“, „Schweregrad“, „Service-Port des Ziels“ und „Ressource“ anzeigen.

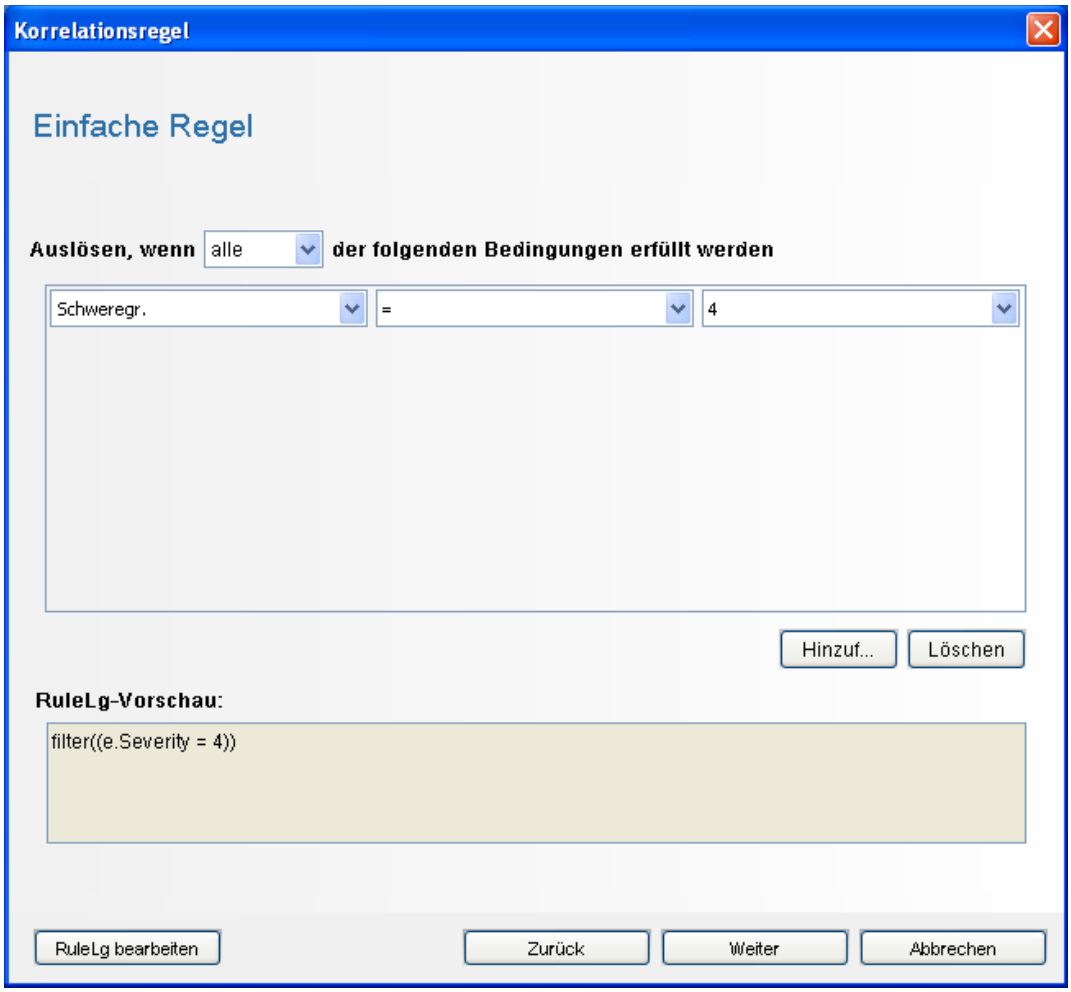
26 Wählen Sie die Registerkarte *Korrelation*. Das Fenster „Manager für Korrelationsregeln“ wird angezeigt.



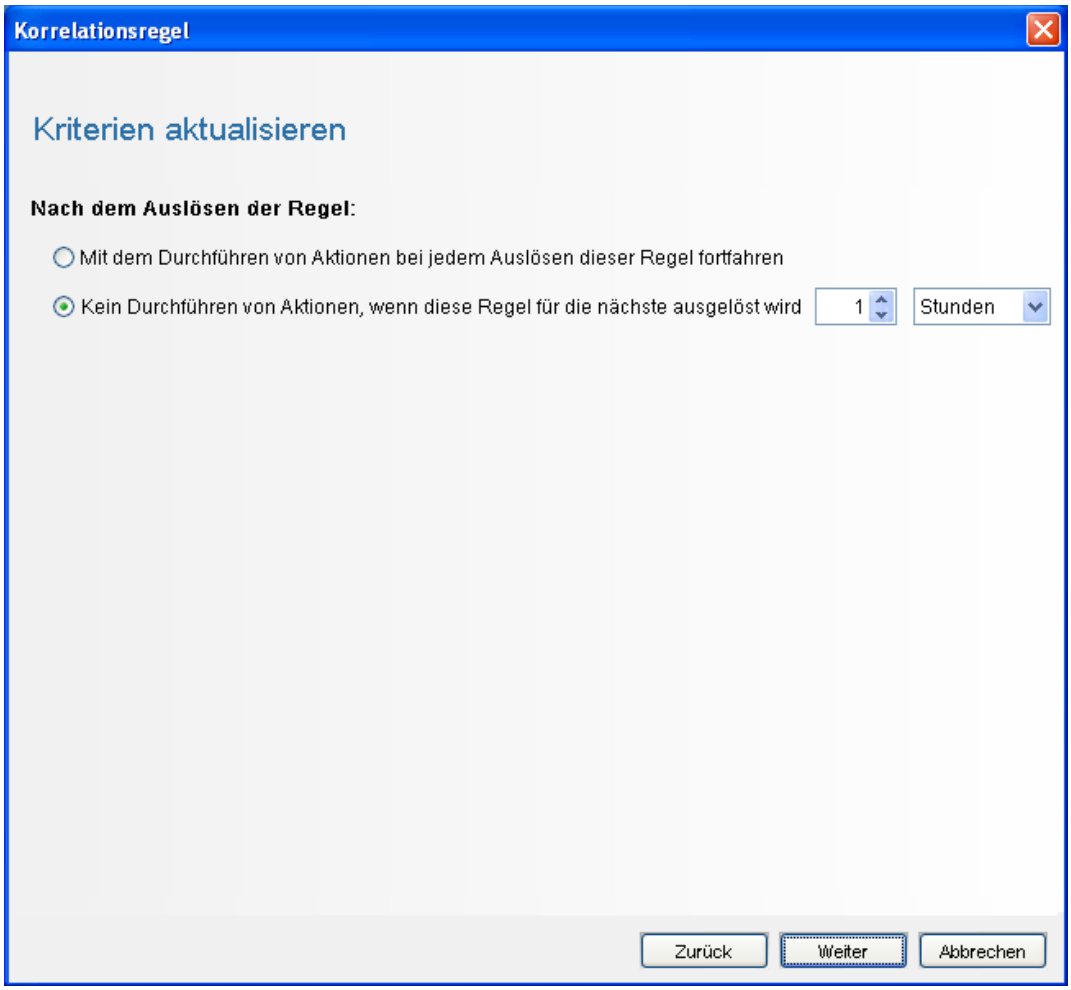
27 Klicken Sie auf *Hinzufügen*. Das Fenster „Assistent für Korrelationsregeln“ wird angezeigt.



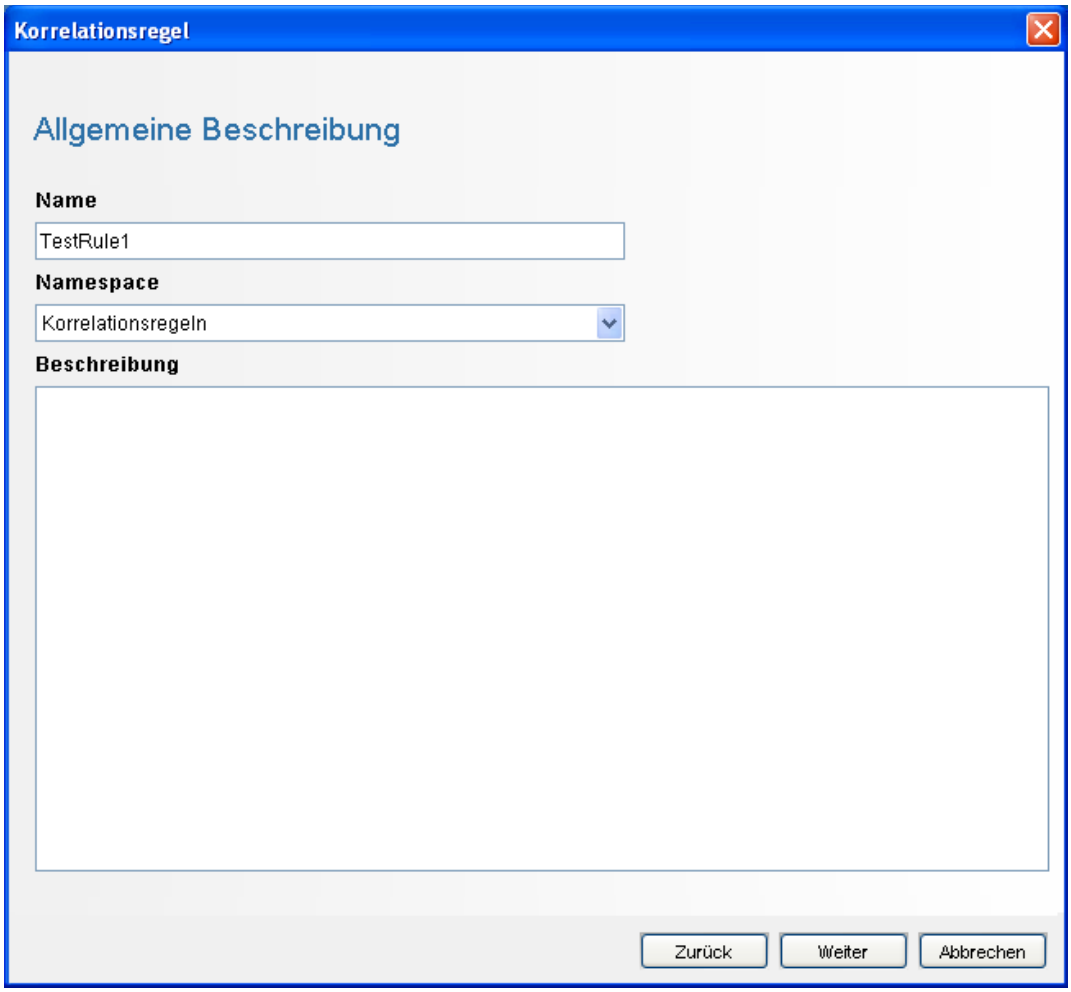
28 Klicken Sie auf *Einfach*. Das Fenster „Einfache Regel“ wird angezeigt.



29 Verwenden Sie die Dropdown-Menüs, um „Schweregrad = 4“ als Kriterium festzulegen und klicken Sie anschließend auf *Weiter*. Das Fenster „Kriterien aktualisieren“ wird angezeigt.



30 Wählen Sie *Kein Durchführen von Aktionen, wenn diese Regel für die nächste ausgelöst wird* aus, stellen Sie die Zeitspanne mithilfe des Dropdown-Menüs auf 1 Minute ein und klicken Sie anschließend auf *Weiter*. Das Fenster „Allgemeine Beschreibung“ wird angezeigt.



31 Nennen Sie die Regel *Testregel1*, geben Sie eine Beschreibung ein und klicken Sie auf *Weiter*.

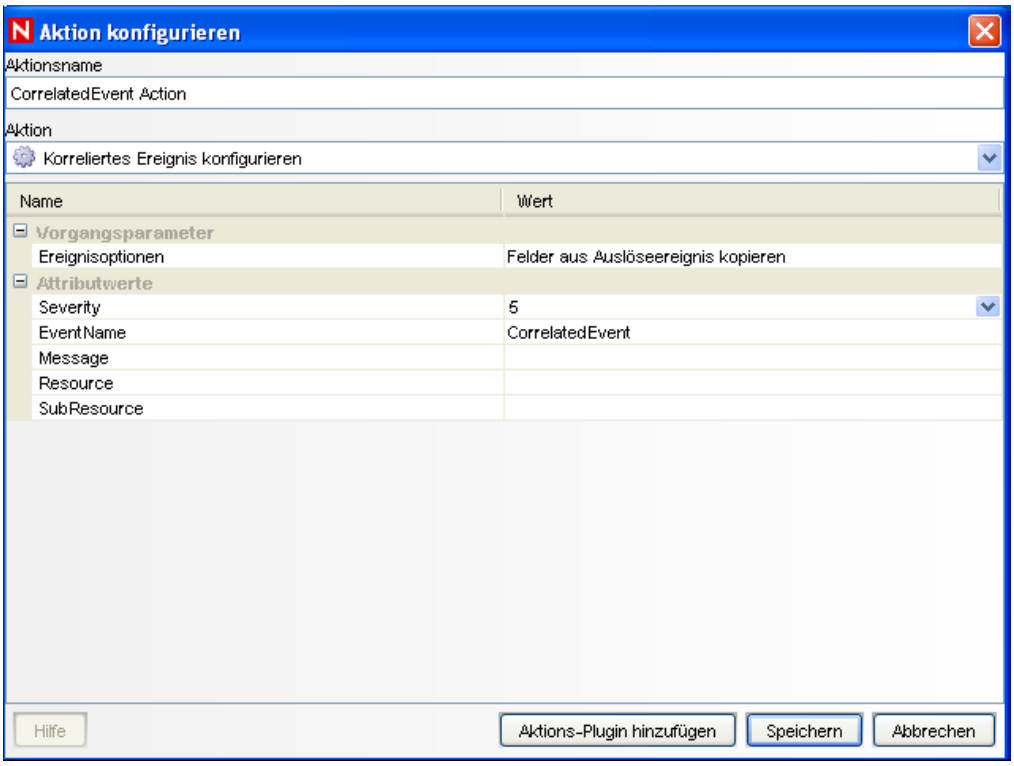
32 Wählen Sie *Nein, erstellen Sie keine andere Regel* und klicken Sie auf *Weiter*.

33 Erstellen Sie eine Aktion, um sie mit der erstellten Regel zu verknüpfen:

33a Führen Sie einen der folgenden Schritte durch:

- Wählen Sie *Werkzeuge* > *Aktionsmanager* > *Hinzufügen*.
- Klicken Sie im Fenster „Regel bereitstellen“ auf *Aktion hinzufügen*. Weitere Informationen finden Sie in den Schritten Schritt 34 bis Schritt 35 auf Seite 81.

Das Fenster „Aktion konfigurieren“ wird angezeigt.



33b Geben Sie im Fenster „Aktion konfigurieren“ Folgendes an:

- Geben Sie den Aktionsnamen an, beispielsweise „CorrelatedEvent Action“.
- Wählen Sie in der Dropdown-Liste *Aktion* die Option *Korreliertes Ereignis konfigurieren* aus.
- Definieren Sie die *Ereignisoptionen*.
- Stellen Sie den *Schweregrad* auf 5 ein.
- Geben Sie den *Ereignisnamen* an, beispielsweise „CorrelatedEvent“.
- Geben Sie bei Bedarf eine Nachricht ein.

Weitere Informationen finden Sie unter „Creating Actions“ (Erstellen von Aktionen) im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch).

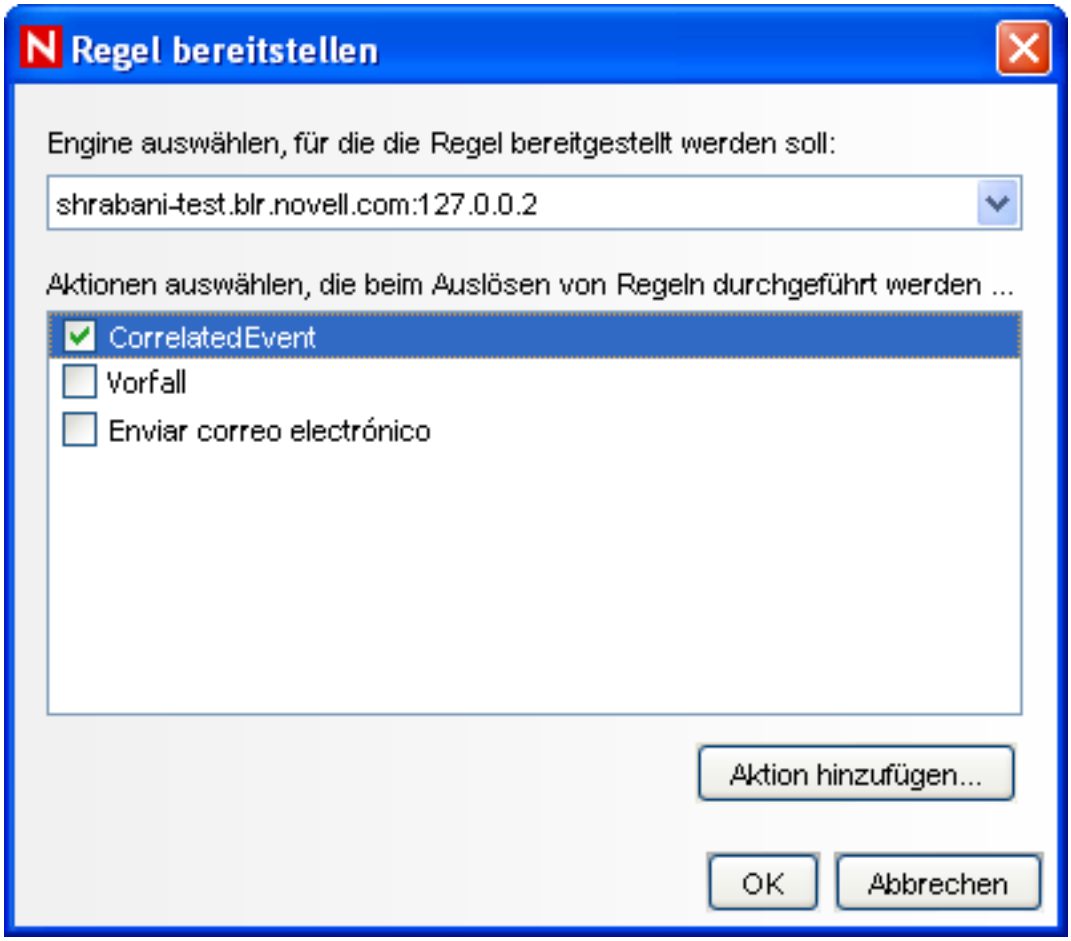
33c Klicken Sie auf *Speichern*.

34 Öffnen Sie das Fenster „Manager für Korrelationsregeln“.

35 Wählen Sie eine Regel aus und klicken Sie anschließend auf den Link *Bereitstellungsregeln*. Das Fenster „Regel bereitstellen“ wird angezeigt.

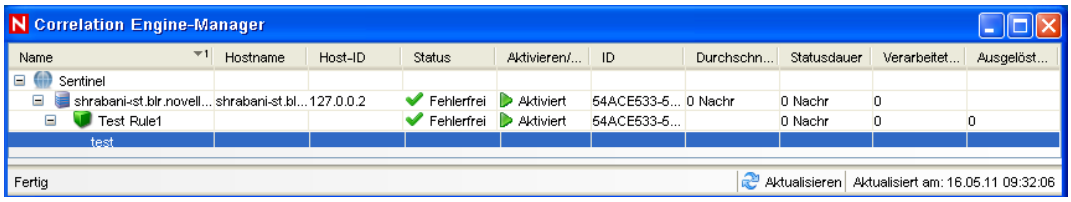
36 Wählen Sie im Fenster „Regel bereitstellen“ die Engine aus, mit der die Regel bereitgestellt werden soll.

37 Wählen Sie die Aktion aus, die Sie in Schritt 33 auf Seite 80 für die Verknüpfung mit der Regel erstellt haben, und klicken Sie anschließend auf *OK*.



38 Wählen Sie *Correlation Engine-Manager* aus.

Sie können unterhalb der Correlation Engine sehen, dass die Regel bereitgestellt und aktiviert wurde.



39 Generieren Sie ein Ereignis mit dem Schweregrad 4, beispielsweise eine fehlgeschlagene Authentifizierung, um die bereitgestellte Korrelationsregel auszulösen.

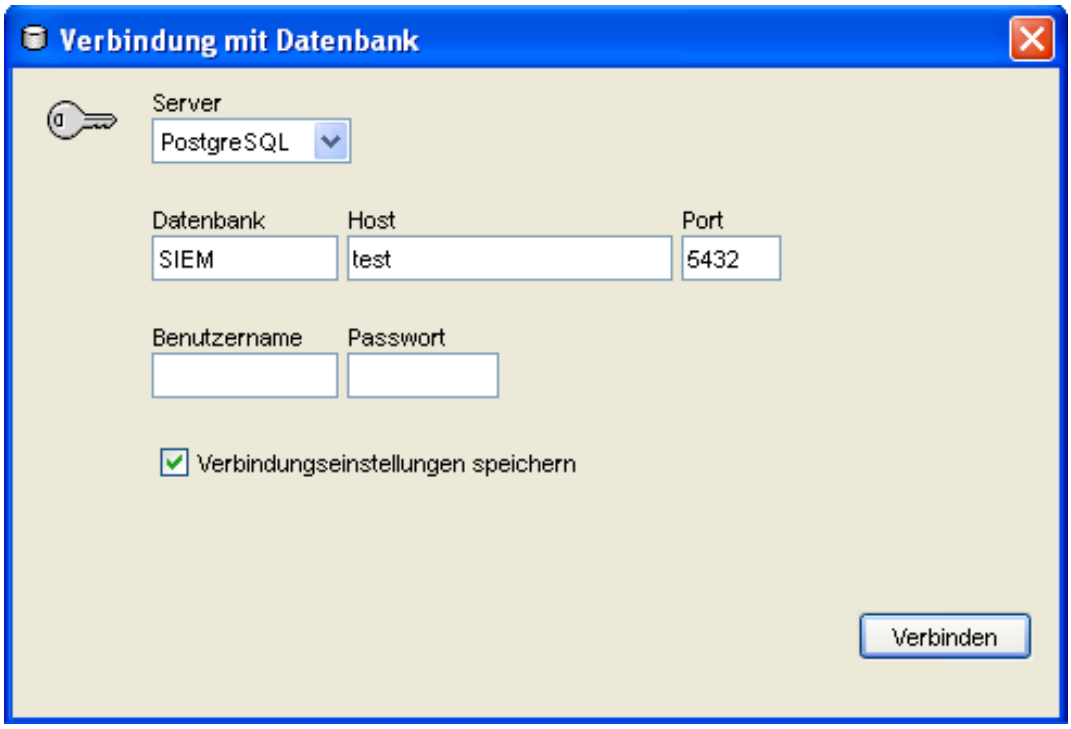
Öffnen Sie beispielsweise ein Fenster für die Anmeldung beim Sentinel Control Center und geben Sie einen falschen Benutzerberechtigungsnachweis ein, um ein solches Ereignis zu generieren.

40 Klicken Sie auf die Registerkarte *Active Views* und überprüfen Sie, ob das korrelierte Ereignis generiert wurde.

41 Schließen Sie Sentinel Control Center.

42 Klicken Sie auf der Seite „Anwendungen“ auf *Sentinel Data Manager starten*.

43 Melden Sie sich als der für die Verwaltung der Datenbank befugte Benutzer bei Sentinel Data Manager an, der während der Installation angegeben wurde (Standard: „dbauser“).



44 Klicken Sie auf jede Registerkarte, um zu überprüfen, ob Sie darauf zugreifen können.

45 Schließen Sie Sentinel Data Manager.

Wenn Sie alle diese Schritte ohne Fehler durchführen konnten, haben Sie die grundlegende Überprüfung der Sentinel-Systeminstallation abgeschlossen.

6.2 Bereinigung nach dem Testen

Nach Abschluss der Systemüberprüfung sollten Sie die für die Tests erstellten Objekte löschen.

1 Melden Sie sich als der verwaltungsbefugte Sentinel-Benutzer beim System an, der während der Installation angegeben wurde (Standard: „admin“).

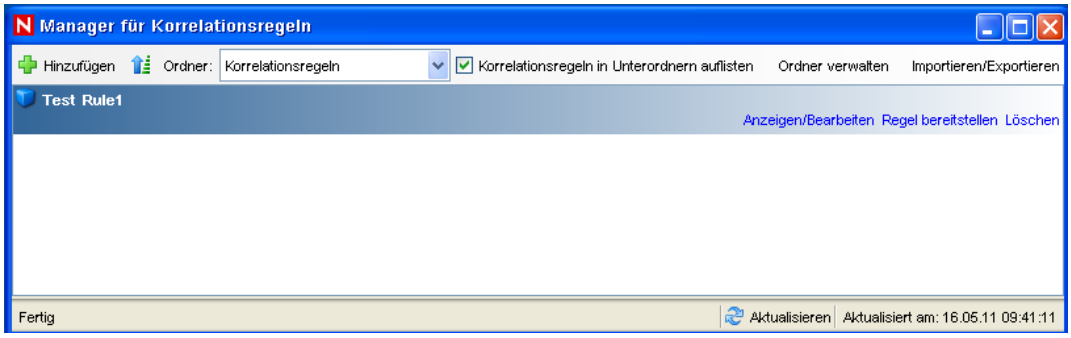
2 Wählen Sie die Registerkarte *Korrelation*.

3 Öffnen Sie den Correlation Engine-Manager.

4 Klicken Sie im Correlation Engine-Manager auf *Testregel1* und wählen Sie *Bereitstellung aufheben*.

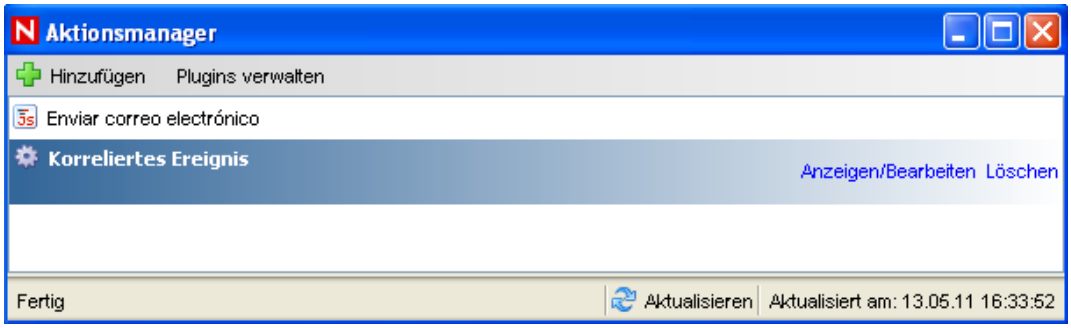
5 Öffnen Sie den Manager für Korrelationsregeln.

6 Wählen Sie *Testregel1* aus und klicken Sie auf *Löschen*.



7 Wählen Sie *Werkzeuge* > *Aktionsmanager*, um das Fenster „Aktionsmanager“ anzuzeigen.

8 Wählen Sie die Aktion *CorrelatedEvent* aus, klicken Sie auf *Löschen* und anschließend auf *Ja*, um den Löschvorgang zu bestätigen.



9 Wählen Sie im Menü *Ereignisquellenverwaltung* die Option *Live-Ansicht* aus.

10 Klicken Sie in der grafischen Ereignisquellenhierarchie mit der rechten Maustaste auf *Allgemeiner Collector* und wählen Sie *Stoppen*.

11 Schließen Sie das Fenster „Ereignisquellenverwaltung“.

12 Klicken Sie auf die Registerkarte *Vorfälle*.

13 Öffnen Sie den Vorfallansichts-Manager.

14 Wählen Sie *Testvorfall1* aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie *Löschen*.

6.3 Verwenden realer Daten

Zum Starten mit echten Daten müssen Sie Collectors importieren und konfigurieren, die für Ihre Umgebung passend sind, Ihre eigenen Regeln erstellen, iTRAC-Workflows erstellen usw. Weitere Informationen finden Sie im *Sentinel Rapid Deployment User Guide* (Sentinel Rapid Deployment-Benutzerhandbuch). Mit Sentinel-Lösungspaketen können Sie schnell starten. Weitere Details finden Sie auf der Webseite Sentinel Content Page (http://support.novell.com/products/sentinel/sentinel61.html).

Deinstallation von Sentinel Rapid Deployment 7

7.1 Deinstallieren des Sentinel Rapid Deployment-Servers

1. Melden Sie sich als `root`-Benutzer an.
2. Wechseln Sie zum `setup`-Verzeichnis.

   `cd <Installationsverzeichnis>/setup`
3. Führen Sie das Skript `uninstall.sh` aus, um den Sentinel Rapid Deployment-Server zu deinstallieren:

   `./uninstall.sh`

   Das Skript informiert Sie darüber, dass Sentinel Rapid Deployment vollständig entfernt wird.
4. Geben Sie an, ob der Benutzer bei der Deinstallation des Sentinel Rapid Deployment-Servers entfernt werden soll. Drücken Sie `y`, wenn der Benutzer entfernt, bzw. `n`, wenn er nicht entfernt werden soll.
5. Geben Sie an, ob die Gruppe bei der Deinstallation des Sentinel Rapid Deployment-Servers entfernt werden soll. Drücken Sie `y`, wenn die Gruppe entfernt, bzw. `n`, wenn sie nicht entfernt werden soll.
6. Drücken Sie `y`, wenn die Gruppe entfernt, bzw. `n`, wenn sie nicht entfernt werden soll.

7.2 Deinstallieren des Remote-Collector-Managers und der Sentinel-Client-Anwendungen

7.2.1 Linux

1. Melden Sie sich als `root`-Benutzer an.
2. Beenden Sie vor der Deinstallation des Collector-Managers ggf. die Sentinel Rapid Deployment-Dienste:

   `<Installationsverzeichnis>/bin/sentinel.sh stop`
3. Gehen Sie zu folgender Position:

   `<Installationsverzeichnis>/_uninst`

4 Führen Sie eine der folgenden Aktionen durch:

Modus	Befehl
GUI	`./uninstall.bin`
	Fahren Sie mit Schritt 5 auf Seite 86 fort.
Konsole	`./uninstall.bin -console`
	Fahren Sie entsprechend den Bildschirmanweisungen fort.

5 Wählen Sie eine Sprache aus und klicken Sie auf *OK*.

6 Klicken Sie im Sentinel-UninstallShield-Assistenten auf *Weiter*.

7 Wählen Sie die zu deinstallierenden Komponenten aus und klicken Sie auf *Weiter*.

8 Stellen Sie sicher, dass alle ausgeführten Sentinel-Anwendungen gestoppt sind, und klicken Sie auf *Weiter*.

Es wird eine Zusammenfassung der für die Deinstallation ausgewählten Funktionen angezeigt.

9 Klicken Sie auf *Deinstallieren*.

10 Klicken Sie auf *Fertig stellen*.

7.2.2 Windows

1 Melden Sie sich als Administratorbenutzer an.

2 Beenden Sie vor der Deinstallation des Collector-Managers ggf. die Sentinel Rapid Deployment-Dienste:

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

3 Führen Sie eine der folgenden Aktionen durch:

- Wählen Sie *Start* > *Alle Programme* > *Sentinel* > *Sentinel deinstallieren*.
- Wählen Sie *Start* > *Ausführen*, geben Sie `<Installationsverzeichnis>\_uninst` ein und doppelklicken Sie auf `uninstall.exe`.

4 Wählen Sie eine Sprache aus und klicken Sie auf *OK*.

Der UninstallShield-Assistent für Sentinel Rapid Deployment wird angezeigt.

5 Klicken Sie auf *Weiter*.

6 Wählen Sie die zu deinstallierenden Komponenten aus und klicken Sie auf *Weiter*.

7 Stellen Sie sicher, dass alle ausgeführten Sentinel-Anwendungen gestoppt sind, und klicken Sie auf *Weiter*.

Es wird eine Zusammenfassung der für die Deinstallation ausgewählten Funktionen angezeigt.

8 Klicken Sie auf *Deinstallieren*.

9 Wählen Sie das Neubooten des Systems aus und klicken Sie auf *Fertig stellen*.

7.2.3 Vorgehensweisen im Anschluss an die Deinstallation

Nach der Deinstallation der Anwendungen bleiben einige Systemeinstellungen bestehen, die manuell entfernt werden können. Diese Einstellungen sollten entfernt werden, bevor eine „saubere“ Installation von Sentinel ausgeführt wird, insbesondere dann, wenn bei der Deinstallation von Sentinel Fehler aufgetreten sind.

Hinweis: Bei Linux wird durch die Deinstallation des Collector-Managers oder der Client-Anwendungen der Sentinel-Administratorbenutzer nicht aus dem Betriebssystem entfernt. Sie müssen bei Bedarf diesen Benutzer manuell entfernen.

- „Linux“ auf Seite 87
- „Windows“ auf Seite 87

Linux

1. Melden Sie sich als `root`-Benutzer an.
2. Entfernen Sie die Inhalte im `<Installationsverzeichnis>` der Sentinel-Software.
3. Entfernen Sie die folgenden Dateien im Verzeichnis`/etc/init.d`, falls vorhanden:

   `sentinel`

   Das gilt nur, wenn Collector-Manager installiert ist.
4. Stellen Sie sicher, dass niemand als Sentinel-Administratorbenutzer angemeldet ist (standardmäßig „esecadm“), und entfernen Sie dann den Benutzer, das Basisverzeichnis sowie die Gruppe „esec“:
   - Führen Sie Folgendes aus: `userdel -r esecadm`.
   - Führen Sie Folgendes aus: `groupdel esec`.
5. Entfernen Sie das Verzeichnis `/root/InstallShield`.
6. Entfernen Sie den InstallShield-Abschnitt von `/etc/profile`.
7. Führen Sie einen Neustart Ihres Computers durch.

Windows

1. Löschen Sie den Ordner `%CommonProgramFiles%\InstallShield\Universal` und seinen gesamten Inhalt.
2. Löschen Sie den Ordner `<Installationsverzeichnis>` (standardmäßig: `C:\Programme\Novell\Sentinel6`).
3. Klicken Sie mit der rechten Maustaste auf *Arbeitsplatz* > *Eigenschaften* > *Registerkarte „Erweitert“*.
4. Klicken Sie auf die Schaltfläche *Umgebungsvariablen*.
5. Löschen Sie die folgenden Variablen (sofern vorhanden):
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME

- ESEC_CONF_FILE
- WORKBENCH_HOME

6. Entfernen Sie alle Einträge in der Umgebungsvariablen PATH, die auf die Sentinel-Installation verweisen.
7. Löschen Sie sämtliche Sentinel-Verknüpfungen vom Desktop.
8. Löschen Sie den Verknüpfungsordner *Start > Programme > Sentinel* aus dem *Startmenü*.
9. Führen Sie einen Neustart Ihres Computers durch.

Aktualisieren des Hostnamens von Sentinel Rapid Deployment

A

A.1 Server

Auf dem Sentinel-Server werden Hostnamen-Änderungen während der Laufzeit oder während der Installation automatisch aktualisiert. Wenn der Server nach einer Hostnamen-Aktualisierung nicht ordnungsgemäß funktioniert, müssen Sie manuell Folgendes überprüfen:

- Alle `jnlp`-Dateien und die Datei `configuration.xml` werden beim Sentinel-Neustart aktualisiert.
- Der Hostnamen-Eintrag in der Datenbanktabelle `sentinel_host` wird aktualisiert.
- Alle Referenzen zur lokalen Schleife (localhost oder 127.0.0.1) in der Datei `<Installationsverzeichnis>/config/configuration.xml` bleiben unverändert.

A.2 Client-Anwendungen

Für die Client-Anwendungen müssen Sie den Server-Hostnamen oder die IP-Adresse an folgenden Stellen manuell so ändern, dass sie auf den korrekten Server verweisen:

- `<Installationsverzeichnis>/config/configuration.xml`.

  Das Sentinel Control Center und der Solution Designer verwenden diese Informationen.
- Die Hilfe-URL, die in der Datei `<Installationsverzeichnis>/config/SentinelPreferences.properties` angegeben ist.
- Führen Sie folgenden Befehl aus, um den Hostnamen in der Datei `sdm.connect` zu aktualisieren:

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

Tipps zur Fehlersuche

B

In diesem Abschnitt finden Sie eine Liste mit Vorschlägen zur Fehlersuche, die Ihnen die Lösung einiger Installationsprobleme, die bei Sentinel Rapid Deployment auftreten können, erleichtern sollen.

B.1 Fehlschlagen der Datenbankauthentifizierung nach der Eingabe eines ungültigen Berechtigungsnachweises

Häufige Ursache: Die Datenbankauthentifizierung schlägt fehl, falls bei der Konfiguration des Sentinel Rapid Deployment-Servers für die LDAP-Authentifizierung ein ungültiger LDAP-Server-Hostname oder eine ungültige IP-Adresse eingegeben wird.

Aktion: Stellen Sie sicher, dass ein gültiger LDAP-Server-Hostname bzw. eine gültige IP-Adresse definiert sind.

B.2 Sentinel-Weboberfläche lässt sich nicht starten

Häufige Ursache: Sie haben Sentinel Rapid Deployment auf einem Computer installiert, auf dem ein Identity Audit-Prozess entweder ausgeführt wird oder unvollständig deinstalliert ist.

Aktion: Sentinel Rapid Deployment und Novell Identity Audit können nicht auf demselben Computer installiert werden. Bevor Sie Sentinel Rapid Deployment auf einem Computer installieren, auf dem Identity Audit installiert ist, sorgen Sie dafür, dass Identity Audit vollständig deinstalliert wird.

Wenn die Identity Audit-Prozesse nicht vollständig gestoppt wurden, kann die Deinstallation von Identity Audit nicht erfolgreich abgeschlossen werden. In diesem Fall besteht das Risiko, dass bei der Installation von Sentinel Rapid Deployment oder beim Starten der zugehörigen Anwendungen Konflikte auftreten.

1. Führen Sie folgenden Befehl aus, um die Identity Audit-Dienste herunterzufahren:

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

2. Führen Sie folgenden Befehl aus, um sicherzustellen, dass alle Identity Audit-Prozesse gestoppt wurden:

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

3. Stoppen Sie etwaige verbliebene Prozesse bei Bedarf manuell.

```
kill -9 pid
```

4 Deinstallieren Sie Identity Audit mit den erforderlichen `root`-Berechtigungen.

Weitere Informationen finden Sie im Benutzerhandbuch für Identity Audit (http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/).

B.3 Der Remote-Collector-Manager erzeugt eine Ausnahme in Windows 2008, wenn UAC aktiviert wird

Problem: Melden Sie sich als ein Benutzer an, der zur Administrator-Gruppe gehört, und führen Sie in einer Terminal-Eingabeaufforderung den Befehl `setup.bat` aus, um den Collector-Manager zu installieren. Führen Sie einen Neustart des Systems durch oder starten Sie den Collector-Manager-Dienst manuell, melden Sie sich dann mit demselben Benutzerberechtigungsnachweis an. In der Datei `collector_manager0.0.log` werden Ausnahmen protokolliert, die sich auf die folgenden Collector-Manager-Funktionen auswirken:

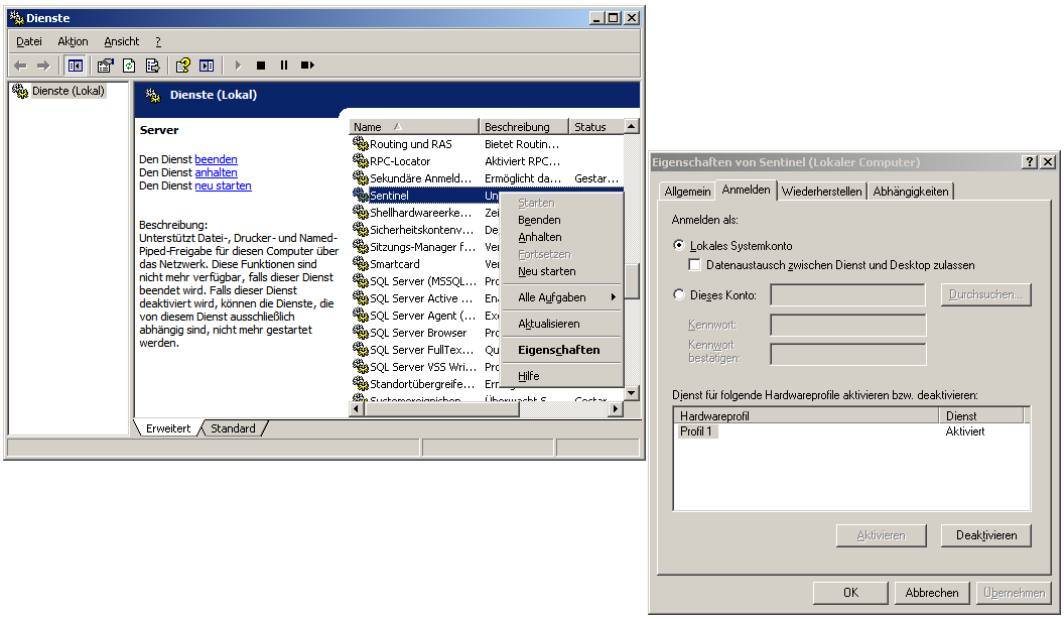
- Die Zuordnungen werden nicht initialisiert.
- Sie können mit dem File Connector keine Ereignisquellendatei im Dateisystem des Collector-Manager-Computers (Win2008) auswählen.

Häufige Ursache: Sie haben den Collector-Manager auf einem Computer mit Windows 2008 SP1 Standardedition 64-Bit installiert. Standardmäßig ist auf dem Computer die Benutzerzugriffssteuerung *aktiviert*.

Aktion: Ändern Sie für die Sentinel Rapid Deployment-Dienste den unter *Anmelden als* angegebenen Benutzer in den aktuellen Benutzer. Standardmäßig ist unter *Anmelden als* die Option *Lokales Systemkonto* ausgewählt. So ändern Sie die Standardeinstellung:

1 Führen Sie `services.msc` aus, um das Fenster *Dienste* zu öffnen.

2 Klicken Sie mit der rechten Maustaste auf „Sentinel“ und wählen Sie dann *Eigenschaften* aus.



3 Wählen Sie im Fenster „Eigenschaften von Sentinel“ die Registerkarte *Anmelden* aus.

4 Wählen Sie *Dieses Konto* aus, geben Sie dann den Berechtigungsnachweis für den aktuellen Benutzer ein, den Sie zum Installieren des Collector-Managers verwendet haben.

B.4 Für Collector-Manager-Images wird keine UUID erstellt

Wenn Sie Images von einem Collector-Manager-Server erstellen (z. B. mit ZenWorks Imaging) und diese Images auf verschiedenen Computern wiederherstellen, führt Sentinel Rapid Deployment keine eindeutige Identifizierung dieser neuen Collector Manager-Instanzen durch. Dies liegt an mehrfach verwendeten UUIDs.

Sie müssen die UUID generieren, indem Sie auf den neu installierten Collector-Manager-Systemen folgende Schritte durchführen:

1 Löschen Sie die Datei `host.id` bzw. `sentinel.id` im Ordner `<Installationsverzeichnis>/data`.

2 Starten Sie den Collector-Manager neu.

Der Collector-Manager generiert automatisch die UUID.

Bewährte Verfahren für die Pflege der PostgreSQL-Datenbank

C

Sie können eine Feinabstimmung der Datenbank vornehmen, um die Leistung des Datenbankservers zu verbessern. Die in diesem Abschnitt angegebenen Begrenzungen sind Näherungswerte. Es handelt sich nicht um „harte“ Begrenzungen. In sehr dynamischen Systemen hat es sich jedoch bewährt, Puffer zu bilden und Wachstum zu ermöglichen.

C.1 Modifizieren der Konfigurationsparameter für den Arbeitsspeicher

Für die Feinabstimmung des PostgreSQL-Datenbankservers können in der Datei `<install_dir>/3rd party/postgresql/data/postgresql.conf` folgende Parameter für die Arbeitsspeicherkonfiguration angepasst werden:

- **shared_buffers:** Legt fest, wieviel Arbeitsspeicher für PostgreSQL-Caching-Daten reserviert wird. Zur Erzielung einer besseren Leistung können Sie diesen Parameterwert auf ein Viertel des verfügbaren RAM einstellen.
- **effective_cache_size:** Legt fest, wieviel Arbeitsspeicher für das Festplatten-Caching des Betriebssystems und der Datenbank zur Verfügung steht. Sie können die Größe des Parameters berechnen, indem Sie einkalkulieren, wie viel vom Betriebssystem und anderen Anwendungen verwendet wird. Für diesen Parameter kann die Hälfte des gesamten verfügbaren Arbeitsspeichers definiert werden.
- **work_mem:** Legt die Menge an Arbeitsspeicher fest, der von internen Sortiervorgängen und Hash-Tabellen verwendet wird, bevor zu temporären Festplattendateien gewechselt wird. Der Wert wird in Kilobyte angegeben. Der Standardwert lautet 1.024 Kilobyte (1 MB).

  Bei einer komplexen Abfrage werden möglicherweise mehrere Sortier- oder Hash-Vorgänge gleichzeitig durchgeführt. Jeder Vorgang nutzt soviel Arbeitsspeicher, wie für den Parameter „work_mem“ angegeben ist, bevor er beginnt, Daten in temporären Festplattendateien abzulegen. Wenn Sie mehrere Berichte in Ihrem Sentinel Rapid Deployment-System planen, setzen Sie diesen Wert auf 500 MB bis 1 GB.
- **maintenance_work_mem:** Legt die maximale Menge an Arbeitsspeicher fest, die für Vorgänge zur Wartung der Datenbank, z. B. VACUUM, CREATE INDEX und ALTER TABLE ADD FOREIGN KEY, verwendet werden soll. Der Wert wird in Kilobyte angegeben. Der Standardwert lautet 16.384 Kilobyte (16 MB).

  Größere Einstellungen können die Leistung für das Bereinigen (Vacuuming) und Wiederherstellen von Datenbank-Dumps verbessern. Ändern Sie diesen Parameter nicht. Der Standardwert ist für die Sentinel Rapid Deployment-Vorgänge ausreichend.

C.2 Verringern der E/A-Auswirkung von Bereinigungs-/Analyse-Prozessen

Es gibt mehrere Möglichkeiten, die Leistung der PostgreSQL-Datenbank zu verbessern.

- Die folgenden beiden Parameter steuern automatische Bereinigungsprozesse. Standardmäßig sind diese Parameter während der Installation des Sentinel Rapid Deployment-Servers auskommentiert, und Sie müssen den Kommentar entfernen und die Werte festlegen.
  - **vacuum_cost_delay:** Legt fest, wie lange der Prozess inaktiv bleibt, wenn die Kostengrenze überschritten wurde. Sie können diesen Wert beispielsweise auf 100 festlegen.
  - **vacuum_cost_limit:** Legt die akkumulierten Kosten fest, die bewirken, dass der Bereinigungs-Prozess (Vacuuming) deaktiviert wird. Sie können diesen Wert beispielsweise auf 10000 festlegen.

    Wenn Sie diese Parameter auf einen Wert ungleich Null setzen, wird die E/A-Auswirkung des Bereinigungs- und Analysebefehls auf die normale Datenbankaktivität verringert. Da die Bereinigung länger als früher dauert, kann das Ausführen der Berichte die Leistung minimal beeinträchtigen.
- Standardmäßig ist der Prozess `autovacuum` auf „true“ gesetzt und wird regelmäßig ausgeführt, um Festplattenspeicherplatz frei zu machen und die Planerstatistik zu aktualisieren. Wenn die Datenbankgröße anwächst, kann `autovacuum` nicht alle Datenbankobjekte warten. Wenn in diesen Fällen die Leistung vermindert ist, führen Sie das Skript `AnalyzePartitions.sh` als Cron(-Daemon)-Auftrag aus. Dieser Cron(-Daemon)-Auftrag sollte von dem Benutzer festgelegt werden, der Eigentümer der Sentinel Rapid Deployment-Prozesse ist.

  Beispiel:

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

  Hierbei gilt:

  - `30` ist die Zeit in Minuten.
  - `11` ist die Zeit in Stunden.
  - `ESEC_HOME` ist der absolute Pfad der Datenbank.

  In diesem Beispiel wird das Skript täglich um 11:30 Uhr ausgeführt.
- Planen Sie die Archivierung nach Möglichkeit nicht während des Zeitraums der Berichterstellung. Wenn Sie beide Prozesse zusammen planen, wechselt die Berichterstellung aufgrund von PostgreSQL-Fehlern in den Wartemodus und beginnt mit der Verarbeitung der Daten erst nach Abschluss der Archivierung. Diese Änderung wirkt sich auf die Leistung der Datenbank aus.